EPRI | ELECTRIC POWER RESEARCH INSTITUTE

EPRI Guidelines for PRA Data Analysis

3002000774

EPRI Guidelines for PRA Data Analysis

3002000774

Technical Update, December 2013

EPRI Project Manager

M. Presley

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATIONS, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Hughes Associates, Inc.

Science Applications International Corporation (SAIC)

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organizations, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Hughes Associates, Inc.
Risk Informed Engineering Section
Power Systems Division
3610 Commerce Drive
Suite 817
Baltimore, MD 21227

Principal Investigator
E. Collins

Technical Analysts
P. Macheret
E. Cook

Science Applications International Corporation (SAIC)
3465-A Box Hill Corporate Center Drive
Abingdon, Maryland 21009

Technical Analyst
C. Frank

This publication is a corporate document that should be cited in the literature in the following manner:

EPRI Guidelines for PRA Data Analysis. EPRI, Palo Alto, CA: 2013. 3002000774.

REPORT SUMMARY

One of the primary tasks to support probabilistic risk assessment (PRA) is a thorough and traceable data analysis to provide as much plant-specific history as possible to the PRA modeling, or well-founded industry information where plant-specific data are insufficient or unavailable, and to characterize the uncertainty surrounding this information to allow sensitivity analyses to be performed.

Recent efforts have been made by industry and the Nuclear Regulatory Commission (NRC) to establish a minimum set of technical requirements (to assess technical adequacy) for the performance of various PRA tasks, including data analysis.

These requirements have formed the basis for the current peer review process sponsored by the Pressurized Water Reactor Owners Group (PWROG) and Boiling Water Reactor Owners Group (BWROG), where teams of experts review PRA inputs and results against the ASME/ANS PRA Standard supporting requirements to identify areas and issues requiring attention with the intent of assessing PRA technical quality to support risk-informed applications. As a result of these peer reviews, insights have been gained that provide feedback to data analysis practices and can inform a set of guidelines for future PRA updates.

It is with this goal in mind that the Electric Power Research Institute (EPRI) is issuing these Data Analysis Guidelines.

Background

This document is aimed primarily at data analysts tasked with supporting Nuclear Power Plant (NPP) PRAs. It is intended to serve the needs of a PRA team by providing a structured framework for conducting and documenting a PRA data analysis. This document pays particular attention to task interfaces and interactions between the data analysis and other disciplines in a PRA. In addition, each technical subsection discusses technical supporting requirements indicated in the ASME/ANS PRA Standard, as endorsed by Regulatory Guide 1.200. The ASME/ANS PRA Standard recognizes that required PRA capability varies with application and defines Supporting Requirements for a range of capabilities in terms of three levels, defined and labeled either Capability Category I, II, or III, "so that requirements can be developed and presented in a manageable way." Regulatory Guide 1.200 states "In general, the staff anticipates that current good practice, that is, Capability Category II of the ASME/ANS standard, is the level of detail that is adequate for the majority of applications."

Objectives

The objective of this report is to provide guidelines for estimating frequencies of initiating events (IEs), component failure and unavailability rates, and common cause failure (CCF) rates in support of PRA quantification. The use of Bayesian updating and the characterization of uncertainty are also discussed, as well as guidance on the documentation of PRA databases. This report cites existing data analysis methods and data sources, but also provides insights based on recent PRA peer reviews, as well as technical requirements indicated in regulatory and consensus standard documents.

Approach

The data analysis guidelines were developed using a structured, systematic approach consisting of the following tasks:

- Framework Development – establishment of an annotated outline with topics for inclusion in the data guidelines
- Draft Guidelines Development – compilation of experience and guidance in the topic areas identified, as well as information on standard requirements and peer review findings
- Public Review and Comment – review by the technical advisory committee to solicit feedback and other perspectives from industry
- Report Publication – incorporation of comments and preparation of a document for public distribution

EPRI Perspective

This report documents a set of guidelines from EPRI on the topic of PRA Data Analysis. It is anticipated that this guidance will be used by the industry as part of NPP PRA updates performed to reflect the most current plant experience. It is also expected that as the methodology is applied at a wide variety of plants, the document may benefit from user feedback, which will be used for future improvements to better support industry-wide data issues regarding the implementation of PRA.

Keywords

Bayesian Updating
Component Reliability
Component Unavailability
Data Analysis
Initiating Event Frequency
Probabilistic Risk Assessment (PRA)

LIST OF ACRONYMS

AC	Alternating Current
ACRS	Advisory Committee on Reactor Safeguards
AIChE	American Institute of Chemical Engineers
ANS	American Nuclear Society
AOP	Abnormal Operating Procedure
AOV	Air-Operated Valve
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without SCRAM
AFW	Auxiliary Feed Water
B&WOG	Babcock & Wilcox Owners Group
BWR	Boiling Water Reactor
BWROG	Boiling Water Reactor Owners Group
CAFTA	Computer-Aided Fault Tree Analysis (software)
CAR	Corrective Action Report
CCCG	Common-Cause Component Group
CCDP	Conditional Core Damage Probability
CCF	Common Cause Failure
CCFA	Common Cause Failure Analysis
CCPS	Center for Chemical Process Safety
CCW	Component Cooling Water
CDF	Core Damage Frequency
CLERP	Conditional Large Early Release Probability
CR	Condition Report
CRDM	Control Rod Drive Mechanism
CS	Containment Spray
CVCS	Chemical and Volume Control System
DA	Data Analysis

DAS	Data Acquisition System
DC	Direct Current
DDP	Diesel-Driven Pump
DF	Dependent Failure
DHR	Decay Heat Removal
EC	Empirical Correlation
ECCS	Emergency Core Cooling Systems
EDG	Emergency Diesel Generator
EF	Error Factor
EHC	Electro-Hydraulic Controls
EOOS	Equipment Out of Service
EOP	Emergency Operating Procedure
EPIX	Equipment Performance and Information Exchange system
EPRI	Electric Power Research Institute
ET	Event Tree
FEG	Functional Equipment Group
FM	Failure Mode
FMEA	Failure Modes and Effects Analysis
FSAR	Final Safety Analysis Report
FTS	Failure to Start
FV	Fussell-Vesely importance measure
HLR	High Level Requirement
HPI	High Pressure Injection
HPSI	High Pressure Safety Injection
HRA	Human Reliability Analysis
HVAC	Heating, Ventilating, and Air Conditioning
ICDE	International Common-Cause Data Exchange
IE	Initiating Event

IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
INPO	Institute for Nuclear Power Operations
IPE	Individual Plant Examination
IPRD	In-Plant Reliability Data system
IPEEE	Individual Plant Examination of External Events
IRT	Independent Review Team
ISLOCA	Interfacing Systems LOCA
LB	Lower Bound
LER	Licensee Event Report
LERF	Large, Early Release Frequency
LLOCA	Large LOCA
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPI	Low Pressure Injection
LPSD	Low Power and/or Shutdown
LWR	Light Water Reactor
MCR	Main Control Room aka Control Room
MDP	Motor-Driven Pump
MLE	Maximum Likelihood Estimate
MLT	Mean-Logistics-Time
MOV	Motor-Operated Valve
MR	Maintenance Rule
MRFF	Maintenance Rule Functional Failure
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSPI	Mitigating System Performance Index
MTBF	Mean-Time-Between Failure

MWO	Maintenance Work Order
NEI	Nuclear Energy Institute
NPP	Nuclear Power Plant
NPRDS	Nuclear Plant Reliability Data System
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
NUREG	Nuclear Regulatory Commission Document
OEM1	Original Equipment Manufacturer
P&ID	Piping and Instrumentation Diagram
PI	Performance Indicator
PM	Preventive Maintenance
PORV	Pressure (Pilot) Operated Relief Valve
POS	Plant Operational State or Plant Operating State
PPC	Plant Process Computer
PRA	Probabilistic Risk Assessment (aka PSA)
PSA	Probabilistic Safety Assessment (aka PRA)
PWR	Pressurized Water Reactor
PWROG	Pressurized Water Reactor Owners Group
RAW	Risk Achievement Worth
RCIC	Reactor Core Isolation Cooling system
RCS	Reactor Coolant System
RES	U.S. NRC Office of Research
RG	Regulatory Guide
RHR	Residual Heat Removal
ROP	Reactor Oversight Program
RPS	Reactor Protection System
SAPHIRE	Systems Analysis Program for Hands-on Integrated Reliability Evaluations (software)

SCNID	Simplified Constrained Non-Informative Distribution
SD	Shutdown
SGTR	Steam Generator Tube Rupture
SISBO	Self-Induced Station Blackout
SI	Safety Injection
SLOCA	Small Loss of Coolant Accident
SOKC	State of Knowledge Correlation
SP	Surveillance Procedure
SPAR	Standardized Plant Analysis Risk
SR	Supporting Requirement
SSCs	Structures, Systems, and Components
SSIE	Support System Initiating Event
SSFF	Safety System Functional Failure
SW	Service Water
TC	Type Code
TDP	Turbine-Driven Pump
TM	Test and Maintenance
TSC	Technical Support Center
TT	Turbine Trip
UAI	Unavailability Index
UB	Upper Bound
UPS	Uninterruptable Power Supply
URI	Unreliability Index
WOG	Westinghouse Owners Group, now merged with the B&WOG to form the PWROG

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

1.1 Background

The occurrence of the accident at Three Mile Island Unit 2 in March 1979 alerted the nuclear power industry to the need to implement probabilistic risk assessment (PRA) for evaluating potential accidents that had not been foreseen in the design basis evaluations. Industry expertise was convened at several conferences under the auspices of the American Nuclear Society (ANS) and the Institute of Electrical and Electronics Engineers (IEEE) to spearhead discussions on the types of methods available and how they could be expanded and enhanced to provide sufficient tools for risk estimation. The results were documented in the PRA Procedures Guide [1] and regulatory requirements[1] soon followed for the nuclear industry to perform PRAs on all existing plants.

While risk modeling could evaluate the design features, and the combination of equipment and human failures that could lead to accident sequences, the actual probability of the model results could not be evaluated without data to characterize the likelihood of the plant perturbations that could set off the chain of undesired events, as well as the probability of component failure to perform its required safety function in response to these initiating events. Thus, it became clear that attention needed to be paid to the data input to the models as well as the logic models themselves.

Programs such as the Maintenance Rule (MR) [2] required plants to gather specific information on their own history of component performance, and industry-wide efforts were initiated to allow a basis of comparison and to provide baseline quantitative information across a wider pool of experience [3, 4, 5].

It is now a matter of course that one of the primary tasks in support of a "living" PRA model that reflect a plant, as built and as operated, is a thorough and traceable data analysis. The intent of the data analysis is to provide as much plant-specific history as possible to the PRA modeling, to provide well-founded industry information where plant-specific data are insufficient or unavailable, and to characterize the uncertainty surrounding this information to allow sensitivity analyses to be performed.

Recent efforts have been made by industry [6, 7] and the Nuclear Regulatory Commission (NRC) [8] to establish a minimum set of technical requirements (to assess technical adequacy) for the performance of various PRA tasks, including data analysis.

---

[1] Generic Letter (GL) 88-20 required all licensees to perform an Independent Plant Examination (IPE), which generally took the form of a PRA. Supplements to GL 88-20 required the performance of IPE for External Events (IPEEE).

These requirements have formed the basis for the current peer review process sponsored by the Pressurized Water Reactor Owners Group (PWROG) and Boiling Water Reactor Owners Group (BWROG), where teams of experts review PRA inputs and results against the American Society of Mechanical Engineers (ASME)/ANS PRA Standard [7] supporting requirements to identify areas and issues requiring attention with the intent of assessing PRA technical quality to support risk-informed applications. As a result of these peer reviews, insights have been gained that provide feedback to data analysis practices and can inform a set of guidelines for future PRA updates.

It is with this goal in mind that the Electric Power Research Institute (EPRI) is issuing these Data Analysis Guidelines.

1.2 Programmatic Overview

This report documents a set of guidelines from EPRI on the topic of PRA Data Analysis. It is anticipated that this guidance will be used by the industry as part of nuclear power plant (NPP) PRA updates performed to reflect the most current plant experience. It is also expected that as the methodology is applied at a wide variety of plants, the document may benefit from user feedback, and future improvements.

1.2.1 Objectives

The objective of this report is to provide guidelines for estimating frequencies of initiating events, component failure and unavailability rates, and common cause failure (CCF) rates in support of PRA quantification. The use of Bayesian updating and the characterization of uncertainty are also discussed, as well as guidance on the documentation of PRA databases. This report cites existing data analysis methods and data sources, but also provides insights based on recent PRA peer reviews, as well as technical requirements indicated in regulatory and consensus standard documents.

The ASME/ANS PRA Standard [7], endorsed by Regulatory Guide 1.200 [8] recognizes that required PRA capability varies with the application and defines Supporting Requirements for a range of capabilities in terms of three levels, defined and labeled either Capability Category I, II, or III, “so that requirements can be developed and presented in a manageable way.” Regulatory Guide 1.200 states “In general, the staff anticipates that current good practice, that is, Capability Category II of the ASME/ANS standard, is the level of detail that is adequate for the majority of applications.”

The guidance in this report is also intended to support a PRA data analysis that would satisfy the relevant data analysis requirements in the ASME/ANS PRA Standard. While these Guidelines cannot “guarantee” the user will meet Capability Category II of the PRA Standard DA data elements by their application, the guidance herein strives to provide the user with the tools, techniques and awareness to achieve Capability Category II.

1.2.2 Project Tasks

The data analysis guidelines were developed using a structured, systematic approach consisting of the following tasks:

- Framework Development – establishment of an annotated outline with topics for inclusion in the data guidelines
- Draft Guidelines Development – compilation of experience and guidance in the topic areas identified, as well as information on standard requirements and peer review findings
- EPRI Review and Comment – review by the EPRI Program Manager and internal contractor review to solicit feedback and other perspectives
- Update and Issuance for Public Review and Comment – incorporation of EPRI comments and preparation of a document for public distribution with the intent of soliciting comments

1.3 Scope

This document describes the process and technical bases for the performance of a data analysis as part of a *Level 1, at power, Internal Events PRA*.

The purpose of PRA data analysis is to identify, characterize, and quantify event sequence initiating events, as well as events representing component failures and unavailabilities used in the development and quantification of a PRA model. Since most plants have already undergone a PRA, these data analyses generally involve the update of a previous dataset to include the latest plant-specific failure information and to ensure that the most current generic data are being applied.

The scope of a PRA data analysis involves several tasks reflecting interrelated activities that are generally characterized by the following categories:

- Initiating Event data – information on the major plant/system disruptions from at-power internal event conditions that can initiate an accident sequence.
- Component Failure data – instances of equipment failure to perform its required function characterized by particular failure modes and modeled as basic events in the PRA models.
- Unavailability data –although unavailability data is collected from a variety of sources, PRA model unavailability data is related to probability that a system, train or component is not capable of supporting a function modeled in the PRA. An understanding of the system and how it is modeled in the PRA model and how it relates to success criteria is needed. This information for each system is documented in the Maintenance Rule (MR) Basis document (if the system is an MR system), and the system notebook, and the success criteria notebook.
- CCF data – estimates of multiple redundant equipment failure due to the same underlying cause.
- Uncertainty Analysis – integral to the data analysis is characterization of the uncertainty surrounding the data estimates input to the PRA models.
- Documentation – providing a thorough description of the process used to develop the data as well as a traceable database that facilitates future updates and peer reviews.

1.4 Intended Audience and Prerequisite Expertise

The purpose of this document is to provide a structured framework for conducting and documenting a PRA data analysis and to highlight the caveats and exceptions that the analyst should be aware of along the way. It is not the intent of this project to develop a new or unique detailed methodology to address PRA data needs, but rather to present existing perspectives and methods while interjecting information based on the experience of the authors and feedback from industry peer reviews. This document pays particular attention to task interfaces and interactions between the data analysis and other disciplines in a PRA. In addition, each technical subsection discusses technical supporting requirements indicated in the ASME/ANS PRA Standard [7].

The data analysis process discussed in these Guidelines presents existing data analysis methods that are currently in widespread use and that address the requirements of the ASME/ANS PRA Standard [7] , as endorsed by Regulatory Guide (RG) 1.200 [8], aimed at Capability Category II. However, some documents are cited in these Guidelines to provide a historical basis because the analyst can expect to see references to them in the PRA literature and in PRAs they are tasked with updating.

It should be recognized that while this document provides sound concepts and guidance, data analysis requires **judgment** throughout the process. The decisions that are made by the analyst to include or exclude certain data and during categorization of the data are an inherent part of the process. It is important, therefore, to document the process followed and the judgments that are made along the way to:

1. Allow reviewers and users of the database to understand the basis for the numerical values
2. Identify areas where analysis can be improved in the future
3. Provide input to the uncertainty and sensitivity analysis task

1.4.1 Guidance for Novice Data Analysts

It is strongly recommended that novice data analysts begin by reading Section 2 of these Guidelines in their entirety to obtain an overview of the data analysis process and the theory of the concepts that are presented later. Then, the novice can access the individual chapters as needed to develop the specific data required by his/her project.

1.4.2 Guidance for Seasoned Data Analysts

Since seasoned data analysts are likely to be familiar with the theory behind the data concepts, they can jump directly to the chapter that covers the topic of interest to them.

1.5 Report Structure

This report is structured in the following sections:

- *Section 1* delineates the objectives and scope of this report, as well as some background information on the motivation for the guidelines.
- *Section 2* provides an overview of the guidance provided in the report. It is intended to show the user various steps in conducting data analysis and how these steps fit into an overall PRA.

- *Section 3* describes the generic process for performing Bayesian updating to combine sparse plant-specific information with broader industry-wide generic data. The concepts in this chapter are then applied to specific data applications (for example, initiating event analysis, component unreliability, and so on) in the proceeding chapters.
- *Section 4* describes the guidance for data analysis for initiating events, the occurrences, or upsets, which cause a plant disruption resulting in a challenge to one or more of the plant systems, characterized via accident sequence analysis.
- *Section 5* provides guidance for component failure data analysis that provides input for the quantification of fault tree basic events related to component failure to function.
- *Section 6* describes analysis of data for maintenance and test-related component unavailability, so that fault tree basic events related to a component not being available (on line) to perform their function can be quantified.
- *Section 7* discusses CCF data analysis guidelines for evaluating the likelihood of multiple cotemporaneous equipment failures due to a common cause.
- *Section 8* describes an overview for what to include in the documentation.
- *Section 9* provides the document references.
- *Appendix A* contains the definition of terms used in this report.

2
DATA GUIDELINES FRAMEWORK

2.1 Introduction

This section is primarily directed at the new data analyst, but also provides a good refresher and background for the seasoned data analyst. The section begins by putting data analysis in perspective with the other tasks of a PRA and by discussing how data analysis is covered in the ASME/ANS PRA Standard [7]. Next, an overview of the data analysis process is provided so that the analyst understands (at a high level) the steps involved in the process and the key concepts, including commonly used formulas, for each of these steps. Details on the specific techniques for performing these data analysis steps are provided in later chapters of these guidelines.

2.2 Relationship to Other PRA Tasks

According to Regulatory Guide 1.200 [8], "Parameter estimation analysis quantifies the frequencies of the initiating events, as well as the equipment failure probabilities and equipment unavailabilities of the modeled systems. The estimation process includes a mechanism for addressing uncertainties and has the ability to combine different sources of data in a coherent manner, including the actual operating history and experience of the plant when it is of sufficient quality, as well as applicable generic experience."

The Data Analysis (DA) element defined in the ASME/ANS PRA Standard [7] interfaces with seven other technical elements that comprise a Level 1/large, early release frequency (LERF) PRA for internal events (excluding internal fire) at-power:

- Initiating Event Analysis (IE)
- Accident Sequence Analysis (AS)
- Success Criteria (SC)
- Systems Analysis (SY)
- Human Reliability Analysis (HR)
- Quantification (QU)
- LERF Analysis (LE)

A brief description of each of the ASME/ANS PRA Standard's technical elements and the data analysis relationship to them is provided in the table below, and details of the interactions are described in more depth in the relevant chapters throughout the document.

PRA data analysis involves the qualitative and quantitative analysis of equipment failures within the NPP context and considering the PRA success criteria for equipment function. The data analysis, therefore, needs the participation of personnel knowledgeable in plant practices relating to operations, maintenance, testing, system function, and those familiar with the plant-specific PRA modeling. PRA requires a multi-disciplinary team to conduct the accident sequence analysis, fault tree modeling, human reliability analysis (HRA), and PRA model quantification.

The data analyst should assist the systems analysts with the appropriate identification and characterization of component basic events and initiating events in the plant PRA model. Correspondingly, the systems analysts should provide the understanding of the context and nature of equipment failure to the data analysts so that the appropriate failure information can be collected and applied. Different PRA software has different format requirements for data input; therefore, the data analyst also needs to be aware of the coding and input database format needs so that the software will properly process and apply the data inputs for PRA model quantification.

2.3 PRA Data Analysis Process

Figure 2-1 provides an overview of the elements of data analysis. Analysis of the various data types used to support PRA follows the same general process depicted in Figure 2-1. This section provides an overview of each step of the data analysis process, and presents key definitions and concepts that are applicable to data analysis, regardless of data type. Subsequent chapters provide detailed guidance on each of these steps, specific to the data type being analyzed. Section 3 provides detailed guidance on one specific data analysis method – Bayesian Updating – that can be used to support step 3.

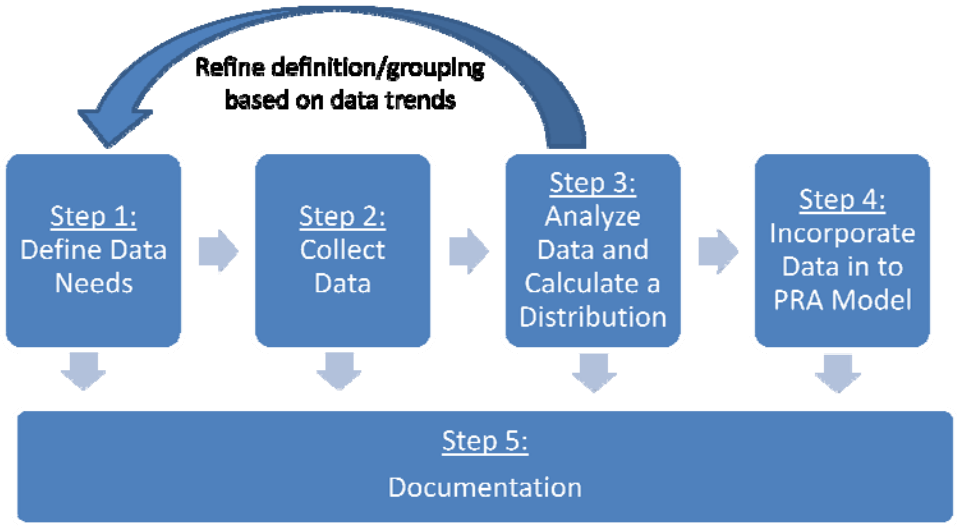

Figure 2-1
PRA data analysis process

Table 2-1
DA interface with other PRA elements

Element	Description	Output to DA	Input from DA
IE	Initiating Event Analysis identifies and quantifies events that challenge normal plant operation and require successful mitigation to prevent core damage.	• Collection and organization of plant-specific information. • List of grouped initiating events that need to be quantified.	• Frequencies from plant-specific and generic sources to quantify these initiating event groups. • Qualitative insights from generic data and precursors to initiators.
AS	Accident Sequence Analysis models the appropriate combinations of system responses and operator actions that affect the key safety functions for each modeled initiating event.	• System alignments related to initiators from plant-specific experience or preferences. • Plant configurations and maintenance practices for dependencies.	• Qualitative insights from plant-specific experience collected and reviewed by the data analysis can inform the system response development.
SC	Success Criteria defines the plant-specific measures of success and failure that support the other technical elements of the PRA.	• Success criteria dictates definition of system/component performance requirements used in DA to determine when to count a failure.	N/A
SY	Systems Analysis is the evaluation of the causes of system failure and unavailability modes represented in the initiating events analysis and sequence definition.	• System logic and context.	• Basic event data (failure rates, probabilities, unavailabilities, CCF data). • Repair times and dependencies. • Environmental conditions impacting reliability.
		Component definitions, including boundaries and basic event naming scheme, are developed jointly with coding to reflect the component types, failure modes, and categories of failure and unavailability.	
HR	Human Reliability Analysis ensures that the impacts of plant personnel actions are reflected in the assessment of risk.	• Test and maintenance unavailability captured by latent Human Failure Events.	• Unavailability failure modes based on plant-specific experience.

Table 2-1 (continued)
DA interface with other PRA elements

Element	Description	Output to DA	Input from DA
QU	Quantification provides an estimate of core damage frequency (CDF) (and supports the quantification of LERF) based upon the plant-specific core damage scenarios.	N/A	• Failure rate and frequencies • Uncertainty intervals related to parameters • Sources of uncertainty as input into sensitivity analysis selection
LE	LERF Analysis identifies and quantifies the contributors to large early releases, based upon plant-specific core damage scenarios.	• Component list to be quantified to support LERF analysis	• Justification for credit for repair • Input to interfacing system failure probability

2.3.1 Data Types Covered in Guidelines

These guidelines cover the typical data needs of a PRA for model quantification. The types of data covered in this report include: initiating event data, component reliability data, unavailability data and common-cause failure data.

2.3.1.1 Initiating Event Data

An initiating event is an event that perturbs the steady state operation of the plant by challenging plant control and safety systems whose failure could potentially lead to core damage or release of airborne fission products [9]. Initiating events include human-caused disruptions and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds) [1].

Initiating events define the scope for the remainder of the PRA model development since different initiating events result in different challenges to the plant control and safety systems. For the at-power mode of operation, an initiating event results in a demand for a plant trip (automatic or manual) [9]. The preferred measure for initiating events is annual frequency.

2.3.1.2 Component Reliability Data

Component failures are identified by the PRA systems analysis task as basic events in the PRA model. Component types that are typically modeled are pumps, valves, diesel generators, and instrumentation. These types are further identified by driver or parameter measured, such as motor-operated valve, turbine-driven pump or pressure indicator. Failure modes are also identified in the basic events, such as failure to run, failure to open on demand or spurious operation. The preferred measure for component reliability data is number of failures out of the number of exposure hours or the number of demands (challenges) to function.

2.3.1.3 Unavailability Data

Component unavailability is also defined by the PRA systems analysis task with PRA model basic events. Unavailability accounts for the time that equipment is out-of-service for scheduled test and maintenance and cannot perform its function if needed during an accident sequence. The preferred measure for component unavailability data is the out-of-service time out of the total system operational time.

2.3.1.4 Common Cause Failure Data

Common cause failures are events in the PRA model where the same cause degrades the function of two or more components that are relied upon for redundant operations, either at the same time or within a short time relative to the overall component mission time. Because CCFs are relatively uncommon, they are addressed with special modeling techniques based on industry-wide data collection.

2.3.2 Data Definition

Each parameter to be estimated must be clearly defined to ensure the data pool contains information that is internally consistent and to provide a point of common understanding between the systems analyst and the data analyst to ensure the data calculated applies properly to the events modeled in the PRA. Furthermore, plants can have literally thousands of specific initiating events and component types, so to make data analysis a manageable task, initiating events and components are often grouped based on common characteristics, and initiating event frequencies or failure and unavailability rates are provided for a given group.

The ASME/ANS PRA Standard requirements regarding parameter definition and grouping are HLR-DA-A and –B and their supporting requirements.

The characteristics that are relevant for defining and binning initiating events are different than those for components. Section 4.3 provides guidance on initiating event grouping. Section 5.2.2 provides guidance on grouping and assigning type codes to components.

2.3.3 Data Collection

There are generally three sources that can be used in data analysis: generic data, plant-specific data and other (for example, expert elicitation). Care should be taken that the data collected in support of parameter estimates are consistent with the parameter definitions and grouping rationale (see ASME/ANS PRA Standard requirement HLR-DA-C and supporting requirements).

Generic data sources provide initiator frequency and component failure rate information obtained from industry-wide experience, and can include data collected across NPPs or data from non-NPPs that has been determined to be applicable to NPP operations. Section 2.5 provides some common sources of generic data that are used in PRA. The initiating event definitions and the component boundaries, types and failure modes in the generic data sources should be reviewed for compatibility with the definitions used by the PRA team. If there are inconsistencies, they should be discussed with the system analysis lead early on in the PRA or update project to align definitions with the generic data sources. Use of generic data source information for initiating events is discussed further in Section 4.3.2.1 and for component failure rates in Section 5.3.1. Component unavailability is only calculated using plant-specific sources. Common cause failure data uses generic factors to assess different combinations of failures.

Depending on the availability of the data, plant-specific data can be used in lieu of generic data, or it can be used to supplement generic data (that is, via Bayesian Updating, see Section 3). Generally, to meet Capability Category II of the ASME/ANS PRA Standard, plant-specific data should be used in data analysis for risk-significant basic events, as available. Plant-specific data comes from a variety of sources, and often one source can provide input to multiple calculations. Therefore, structuring the data collection process at the outset helps to eliminate duplications and omissions of the input information required to calculate the PRA data needs. The analyst should first identify the data needs to support the estimation of initiator frequencies, component failure rates and component unavailabilities. These are discussed in more detail for each data type in the following chapters.

For a new plant, the analyst would start with generic (industry-wide) data because there would not yet be any specific operating experience to use. But in most cases, the analyst will be updating an existing database for a plant that has operated for some time with plant-specific information.

In some cases, there is not sufficient data—generic or plant-specific—to calculate a failure rate or initiating event frequency. LOCA frequencies are one such example. In these cases, analytic methods based on first principles and/or expert elicitation may be used to develop a failure rate or initiating event frequency distribution. Guidance for this sort of analysis is not covered in this report; however, Bayesian analysis—described in detail in Section 3—can be used to incorporate data if data becomes available.

2.3.4 Data Analysis and Uncertainty

Once the relevant data is gathered, the data can be analyzed and a distribution can be calculated. The ASME/ANS PRA Standard requirement relevant to this step of data analysis is HLR-DA-D and its supporting requirements. In this context, analysis entails combining various data sources (for example, generic and plant-specific) to obtain a mean estimate, characterizing the uncertainty through development of a distribution and reviewing the output to ensure its applicability.

2.3.4.1 Need to Evaluate Uncertainties

Ultimately, the point of the PRA is to understand the risk contributors to plant operations. Uncertainties – both qualitative and quantitative – are evaluated to provide the most robust information available to support decision making. Key references for understanding uncertainty in the context of PRA and risk informed decision making, including application of the State of Knowledge Correlation (SOKC), are NUREG-1855 [10] and its companion documents EPRI 1016737 [11] and EPRI 1026511 [12].

While there are many sources of uncertainty in a PRA (model uncertainty, parameter uncertainty, and so on), the data analysis task is only concerned with uncertainty in parameter estimation. Uncertainties arise in the applicability of data to represent the parameter of interest, in assumptions made in performing the analysis, or in the precision with which the data was collected. In order to best represent the state of knowledge regarding a failure rate or probability, the output of the data analysis is a distribution which conveys the certainty of the information. The point estimates assigned to the model basic events are mean values of the corresponding probability distributions. Other values drawn from the distribution (for example, the 95th percentile value) may be used in sensitivity studies to identify key sources of uncertainty.

Footnote 13 on page 38 of RG 1.200 defines a “key source of uncertainty” as:

> [an uncertainty] that is related to an issue in which there is no consensus approach or model and where the choice of approach or model is known to have an impact on the risk profile (for example, total CDF and total LERF, the set of initiating events and accident sequences that contribute most to CDF and to LERF) such that it influences a decision being made using the PRA. Such an impact might occur, for example, by introducing a new functional accident sequence or a change to the overall CDF or LERF estimates significant enough to affect insights gained from the PRA [8].

In addition, the following SR from another area of the ASME/ANS PRA Standard [7] applies to, and interfaces with, the uncertainty analysis task:

> HLR-QU-E – Uncertainties in the PRA results shall be characterized. Sources of model uncertainty and related assumptions shall be identified, and their potential impact on the results understood.

2.3.4.2 Qualitative Uncertainty

Analysts identify the sources of parametric uncertainty from a qualitative standpoint to provide awareness of potential quantitative effects. For example:

- Initiating event frequencies can be based on conservative generic data. Performing Bayesian updating helps remove conservatism found in the industry data and provides a more accurate estimation.
- As with any data collection effort, uncertainties arise in evaluating and categorizing the data, whether generic data only are used or if it is updated with plant-specific data. This uncertainty is minimized wherever practicable, such as through engineering judgment by experienced analysts to interpret and develop available data.
- Component boundary and other decisions can impact uncertainty, such as: Control circuit power supply, signal isolators, comparators, and current/voltage input modules fail in a direction that prevents a signal, thereby disabling the channel. Failure of these components is non-detectable between testing intervals and failure data are difficult to obtain, therefore worst case failure modes are generally assumed.
- Staggered testing assumes all of the CCF candidates will be discovered during the test. This assumption is evaluated and applied carefully since the component testing interval has significant bearing on the quantification.

Uncertainty in data can be qualitatively reduced by actively involving plant operating personnel in the study and establishing a comprehensive method for managing and checking input data.

2.3.4.3 Quantitative Uncertainty: Bayesian vs. Frequentist Approach

The ASME/ANS PRA Standard [7] SR DA-D3 identifies three acceptable methods for quantitatively characterizing the uncertainty of basic event parameters (for Capability Categories II and III): 1) the frequentist method, 2) Bayesian updating, and 3) expert judgment.

In a frequentist or classical statistical approach, the failure statistics for the PRA are calculated using, for example, a numerator of the number of observed failures and a denominator of the number of operating hours. If there were multiple data sources, the numerators would be added together and the denominators would be added together and the ratio of the cumulative numerator over the cumulative denominator would provide the mean value. Using this method, the various data sources are equally weighted. However, data from reliable equipment are typically sparse, experiencing few or even zero observed failures, so classical (frequentist) statistical methods can result in wide uncertainty (or confidence) intervals.

The frequentist approach converts raw data into a distribution by calculating the point estimate, usually the maximum likelihood estimate (MLE) and then calculating confidence intervals and fitting them to an assumed distribution. This report does not provide further guidance on the frequentist approach. However, NUREG/CR-6823 [13] Sections 6.2.1 and 6.3.1 provide guidance on frequentist or classical estimation techniques for failure rates (failure over time) and failure probabilities (failure per demand), respectively.

The Bayesian analysis method uses Bayes theorem to statistically combine data sets. Unlike the frequentist approach, the Bayesian framework does not necessarily equally weight all the data sources, but can account for varied degree of confidence in different data sources. In the Bayesian framework, probability distributions are used to quantify an analyst's degree of belief about the value of an unknown parameter, whether it is the annual frequency of a given initiating event, or the failure rate of a particular type of component. In this approach, a distribution is used to describe the occurrence of an event (for example, probability of the initiating event occurring over a period of time, or of failure events for the type of component under consideration). This distribution, called a "prior" represents the degree of belief around that parameter value. As empirical data are gathered, this prior distribution is updated mathematically to produce a "posterior" probability distribution that combines the information from the prior distribution with that gathered from the experiential data.

One of the principal reasons why Bayesian methods have been adopted is their capability to integrate information from various sources into a coherent statistical framework. Bayesian methods also make extensive use of probability distributions to express uncertainty around parameters. This allows individual component uncertainties to be propagated in order to calculate the overall uncertainty distribution for a system made up of multiple components.

Section 3 provides detailed guidance on the use of Bayesian Analysis; the methods presented in this chapter are independent of the type of data being analyzed (for example, initiating events versus component failure rates).

Expert judgment can be used when there is little or no data to support calculation of a distribution (that is, rare events). When sparse data is available, expert judgment can be used as an input into the Bayesian analysis or, if no data is available, it can be used as-is. Detailed guidance on performing expert elicitation is out of the scope of this document. However, there are other references [14, 15, 16] which provide guidance on performing expert elicitation, including calibration of experts and controlling for bias.

Regardless of what method was used to characterize the uncertainty, uncertainty is mathematically expressed and input into the PRA in the form of a distribution. PRA data parameter uncertainty bounds are traditionally expressed in terms of the 90% confidence interval with a lower limit of the 5^{th} percentile value and an upper limit of the 95^{th} percentile value, as shown in Figure 2-3. The uncertainty ranges characterized by the distribution vary in origin. For example, if the estimates are based on plant-specific data, the range is characteristic of statistical uncertainty. If the estimates are generic (or non-plant-specific) the range is characteristic of the factors that may affect the failure properties of the component in different uses and

environments. Therefore, the range will include plant-to-plant variation. The type of distribution used (for example, Lognormal, Beta, Gamma, and so on) and associated parameters dictate the shape and values of the distribution. The next section provides a description of commonly used distributions in PRA data analysis and when they are most applicable.

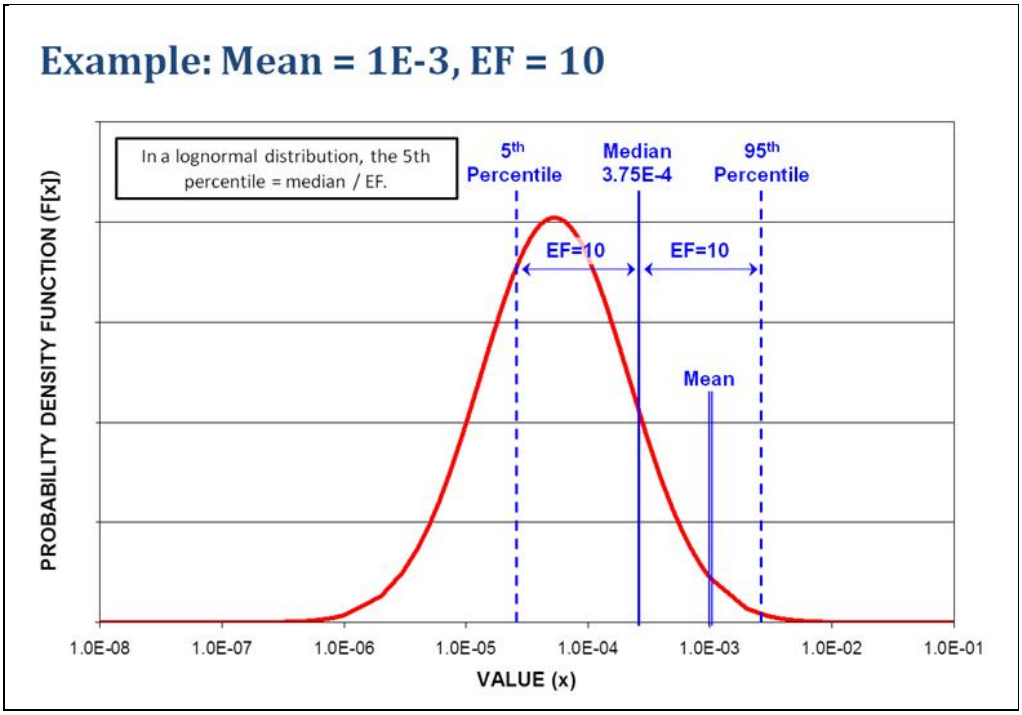

Figure 2-2
Typical PRA uncertainty parameters

2.3.4.4 Commonly Used Distributions

In this guideline, there are five commonly referenced distributions. These are described here, with formulas, and referenced throughout the rest of the document. These are not the only distributions that can be used in PRA, but are among the most common: Poisson, Binomial, Lognormal, Gamma, and Beta.

Poisson

The Poisson distribution is a discrete distribution (that is, the value of the variate is permitted to take only discrete values) that is appropriate for representing the distribution of number of occurrences of events that occur over a continuous interval (for example, number of events over a period of time). Poisson distributions are commonly used to model initiating event frequencies and component failure rates (for example, failure to run). The assumptions behind a Poisson distribution include [17]:

- An event can occur at random and at any time.
- The occurrence of an event is independent of other events in that interval.
- The mean rate of occurrence of the event is assumed to be constant (constant failure rate over period of interest).
- The probability of two or more occurrences in Δt is negligible.

The probability of X number of occurrences of an event in time, *t* is given by:

$$\boldsymbol{P(X = x) = \frac{(\lambda t)^x}{x!} e^{-\lambda t}} \quad \textbf{Eq. 2-1}$$

where λ is the mean failure rate and *t* is the time interval.

The mean and variance of X are:

$$\boldsymbol{E(X) = \lambda t} \quad \textbf{Eq. 2-2}$$

$$\boldsymbol{var(X) = \lambda t} \quad \textbf{Eq. 2-3}$$

Binomal

The Binomial distribution is a discrete distribution (that is, the value of the variate is permitted to take only discrete values) that is appropriate for representing the distribution of number of occurrences of events that occur over number of discrete trial (for example, number of failures versus demands). Binomial distributions are commonly used to model component failure rates (for example, failure to start or failure on demand). The binomial distribution can be used if the process follows the assumptions associated with a Bernoulli sequence [17]:

- Each demand only has two possible outcomes (for example, failed or not-failed)
- The probability of occurrence of the event in each trial is constant
- The trials are independent

The probability of X number of occurrences of an event in *n* demands is given by:

$$\boldsymbol{P(X = x) = \binom{n}{x} p^x (1 - p)^{n-x}} \quad \textbf{Eq. 2-4}$$

where *x* is the number of failures, *p* is the probability of failure and *n* is the number of demands and:

$$\binom{n}{x} = \frac{n!}{x!(n-x)!}.$$

Lognormal

The lognormal distribution is a continuous distribution (that is, the variate can take on values over a continuous range) used to express the uncertainty in many PRA data parameters such as failure rates, initiating event frequencies and basic event probabilities. Lognormal was the distribution of choice in the original PRA study WASH-1400 [18], and historically has been used since. This distribution type was chosen because the values are always positive and, due to its logarithmic nature, it is a "'natural' distribution for describing data which can vary by factors in same way that a normal distribution is 'natural' when the data can vary by additive or subtractive increments". In addition, "the lognormal distribution form, in particular its positive skewness, can incorporate general reliability-associated behaviors of the assessed data (the positive skewness accounts for the occurrence of less likely but large deviations, such as abnormally high failure rates due to batch defects, environmental degradation, and other outlier causing effects) [18]." Because of its relationship to the normal distribution, the lognormal distribution is mathematically convenient to and obtain key parameters (for example, 5th and 95th percentiles).

A random variable X is said to have the *lognormal distribution* with parameters μ and σ if ln(X) has the normal distribution with mean μ and standard deviation σ. The probability density function of the log-normal distribution is:

$$\boldsymbol{f(x)} = \frac{\mathbf{1}}{\boldsymbol{\sigma x\sqrt{2\pi}}} \boldsymbol{e}^{-\frac{[\ln(x)-\mu]^2}{2\sigma^2}} \text{ , } x \in (0,\infty) \qquad \textbf{Eq. 2-5}$$

The cumulative distribution function is given by:

$$\boldsymbol{F(x)} = \boldsymbol{\Phi}[\frac{\ln(x)-\mu}{\sigma}] \text{ , } x \in (0,\infty) \qquad \textbf{Eq. 2-6}$$

The mean and variance of X are:

$$\boldsymbol{E(X)} = \boldsymbol{e}^{(\mu+\frac{1}{2}\sigma^2)} \qquad \textbf{Eq. 2-7}$$

$$\boldsymbol{var(X)} = \boldsymbol{e}^{2(\mu+\sigma^2)} - \boldsymbol{e}^{(2\mu+\sigma^2)} \qquad \textbf{Eq. 2-8}$$

The 5th, 95th and Median can are related to the error factor (EF) in the following manner:

$$\boldsymbol{EF} = \frac{\boldsymbol{x_{50}}}{\boldsymbol{x_5}} = \frac{\boldsymbol{x_{95}}}{\boldsymbol{x_{50}}} \qquad \textbf{Eq. 2-9}$$

where x_{50} is the median, x_{550} is the 5th percentile and x_{95} is the 95th percentile value. See Figure 2-3 for an illustration.

Gamma

The gamma distribution is also useful distribution to model failure rates (for example, distribution of component reliability failure to run rates or initiating event frequencies). Like the lognormal, the random variable ranges from 0 to ∞, can span several orders of magnitude and exhibits the same positive skewness. The gamma distribution is also mathematically very convenient to use in Bayesian updating.

The gamma probability distribution function used for calculation of the failure rate λ (units of events/time expressed as hours) is the following [13]:

$$f(\lambda) = \frac{(\beta)^{\alpha}}{\Gamma(\alpha)} \lambda^{\alpha-1} \exp(-\lambda\beta) \qquad \textbf{Eq. 2-10}$$

where λ, α, and $\beta > 0$. Alpha (α) is known as the shape parameter (dimensionless) and β is the scale parameter (whose dimension is a unit of time, that is, year for an initiating event, and hour for an equipment failure rate). $\Gamma(\alpha)$ is defined as:

$$\Gamma(\alpha) = \int_0^{\infty} x^{\alpha-1} e^{-x} dx. \qquad \textbf{Eq. 2-11}$$

where the gamma function evaluated at α, and if α is a positive integer, Γ(α) = (α - l).

The mean of this distribution is

$$\lambda_{mean} = \frac{\alpha}{\beta} \quad \textbf{Eq. 2-12}$$

and the variance is

$$\lambda_{variance} = \frac{\alpha}{\beta^2} \quad \textbf{Eq. 2-13}$$

NOTE: Microsoft Excel and other applications define β as the inverse of the β used here.

Calculating the 5th, 95th and Median:

Unlike the lognormal, there is no simple formula to calculate the 5th, 95th and median values of a Gamma distribution, however, it can be done numerically in MS EXCEL 2007 using "GAMMAINV(probability, α, β)," where "probability" was the percentile of interest.

Beta

The beta distribution is a useful distribution to model failure probabilities upon demand types of inputs (for example, distribution of a failure probability for component failure to start, failure to open/close, and so on). It is suitable to this type of modeling particularly because the distribution is constrained between two values (in the formulation below, p is constrained to $0 \le p \le 1$). The beta distribution function for probability upon demand p is the following [13]:

$$f(p) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad \textbf{Eq. 2-14}$$

for $0 \le p \le 1$ and α and $\beta > 0$, where α denotes the number of failures and β indicates the number of demands experienced by the component during the data window. $\Gamma(\alpha)$ is defined as:

$$\Gamma(\alpha) = \int_0^\infty x^{\alpha-1} e^{-x} dx. \quad \textbf{Eq. 2-15}$$

The beta distribution is denoted beta (α, β). The mean of this distribution is

$$P_{mean} = \frac{\alpha}{\alpha+\beta} \quad \textbf{Eq. 2-16}$$

and the variance is

$$P_{variance} = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \quad \textbf{Eq. 2-17}$$

Calculating the 5th, 95th and Median:

Unlike the lognormal, there is no simple formula to calculate the 5th, 95th and median values of a Beta distribution, however, it can be done numerically in MS EXCEL 2007 using "BETAINV(probability, α, β)," where "probability" was the percentile of interest.

2.3.4.5 Data Analysis and Iteration

Data analysts should be aware of trends that are demonstrated in the data. ASME/ANS PRA Standard Supporting Requirement DA-B2 states that outliers should NOT be included in component groups (such as valves that are never tested and unlikely to be operated with those that are tested or otherwise manipulated frequently). It is common when analyzing data to note that certain components of a similar type fail more frequently than others or that the operating time for certain equipment is significantly different than others in the same system or of the same type. Similarly, when combining generic data with plant-specific data, the analyst may find a large discrepancy between the two, suggesting that the generic data may not be a suitable representation of that plant (for example, due to design, maintenance or other differences). If the data demonstrates that outliers exist, or there are large discrepancies between data sources being combined, the data sources used or grouping definitions may need to be revised. Section 3.6 provides guidance on determining the suitability of combining data from various sources.

2.3.5 Incorporating Data into the PRA Model

The Data Analyst needs to support the System Analysts and PRA Quantification analyst by (a) providing the data types identified below in the format consistent with the PRA model quantification software and (b) by notifying these analysts as soon as possible if there are changes to the values in the database because this will impact quantification and PRA model results. Correspondingly, if new information is added to the PRA model that requires data, that data need should be communicated to the Data Analyst as soon as possible since effort is required to develop the data and this could cause a schedule impact. Where and at what level the data is incorporated into the PRA model is specific to the data type, and discussed in more detail in the relevant chapters.

2.3.6 Documentation

A data analysis report for the PRA supporting documentation should describe all tasks of the analysis in sufficient detail to permit the reader to understand which parameters were developed, what data sources were used, what analytical methods were employed, and how the data pathway flows from initial data source to the table of results input to the PRA models. For example, for component failure data, this would mean that any Maintenance Work Orders (MWOs) that were used as input to failure rates are cited by MWO number and associated with the component type and failure mode to which they were attributed.

Interim or draft reports should be reviewed by those responsible for ensuring technical quality as part of the overall PRA QA program, focusing on the emphasis placed on the results, on the interpretation of the results, and on verifying that the document is comprehensible and usable. To achieve the latter, it is necessary to ensure that all assumptions are clearly stated, data sources are given, and the results presented are reproducible.

The documentation and supporting calculations should be retained for future use and as a resource when questions arise.

Chapter 8 of these Guidelines provides further information on proper documentation for a PRA data analysis. The relevant ASME/ANS PRA Standard requirement for documentation of the data analysis is HLR-DA-E and its supporting requirements.

2.4 Risk Monitor vs. PRA

PRA is "a qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public [7]."

A PRA is typically used to report the *average* condition of the plant, but can also be used as part of a risk monitor. A Risk Monitor (for example, EOOS) is "a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components [19]." Risk Monitors are used to generate risk information for use in the day-to-day management of plant operational safety and to provide input to maintenance planning. They provide information on the components that should be returned to service before particular maintenance activities are carried out and which of the remaining operational components are the most important to plant safety during scheduled maintenance outages. Risk monitors can also provide a basis for changes in a plant's licensing basis; for example, for performing more online maintenance without increasing the overall risk [20].

The following comparison table (Table 2-2) is based on information from Reference [20].

Table 2-2
Comparison between risk monitor and PRA features and usage

Risk Monitor	PRA
Used on-line	Used off-line
Provides estimate of point-in-time risk	Provides estimate of average risk over all plant operational states and configurations
Reflects current plant configuration	Averages over all plant configurations
Can be used by all plant staff in support of operational decisions, and utility and regulatory staff who have access	Used by PRA specialists

Despite the differences in usage, the Risk Monitor and PRA are consistent with each other because the safety system success criteria and much of the data used are the same. So when the PRA is updated, the Risk Monitor should also be updated. However, there are some cases where the input data to the risk monitor might differ than that from the PRA. These cases are highlighted in the subsequent guidance.

2.5 Data References and Sources

Table 2-3 provides a common set of published and website posted references for PRA data, separated into those that are primary sources for nuclear industry PRA and those that are alternative or supplementary sources for components not included in the primary data sources or for applications other than the nuclear power industry.

Table 2-3
Common generic data sources

Data Source Reference	Years of Applicability	Continuously Updated?	Description
Primary Nuclear Industry Data Sources			
U.S. NRC operational experience website [21]	FY1988-2012	Yes	Generic BWR and PWR data based on operating experience. Data categories include: • Initiating Event Frequencies • Loss of Offsite Power (LOOP) data • Component Failure Data • Common Cause Failure Parameters
NUREG/CR-6928 [4]	Baseline periods with start years of 1988 to 1998, but all ending in 2002	No, revision to this NUREG is not expected. Updated information is provided on the NRC operational experience website.	Generic BWR and PWR initiator frequency data based upon nuclear plant experience.
EPRI 3002000079 [22]	1970 through 2009	No (updated regularly, but not continuously).	Piping system failure rates (for example, for internal flooding).
NUREG/CR-6890 [5]	1986-2004	No, but updated information available on NRC website.	LOOP data.
EPRI reports: LOOPs at US Nuclear Power Plants [23-34]	1980-2012	Yes (new report issued periodically).	LOOP data.
Alternative Data Sources (Used for Equipment in PRA Model not Included in Primary Sources)			
NUREG/CR-4639 [35]	Prior to 1994	No.	NUCLARR; compendium of component reliability data from older sources.
IEEE Std. 493 [36]	Prior to 1997	Reviewed for update or reaffirmation every 5 years.	“Gold Book”; power generating component reliability data.

Table 2-3 (continued)
Common generic data sources

Data Source Reference	Years of Applicability	Continuously Updated?	Description
Alternative Data Sources (Used for Equipment in PRA Model not Included in Primary Sources)			
T.R. Moss, The Reliability Data Handbook [37]	Not specified	No.	Appendix with tables of component reliability data.
NPRD-95 [38]	Prior to 1994	No.	Component reliability data from military experience for devices used beyond nuclear applications.
MIL-HDBK-217F [39]	Prior to 1991	No, but occasional updates are issued.	Electronic component reliability data from military applications.
OREDA [40]	1993 - 2000	No, but occasional updates are issued.	Offshore oil/gas platform component reliability data.

3
BAYESIAN UPDATING

3.1 Introduction

Data from reliable equipment are typically sparse, experiencing few or even zero observed failures. Because of this, it is considered to be appropriate to draw upon other sources of information to provide a reasonable and defensible data set.

The principal reasons why Bayesian methods have been adopted are that they provide:

- A consistent way to incorporate generic/industry data and plant specific evidence in parametric uncertainty distributions
- Weights to generic data and plant specific evidence to account for the statistical significance of the data
- A means to support parameter estimates when plant specific data is limited
- A consistent way to treat zero failures

For these reasons, Bayesian approaches for the evaluation of initiating event frequency and component reliability have been used in the nuclear industry for several decades. For example, as stated in the PRA Procedures Guide (NUREG/CR-2300 [1]):

> The main benefit in using the Bayesian approach to data reduction is that it provides a formal way of explicitly organizing and introducing into the analysis assumptions about prior knowledge. This knowledge may be based on past generic industry-wide data and experience, engineering judgment, expert opinion, and so forth, with varying degrees of subjectivity. The parameter estimates will then reflect this knowledge. A noteworthy feature of the nuclear industry is that such prior information is often available to the extent that it may contribute more to the knowledge about the parameter than does the more directly applicable (but sparse) plant specific information.

This chapter begins by introducing the key elements of the Bayesian updating approach: the prior, likelihood and posterior distributions and then discusses each of these elements further. Examples are then provided for performing Bayesian updating considering the input data and the use of conventional PRA modeling software.

3.2 Overview

Uncertainty characterization is an integral part of parameter estimation, and analyst can use Bayesian updating to incorporate data from various sources and of varying certainty to form a probability distribution which reflects the analyst's state of knowledge regarding the value a given parameter. Bayesian updating uses quantitative data, to update a distribution based on the calculated likelihood of the observed evidence. The generic process of Bayesian updating is

discussed here; for PRA applications, the specific parameter being updated could be the annual frequency of a given initiating event (as discussed in Section 4) or the failure rate for component type and failure mode (as discussed in Section 5). There are three elements to the Bayesian process:

- Prior distribution
- Likelihood distribution
- Posterior distribution

Prior – The prior distribution captures the state-of-knowledge prior to receiving evidence. This distribution can be based on generic industry data for a component or event, or can be based on expert opinion. Alternatively, if no information is known about the system, a non-informative prior can be used. The prior distribution can be expressed as a discrete or continuous probability distribution. Selection and calculation of a prior distribution is discussed in Section 3.3.

Likelihood – The likelihood is a probability distribution that expresses the probability of the observed empirical data (evidence). The likelihood distribution is usually derived from plant-specific data, such as the plant-specific component numerator (number of failures) and denominator (hours or demands) information. Calculation of a likelihood distribution is discussed in Section 3.4.

Posterior – The posterior probability distribution is the output result from "updating" the prior distribution with the likelihood information. It is the data that is developed in a statistically precise way to combine the richness of generic industry experience with the specific data from the operating experience of the plant that is the subject of the PRA. The posterior data distribution is the information used in the PRA model quantification, such as for a component basic event in a PRA fault tree. Calculation of a posterior distribution is discussed in Section 3.5, and Section 3.7 discusses incorporation of the posterior distribution into the PRA.

Model Validation – A crucial part of the Bayesian update process is to check the input and the resulting posterior distribution for "reasonableness." For example, discrepancies may arise when the prior distribution is inadequate to accommodate the evidence (for example, the prior distribution is too narrow). Similarly, if the posterior distribution differs greatly from the prior distribution that may indicate that the prior distribution is not appropriate or the data may contain outliers that should be disregarded. Section 3.6 provides guidance on this step.

The general process for Bayesian updating is summarized in Figure 3-1. Note that the process of Bayesian updating involves a fair amount of engineering **judgment** and may require some iteration before a final distribution is attained; this is discussed further in the following sections. This chapter does not intended to provide step-by-step guidance on how to perform Bayesian updating or provide information on all possible distribution types that can be used, but rather to provide context for the methods discussed in NUREG/CR-6823 [13] and guidance on avoiding common pitfalls seen in industry use of Bayesian updating. As such, the analyst should refer to NUREG/CR-6823 [13] for more detailed background information on Bayesian analysis for PRA. Sections 4 and 5 of this report provide guidance on appropriate data sources and application of Bayesian techniques to inform initiating event and component reliability calculations.

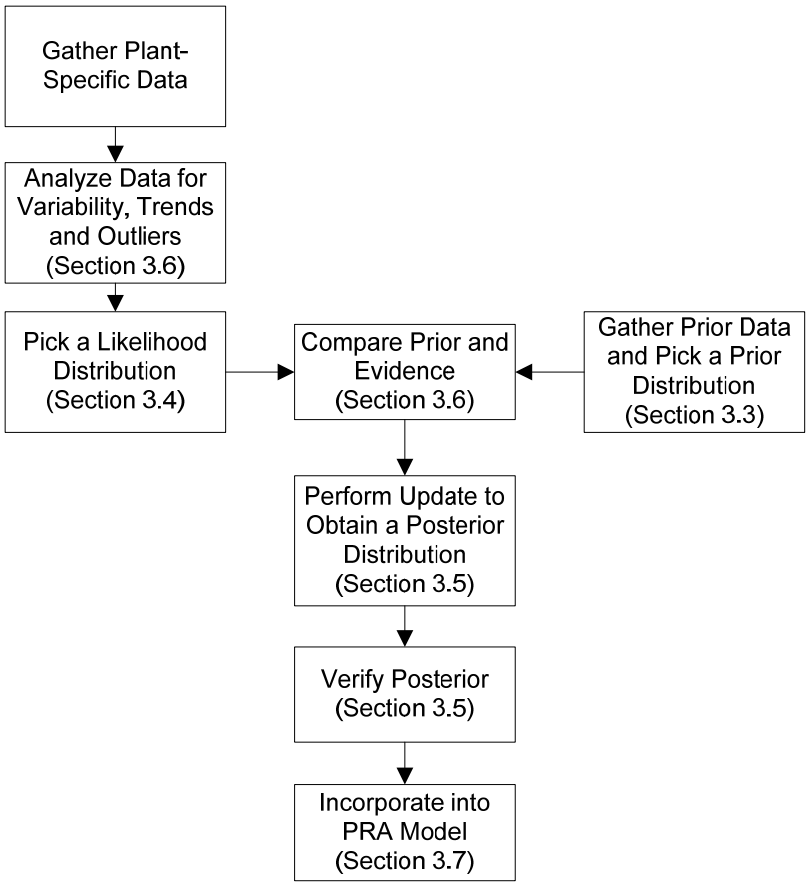

Figure 3-1
Bayesian update process summary

3.3 Prior Distribution

Due to the general reliability of equipment and the low frequency of most initiating events, it is unlikely that there will be sufficient plant-specific (likelihood) data to substantiate a justifiable estimate, as required by the ASME/ANS PRA Standard. For this reason, it is recognized that a wider base of information is needed to properly estimate the parameters needed for the PRA. Generic, or industry generated, data is therefore used to supplement or replace the plant-specific information, or provide a basis for comparison. ASME/ANS PRA Standard Requirement DA-E2 [7] says, for all capability categories, that the data analyst must document "the rationale for any distributions used as priors for Bayesian updates." This suggests that priors should be selected carefully and with consideration for the PRA model use to which they will be applied and the plant-specific information with which they will be combined.

Additional guidance on selecting initiating event and component reliability generic data for use as priors is provided in the chapter 4 and 5 subsections on Generic Data.

The prior distribution reflects the analyst's state of knowledge regarding the parameter of interest prior to receiving evidence. This section discusses several issues regarding the use of a prior distribution. Any kind of distribution can be used as a prior, however, a few specific types are discussed in this section. **Informative distributions** use information from potentially different sources of data, and can include generic data, expert judgment, or a combination of the two.

Non-informative distributions are broad generic distributions that convey no prior information and can be used when the analyst has no prior information regarding the parameter of interest or sufficient plant-specific data that it would drive the resulting distribution. **Constrained non-informative distributions** are a combination of informative and non-informative distributions – they incorporate prior information to inform the mean of the distribution, but retain the diffuse uncertainty associated with non-informative distributions. Constrained non-informative distributions are a good choice when the analyst is uncertain whether the prior data is fully applicable to the parameter of interest.

Conjugate distributions are pairs of prior/likelihood distributions that yield posterior distributions that are easy to calculate (closed form). These are most commonly used due to ease of analysis. **Non-conjugate distributions** are all other continuous distributions, and require numerical analysis to perform the Bayesian update and yield a posterior.

Typically, if there is generic data available from a published source, it is provided in the form of parameters of a conjugate (for example, Gamma or Beta) distribution or a non-conjugate distribution (for example, Lognormal). In some cases, however, the analyst may need to construct a prior distribution from raw data, or combine multiple sources of generic data. The conversion of raw data into a distribution can be done using Bayesian techniques (that is, 2-stage Bayes) or using classical techniques (that is, empirical Bayes) (see Section 5.1.1 and 5.1.2, respectively, of Siu and Kelly [41] or chapter 8 of NUREG/CR-6823 [13]). **Two-stage Bayes** typically starts with a non-informative distribution which is then updated using the raw generic data to create the distribution which will be used as a prior in plant-specific Bayesian Update. **Empirical Bayes** uses classical statistical methods (for example, moment matching methods or maximum likelihood method) to fit the raw data to a distribution which will be used as a prior in plant-specific Bayesian Update.

When using expert judgment to construct a prior distribution, the analyst should be aware of cognitive biases and conservatisms to ensure the distribution most realistically represents the available state of knowledge [41].

Table 3-1 provides a high level overview of the tradeoffs for each distribution type discussed below.

Table 3-1
Summary of prior distribution types

Category	Pros	Cons
Informative conjugate distributions	Bayesian updating using conjugate pairs is mathematically convenient and intuitive. *Gamma/Poisson* distributions are generally a good choice for failures in time (for example, initiating event failure frequency). *Beta/Binomial* distributions are generally a good choice for failure per demand (for example, component reliability) data. Generic data sources, such as those provided by the NRC, often express the data in the form of parameters for a Gamma or Beta distribution.	If the conjugate distribution is highly skewed (for example, gamma with $\alpha < 0.5$) and the evidence contains zero failures, Bayesian updating may yield unrealistic results. In these cases, an alternate (such as non-conjugate) prior distribution should be considered.
Informative non-conjugate distributions	Non-conjugate distributions should be used if the conjugate distributions are not a good fit for the data. Some older sources provide data in the form of parameters of a lognormal distribution; here the data can be converted to a conjugate distribution or evaluated numerically.	The update process is mathematically more complex and output is not closed form (and therefore may be less intuitive to check). However, many tools exist that can perform the numerical integration and PRA codes such as CAFTA can take some non-conjugate distributions (that is, lognormal) directly as input and perform the update.
Non-informative distributions	If there is no prior information that can be used, a non-informative distribution can be used. Non-informative Gamma and Beta distributions are available and can be used for mathematical convenience (called Jeffreys priors). This distribution type is useful when comparing data from multiple sources because the resulting distribution will not be unduly influenced by the prior.	Because there is no prior information, the output will have a broad distribution if the evidence is weak; not much different than what a frequentist method would yield. Not a good choice when evidence is sparse (for example, 0 failures in *n* trials where *n* is small); in these cases output can be sensitive to the specific form of the prior. For dominant risk contributors, an informative distribution is recommended even if information is only based on expert judgment of the bounds.
Constrained non-informative distributions	If the analyst is uncertain as to the completeness or applicability of the prior data, a constrained non-informative distribution can be used. Here the prior mean is based on the data, but has a diffuse uncertainty to indicate that the evidence is weak or uncertain.	Output will have a broad distribution if the evidence is weak.

3.3.1 Conjugate Prior Distributions

The Bayesian updating process can be very simple if the prior information and the likelihood information are expressed in terms that facilitate their combination.

If the prior and the posterior are in the same family, they are called conjugate distributions and the prior is called a conjugate prior for the likelihood. A conjugate prior is an algebraic convenience, giving a closed-form expression for the posterior; otherwise a difficult numerical integration may be necessary. In addition, conjugate priors show more clearly how the likelihood updates the distribution.

The conjugate distribution pairs that are most widely used in PRA applications and PRA software due to their ease of use are:

- Gamma-Poisson
- Beta-binomial

In applying Bayes' theorem, a prior distribution that follows a gamma distribution, updated with data whose likelihood is expressed via a Poisson distribution, yields a posterior distribution that is also a gamma. Similarly, a prior distribution that follows a beta distribution, updated with data whose likelihood is expressed via a binomial distribution, yields a posterior that is also a beta.

3.3.1.1 Gamma-Poisson

For a prior gamma distribution that has shape parameter α_0 (dimensionless) and scale parameter β_0 (whose dimension is a unit of time, that is, year for an initiating event, and hour for an equipment failure rate), the posterior distribution is gamma with shape parameter α_1 and scale parameter β_1 such that (Ref. [13], Section 6.2.2.4.2):

$$\alpha_1 = \alpha_0 + x \text{ and } \beta_1 = \beta_0 + T \qquad \textbf{Eq. 3-1 and Eq. 3-2}$$

where x is the number of failures recorded over the update period t (t should be in the same unit as β_0). The mean of the posterior distribution is equal to α_1/β_1. As is apparent from Equation 3-1, α_0 and β_0 of the prior gamma distribution can be respectively interpreted as a prior number of failures observed over a prior exposure time. The posterior parameters α_1 and β_1 update the prior parameters based on the failure data.

Section 2.3.4.4 provides the general form for Gamma and Poisson distributions. Depending on the prior information available, the parameters for the prior distribution (α_0, β_0) can be estimated using engineering judgment or expert elicitation, or constructed from generic data. However, these parameters are often already calculated and provided for the analyst in the generic data sources (for example, data updates on the NRC website [21]).

NOTE: Alternative definitions of the gamma distribution (such as those in the Microsoft Excel software) define β as the inverse of the β used in this report. The β used in this report is consistent with that defined in NUREG/CR-6928 [4].

NOTE: If the gamma distribution is highly skewed (for example, $\alpha < 0.5$) and the evidence contains zero failures, Bayesian updating may yield unrealistic results in the lower percentiles, and a non-conjugate prior should be considered.

Example:

Suppose we have the following plant-specific data that has been collected since the last PRA update was performed:

Circulating water pumps Fails to run (FTR) 1 failure out of 130000 hours

The plant-specific data constitutes the likelihood information in Poisson form for the FTR.

To perform the update, the following data would be selected from NUREG/CR-6928 [4], Table A.2.27-6 for the prior:

FTR $\alpha = 1.655$; $\beta = 3.649E+05$ (parameters of Gamma distribution)

For the fails to run data, the update using the Gamma distribution would yield a posterior mean of:

$$\text{Posterior mean} = \frac{(\alpha_0 + x)}{(\beta_0 + T)} \qquad \textbf{Eq. 3-3}$$

where α_0 and β_0 are the alpha and beta of the generic data and x and T are the number of failures and number of hours that the pump was running within the data window, respectively, from the plant-specific data.

For our specific example, the posterior distribution parameters would be:

$\alpha_1 = (1.655 + 1) = 2.655$

$\beta_1 = (364900 + 130000) = 494900$

yielding a posterior mean value of 5.36E-06 failures per hour. Figure 3-2 shows the prior versus posterior distributions (PDF) for this update.

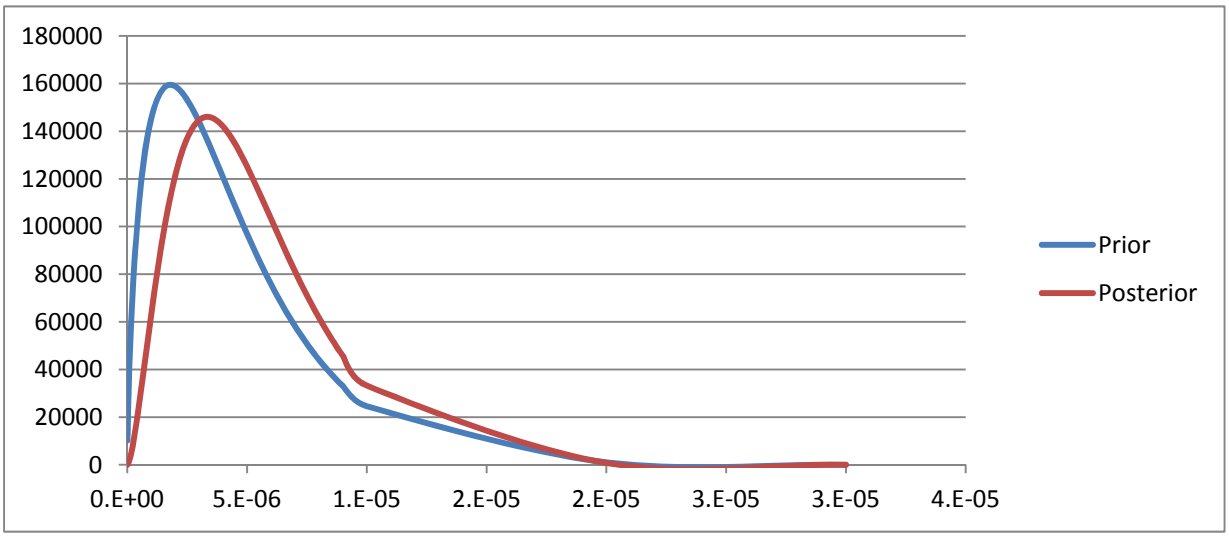

Figure 3-2
Example Bayesian update using Gamma-Poisson: failure to run for circulating water pumps

NOTE: It is possible for the generic data and the plant-specific data to overlap (for example, overlap in data window and database contents such that the generic data includes some or all of the plant-specific data). Double counting can result in a potentially non-conservative reduction in the uncertainty. This double counting is usually negligible for most cases of interest. The exception is when the generic data is sparse and/or is dominated by data from the plant in question.

3.3.1.2 Beta-Binomial

The Beta-Binomial conjugate pair is used when calculating failure probabilities (as opposed to failure *rates*), or number of failure per demand. For a prior beta distribution that has parameters α_0 and β_0 (both dimensionless), the posterior beta distribution is beta with parameters α_1 and β_1 such that (Ref. [13], Section 6.3.2.2.2):

$$\alpha_1 = \alpha_0 + x \text{ and } \beta_1 = \beta_0 + (n - x) \qquad \text{Eq. 3-4}$$

where x is the number of failures recorded over n demands. The mean of the posterior distribution is $\alpha_1/(\alpha_1 + \beta_1)$. As is apparent from Equation 2-15, α_0 and β_0 of the prior beta distribution can be respectively interpreted as a prior number of failures observed over a prior number of demands. The posterior parameters α_1 and β_1 update the prior parameters based on the failure data.

Section 2.3.4.4 provides the general form for Beta and Binomial distributions. Depending on the prior information available, the parameters for the prior distribution (α_0, β_0) can be estimated using engineering judgment or expert elicitation, or constructed from generic data. However, these parameters are often already calculated and provided for the analyst in the generic data sources (for example, data updates on the NRC website [21]).

NOTE: If the beta distribution is highly skewed, and the evidence contains zero failures, Bayesian updating may yield unrealistic results, and a non-conjugate prior should be considered.

Example:

An example of the use of conjugate pairs can be provided for motor driven pumps using the following data from NUREG/CR-6928 [4]:

For this example, the following plant-specific data is assumed to have been collected since the time the last PRA update was performed:

Circulating water pumps Fails to start (FTS) 0 failures out of 80 demands

The plant-specific data constitutes the likelihood information in binomial form for the FTS.

To perform the update, the following data would be selected from NUREG/CR-6928 [4], Table A.2.27-6 for the prior:

Running/Alternating, FTS $\alpha = 0.881$; $\beta = 3.942E+02$ (parameters of Beta distribution)

For our specific example, the posterior Beta distribution parameters would be:

$\alpha_1 = (0.881+0) = 0.881$

$\beta_1 = [394.20 + (80-0)] = 474.2$

The Beta posterior mean would be calculated as follows:

$$\text{posterior mean} = \frac{\alpha_p}{\alpha_p + \beta_p} = \frac{\alpha_0 + x}{\alpha_0 + \beta_0 + n} \qquad \textbf{Eq. 3-5}$$

where α_0 and β_0 are the alpha and beta of the generic data and x and n are the number of failures and number of demands the pump experienced during the data window, respectively, from the plant-specific data.

$\alpha_p = \alpha_0 + x = (0.881+0) = 0.881$

$\alpha_p + \beta_p = \alpha_0 + \beta_0 + n = (0.881+394.2+80) = 474.881$

yielding a posterior mean value of 1.85E-03 failures per demand. Figure 3-3 shows the prior versus posterior distributions (CDF) for this update.

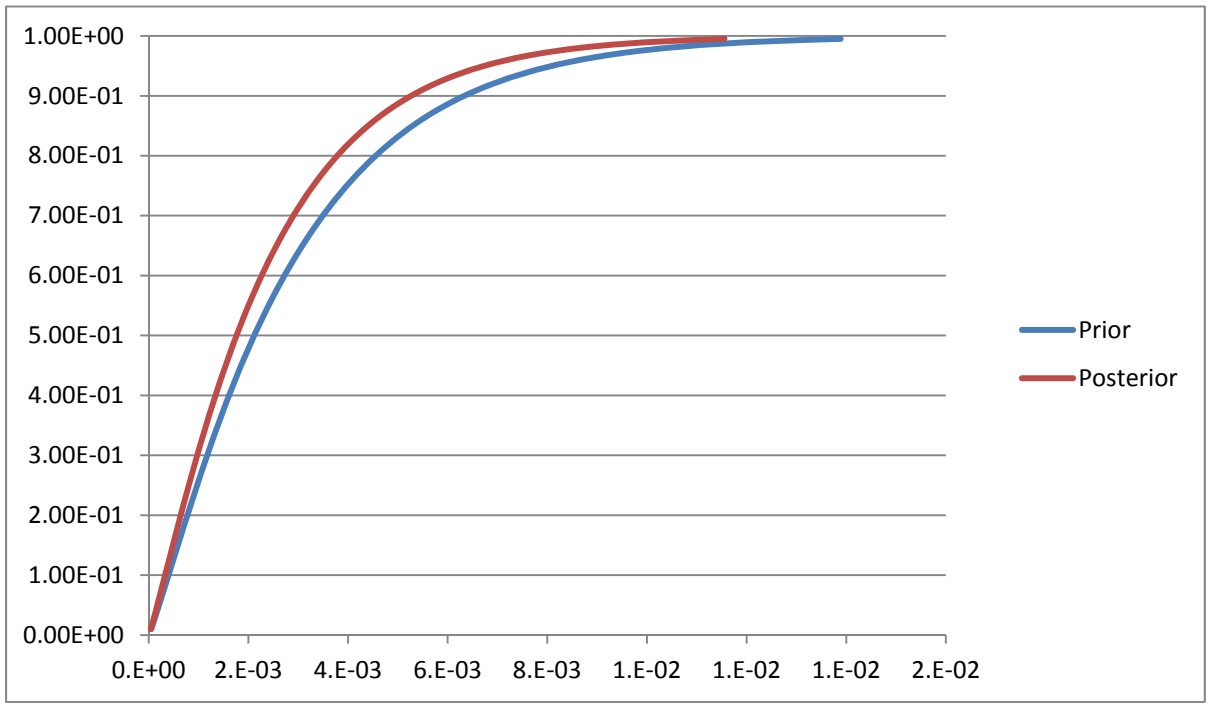

Figure 3-3
Example Bayesian update using Beta-Binomial: failure to start for circulating water pumps

NOTE: It is possible that there is some overlap between the generic data and the plant-specific data (for example, overlap in data window and database contents such that the generic data includes some or all of the plant-specific data). In this case there is potential for double counting that can result in a potentially non-conservative reduction in the uncertainty. This double counting is usually negligible for most cases of interest. The exception is when the generic data is sparse and/or is dominated by data from the plant in question.

3.3.2 Nonconjugate Prior Distributions

In the general case where the prior distribution and the likelihood function are not conjugate pairs, application of Bayes' theorem typically fails to yield a posterior distribution in a simple analytical form, requiring numerical evaluations for the posterior distribution. For this reason, non-conjugate distributions may be harder to visually check for reasonableness since the effect of the data may not be as intuitive.

As discussed in NUREG/CR-6928, section 6.2.2.6 [4], "Any continuous distribution defined on the allowed range of λ can, in principle, be used as a prior. The resulting posterior distribution is a continuous distribution, with no simple form. (Because the posterior distribution does not have a simple analytical form, it cannot be entered directly as an input to most PRA codes. Instead, a discrete approximation of the posterior distribution must usually be used.)" [NOTE: CAFTA software is able to use lognormal inputs to perform the update, as discussed further in Section 3.7].

Many of the older generic data sources, for example, contain only the lognormal mean and uncertainty (5th, 95th, Error Factor) parameters. The disadvantage of using the lognormal distribution as a prior distribution is that the posterior distribution obtained via Bayes' Theorem cannot be obtained in closed form as in the case of the beta or gamma distribution. In other words, the lognormal prior is not a conjugate prior. Consequently, the Bayes' update process is often performed by approximating the distribution by a similar conjugate prior, by using sampling routines, or by approximating the distribution by a discrete distribution.

A non-conjugate distribution (for example, lognormal) can be approximated by a similar conjugate prior (for example, gamma) using methods of moment matching as discussed in NUREG/CR-6928, section 6.2.2.7.2 [4]. If this approach is used, the analyst should note that if the evidence contains zero failures, Bayesian updating may yield unrealistic results, and the analyst should use an alternate way to perform the update (for example, numerical integration or assume ½ failure).

NOTE: An issue that has been encountered when using NUREG/CR-6928 [4] for priors in a Bayesian update is the following:

NUREG/CR-6928 presents the industry-average failure probabilities/rates as beta or gamma distributions, with alpha and beta parameters. However, that document also lists the mean and error factor (EF). If one uses the mean and EF listed and declares the prior to be lognormal and then performs a Bayesian update by converting that lognormal distribution (mean and EF) to a beta (or gamma) distribution, the resulting beta (or gamma) prior distribution is not the same as the original one listed in the NUREG. Specifically, the alpha parameter for the regenerated beta (or gamma) distribution can be much smaller than the original alpha parameter (a "weaker" prior). Then if the plant-specific data include no failures, the impact of the plant-specific data is much greater and can result in a posterior distribution that can be much lower than the result using the original beta (or gamma) distribution from the NUREG as the prior. In this case, the original gamma or beta distribution should be used.

NUREG/CR-6928, section 6.2.2.6 [4] discusses several other techniques that can be used, such as numerical integration, simple random sampling methods or Markov Chain Monte Carlo (MCMC) simulations (which it considers overkill for the purposes of this process).

Numerical integration methods utilize a "divide and conquer" strategy, where an integral on a relatively large set is broken down into integrals on smaller sets. These techniques, such as the trapezoidal rule or Simpson's rule can be programmed in a spreadsheet. Information on these methods can be found in some calculus texts, and in books on numerical methods [32].

Another approach is to generate a large random sample from the posterior distribution, and use the sample to approximate the properties of the distribution. This algorithm generates possible values of λ from the prior distribution, and discards most of those that are not very consistent with the data. The result is a sample from the posterior distribution. One such algorithm is called the rejection method for sampling from a distribution and is discussed in detail in NUREG/ CR-6928, section 6.2.2.6.2 [4]. Rejection sampling is based on the observation that to sample a random variable one can sample uniformly from the region under the graph of its density function. This and other Monte Carlo statistical methods are discussed in Robert and Casella [42].

Commercially available statistical software packages contain modules for Monte Carlo analysis and some contain a MCMC algorithm as well[2]. A Markov chain is a mathematical system that undergoes transitions from one state to another, between a finite or countable number of possible states. It is a random process usually characterized as memoryless: the next state depends only on the current state and not on the sequence of events that preceded it. In MCMC, the Markov chain is combined with Monte Carlo methods, which rely on repeated random sampling to compute their results. These MCMC software packages usually support a number of continuous and discrete distributions that can be used to specify either the prior distribution for the parameters or the sampling distribution for the dependent variables.

[2] Section 6.2.2.6.2 of NUREG/CR-6928 [4] provides a link to the WinBUGS software which can perform MCMC sampling.

It is not considered the province of these Guidelines to provide detailed information on these techniques since statistical software packages and reference materials have already covered the topic more thoroughly.

3.3.3 Non-Informative Prior Distributions

The ASME/ANS PRA Standard Requirement DA-D1 [7] mentions the possible use of a non-informative prior for Bayesian updating.

Non-informative priors are distributions that convey little prior information. Thus, when combined with likelihood data in the Bayesian update, the posterior distribution is mainly governed by the likelihood (plant-specific) data.

Several types of non-informative priors have been used in PRA applications, such as 1) Jeffreys non-informative priors, and 2) constrained non-informative priors, which are a type of minimally informative priors that only capture basic prior knowledge about the parameter being investigated, such as a point-estimate mean or median.

Since the likelihood data will dominate the posterior distribution, the use of non-informative priors is recommended when:

- There is extensive likelihood data available
- There is no consensus on the prior distribution

Ref. [13] provides the following parameter values for Jeffreys non-informative priors in Gamma and Beta form (using the notations cited earlier):

- **Gamma non-informative prior** (used for failure rates) has parameters $\alpha_0 = 0.5$ and $\beta_0 = 0$.

  If x failures have been observed over a timeframe of t hours, the mean posterior failure rate is equal to $(0.5 + x)/t$.

- **Beta non-informative prior** (used for failures on demand) has parameters $\alpha_0 = 0.5$ and $\beta_0 = 0.5$.

  If x failures have been observed over a number n of demands, the mean posterior failure probability is equal to $(0.5 + x)/(n + 1)$.

Constrained non-informative priors have not been widely used, and are not discussed further here. NUREG/CR-6823 [13] Sections 6.2.2.5.3 and 6.3.2.3.3/6.3.2.5.3 provide more detail on Gamma and Beta forms for constrained non-informative priors.

A Bayesian update based on a non-informative prior distribution will produce a posterior dominated by information from the data, making its use beneficial to avoid spending unnecessary resources on an informative prior distribution whose contribution will be overwhelmed by plant-specific data. In the situations where there are only scarce data, the influence of the non-informative prior may not be negligible, and as such the choice of the non-informative needs to be reviewed to ensure its adequacy, particularly for dominant risk contributors. In such cases, the following caveat is noted.

The non-informative prior may lead to overly conservative results – This situation may typically arise when a Jeffreys non-informative prior is used on a component type expected to be reliable but for which little specific operating experience is available. It is likely that in such a case no failure would be recorded over the observation period. The Bayesian update could thus yield a posterior distribution several orders of magnitude over the estimates that would be obtained if more operating experience was available. Using Jeffreys non-informative prior distributions as an example zero (0) failures recorded over an observation time t would yield a posterior mean failure rate equal to $0.5/t$. Similarly, zero (0) failures recorded over n demands would yield a posterior mean failure probability equal to $0.5/(n + 1)$. Thus in these cases the posterior distribution is almost entirely controlled by the plant-specific operating experience, via the value of t or n. As such, it may inappropriately overestimate the failure rate or failure probability, since there may not be nearly enough operating experience for t or n to be in the range that will bring the posterior distribution to values expected for reliable components. In these types of situations, it would be beneficial to model, in an informative prior, the knowledge about the component reliability (which is here the basis for why the component type is thought to be reliable). Pursuing with the previous example, this would be equivalent to postulating prior values α_0 and β_0 that are in line with what is a priori known about the component reliability. In particular, the value of β_0 will be sufficiently large to ensure that the posterior distribution is not controlled by t or n (it will instead be controlled by $t + \beta_0$ or $n + \beta_0$). This may be done based on generic information on similar components, adjusted with expert judgment as needed. A minimally informative prior distribution, such as the constrained non-informative prior, is sometimes used as a way to capture this type of prior information about the component being considered.

3.4 Observed Data and Likelihood Distribution

The "likelihood" portion of the Bayesian updating process is the probability function based on the plant-specific data that is collected for initiating events or components modeled in the PRA, as discussed in Sections 4 and 5. While the likelihood distribution can take on many forms, the most commonly used distributions in PRA are the Poisson and Binomial distributions discussed here.

For hourly failure rates, the Poisson distribution is used, with the possible values of the failure rate denoted as λ_i, per the following equation:

$$\boldsymbol{P(E|\lambda_i) = \frac{(\lambda_i t)^k}{k!} e^{(-\lambda_i t)}} \qquad \textbf{Eq. 3-6}$$

The plant operational evidence for the Poisson distribution is expressed in the form of k failures in t component exposure hours.

For failures on demand, the Binomial distribution is used. The possible values of the failure rate are expressed as x_i, per the following equation:

$$\boldsymbol{P(E|x_i) = \left(\frac{n!}{k!(n-k)!}\right) x_i^{\,k} (1 - x_i)^{(n-k)}} \qquad \textbf{Eq. 3-7}$$

For the Binomial distribution, the observed evidence from plant operational history is expressed in the form of k failures in n trials (or demands to function).

There are two underlying assumptions with these distributions: 1) that the underlying failure rate or probability (λ, x) is constant for all the data represented in the plant-specific dataset and 2) that the failures are independent. For the first assumption, the analyst should ensure there are no significant trends within the data or outliers in the dataset – this is referred to as "poolability." Section 3.6 provides further guidance on visual and statistical tests that can be used to verify the poolability of the plant-specific data. Non-continuities in the data may arise, for example, from aging trends in the data, evidence of early burn-in failures, a portion of the data may come from components operating in a significantly different environment, and so on. The second assumption relates to common-cause failures – the analyst should count dependent failures that occur close in time as one failure for the purposes of Bayesian updating.

One of the benefits of performing Bayesian updating is that if zero failures are experienced in the plant-specific likelihood data, there is no need to come up with an estimation technique for a numerator; the Bayesian combination with the prior resolves the problem.

3.5 Posterior Distribution

The output from the Bayesian updating process, combining together the prior information and the likelihood evidence, is called the posterior distribution. Calculation of the posterior is dependent on the form of the prior and likelihood, discussed in the previous sections. The general formula for Bayesian updating is:

$$\boldsymbol{\pi_1(\theta|E) = \frac{L(E|\theta)\pi_0(\theta)}{\int L(E|\theta)\pi_0(\theta)d\theta}} \qquad \textbf{Eq. 3-8}$$

Where $\pi_0(\theta)$ is the prior probability density function for parameter θ; $L(E|\theta)$ is the likelihood function using the observed evidence, E; and $\pi_1(\theta|E)$ is the posterior probability density function for parameter θ.

In order to meet Capability Category II the ASME/ANS PRA Standard Requirement DA-D4 [7] requires that the analyst check the reasonableness of the posterior by considering the relative weight of evidence provided by the prior and the plant-specific data.

The following examples are tests that are mentioned in this SR to evaluate whether or not the Bayesian update has been performed correctly:

- Confirm that the Bayesian update does not produce a posterior distribution with a single bin histogram when discrete distributions are used.
- Plot the posterior distribution to see if the shape is multimodal or otherwise unusual and investigate the cause.
- Check for inconsistencies between the prior distribution and the plant specific data.
  - Beware of overly narrow prior (informative) distributions: if "even large amounts of data have little or no effect on the posterior distribution, the prior distribution needs to be examined carefully, especially in the case of generic prior distributions [41]."
- Look at the reasonableness of posterior distribution over the whole range of values.
  - Beware that use of non-informative distributions with weak plant-specific data may produce overly conservative results for what is considered reliable equipment [41].
- Look at the posterior mean value to see if it is reasonable given the input data.

Section 3.6 provides further guidance on visual and statistical tests that can be used to verify the reasonableness of the posterior.

As with any data combination, it is important to understand the nature of the input information and how it influences the output data rather than just arbitrarily entering data into a program that does not include traceability of the interim process. Analysts who are unfamiliar with Bayesian estimation are strongly encouraged to work through some of the examples given in Section 6 of NUREG/CR-6823 [13] to develop a sense of how the process works and how the posterior distribution depends on the prior and on the data.

3.6 Model Validation

Model validation consists of both confirming the poolability of the plant-specific data and ensuring that the prior distribution reasonably represents the plant data observed. Generally, the data is first examined visually to identify possible inconsistencies. Then, if possible, mathematical methods may be applied to determine the statistical significance, or the strength, of the inconsistency. Finally, the results of the statistical tests are weighed against qualitative information about the systems or components to make a final determination.

From the engineering standpoint, the analyst needs to review the component boundary information from the plant-specific observed data vs. the boundary from the generic prior to ensure they are consistent. Joint discussions in cases of inconsistency should be held between the system analyst(s), the data analyst, and the person responsible for EPIX and Maintenance Rule reporting.

Section 6.3.3.1 of NUREG/CR-6823 [13] discusses how the "poolability" of data can be evaluated through graphical techniques or statistical tests. Examples of each are provided in the following subsections; these examples are geared towards checking the reasonableness of the posterior, but the same techniques can be used to check poolability of the plant-specific data.

3.6.1 Visual Review

By plotting the data subsets with confidence intervals on the same axis, it is possible to do an initial "eyeball" review and comparison to evaluate whether or not they should be combined together.

Some examples of plots comparing various priors, likelihoods and posteriors are presented below. See Section 2.3.4.4 for guidance on how to calculate the parameters of interest (mean, median, 5^{th} and 95^{th} percentile values) for the relevant distributions used in the visual review. The bounds for the curve labeled "likelihood" can be calculated using frequentist methods, such as those presented in Sections 6.2.1 and 6.3.1 of NUREG/CR-6823 [13].

Figure 3-4 plots data for a Motor-Driven Pump Fails to Continue to Run (from a non-nuclear application, hence the small industrial experience running hours):

Prior	$\alpha_0 = 0.35$	$\beta_0 = 17{,}805$
Observed data	$x = 35$ failures	$T = 456{,}567$ hours

In this instance, there is not much evidence in the prior, while the observed data has significant information. Due to the differences and the minimal degree of overlap of the distributions, there are questions regarding whether the two distributions should be combined. The number of plant-specific failures could be evidence of early burn-in failures or a different operating environment, either of which should be checked by plotting each failure along a timeline and reviewing additional plant information regarding the medium of exchange or location of equipment. Depending on the strength of the qualitative argument, the posterior may be considered acceptable.

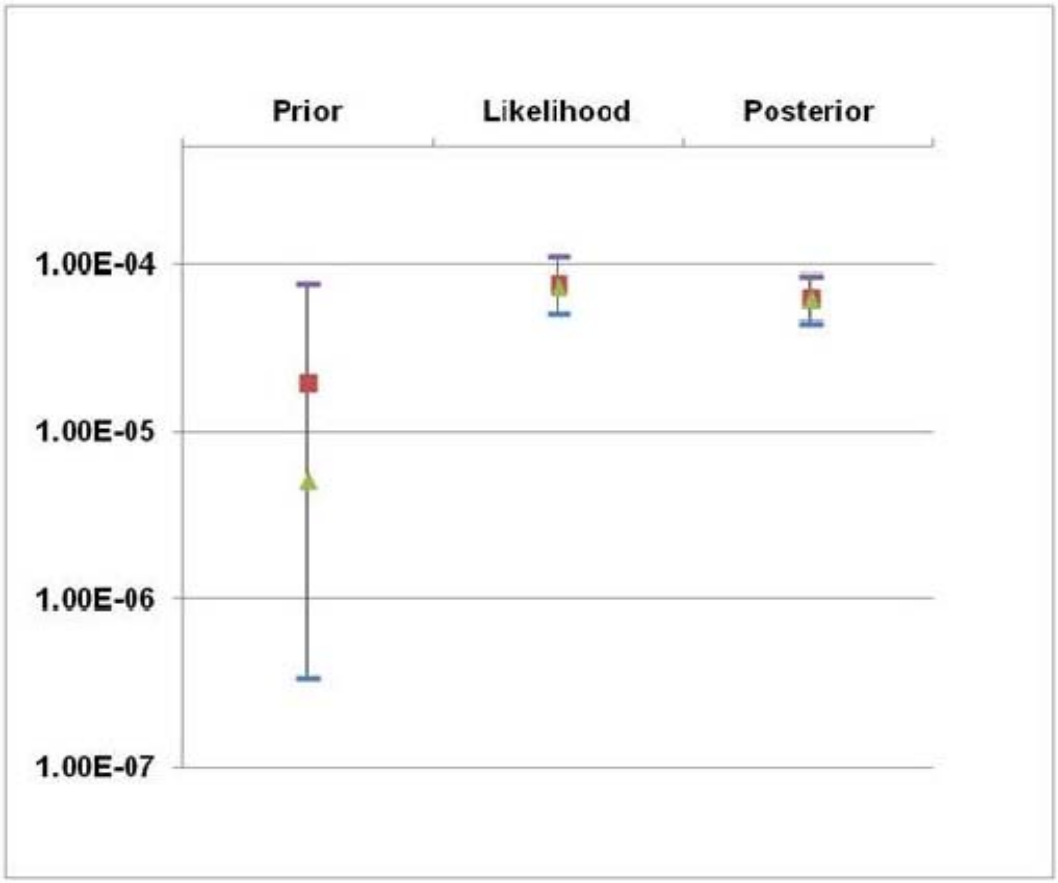

Figure 3-4
Example Bayesian update for failure of motor-driven pump [fails to continue to run]

The next plot, Figure 3-5, data is presented for the Break or Rupture of an Aftercooler:

Prior	$\alpha_0 = 1.63$	$\beta_0 = 1{,}368{,}987$
Likelihood	$x = 0.3$ failures	$T = 87{,}451$ hours

[Note that the likelihood numerator is actually zero failures but 1/3 failure was used to estimate the mean for the plot. In actuality, the zero failure value of the likelihood would be used "as is" for the Bayesian update.]

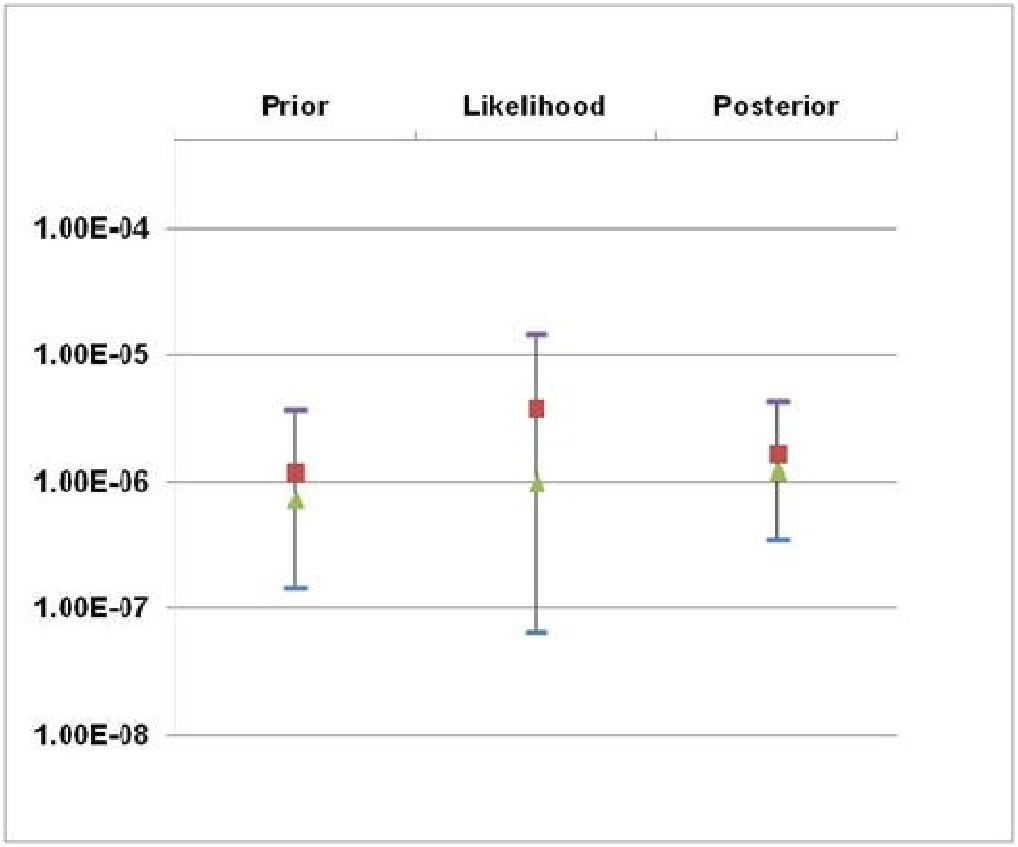

Figure 3-5
Example Bayesian update for break or rupture of an aftercooler

As we would normally expect, there is more evidence from the prior than from the likelihood, but the distributions are comparable so updating is reasonable. Note that the uncertainty bounds narrow with the combined information.

Finally, Figure 3-6 plots data for Relief Valve with a failure mode of Transfers Open:

Prior	$\alpha_0 = 0.35$	$\beta_0 = 2{,}896{,}627$
Likelihood	$x = 5$ failures	$T = 913{,}133$ hours

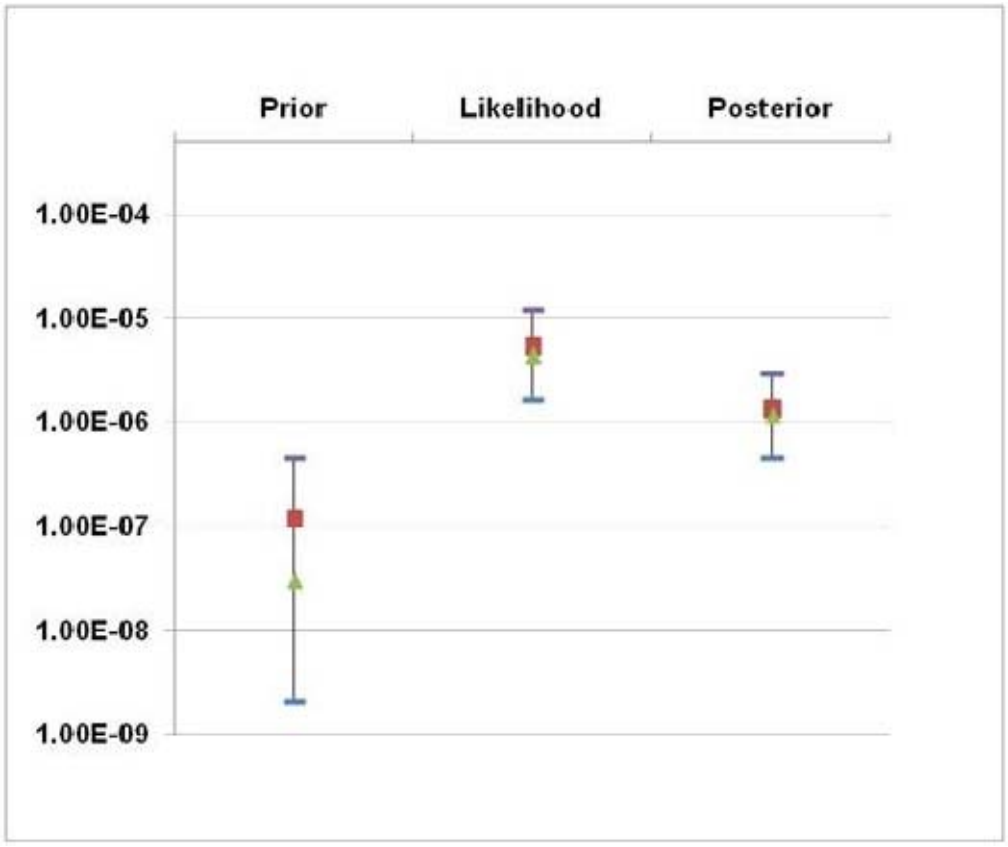

Figure 3-6
Example Bayesian update for failure of relief valve [transfers open]

The disparity between the prior and likelihood mandates that the analyst investigate whether they are in fact part of the same population or whether it would be better not to update but to choose between the estimates.

3.6.2 Statistical Testing

NUREG/CR-6823 [13] provides many different types of statistical tests that can be used in the model validation process to both 1) ensure the poolability of the evidence and 2) to check the consistency of the prior data with the observed evidence (a detailed example is provided for this second application). Table 3-2 provides a summary of these tests and their applicability.

Table 3-2
Summary of statistical tests for model validation

Test	Description	Caveats	NUREG/CR-6823 [13] Section Reference
Chi-Squared Test	This test allows the analyst to determine the statistical significance of a postulated hypothesis based on binned data. This can be used to determine if there are outliers (for example, H_0: λ is the same in all the data subsets) or trends (for example, H_0: λ is consistent over time) in the data. For failure on demand, this test is also commonly called a "contingency table" when testing for outliers.	The total count is large (see reference for more precise definitions of "large").	6.2.3.1.2 (Gamma, outlier) 6.2.3.2.2 (Gamma, time trend) 6.3.3.1.2 (Beta, outlier) 6.3.3.2.2 (Beta, time trend)
Laplace Test	This is a two-sided test that can be used to determine if there monotonic trends in the data. (Gamma)	The Laplace test has more power for detecting trends, but cannot detect erratic changes in the data that would suggest the data does not have the same underlying failure rate the way the Chi-Squared test can.	6.2.3.2.2
Wilcoxon-Mann-Whitney Test	Similar to the Laplace test, but for demand-based data. (Beta)		6.3.3.2.2
Consistency of Data and Prior	This tests the ability of the prior to predict the evidence. If the evidence is unlikely given the prior distribution that may indicate that the prior distribution is not representative of the data. (Gamma, Lognormal, Beta)	For prior distribution types other than gamma and beta, the solution does not have a direct analytical form and must be evaluated numerically.	6.2.3.5 6.3.3.4

Example: Examining Consistency of Data and Prior to Test for Outliers

The consistency check process cited in Sections 6.2.3.5 (time-related data) and 6.3.3.4 (demand data) of NUREG/CR-6823 [13] can also be used to determine if an outlier should be excluded.

The process described in that document asks what the prior probability is of getting the observed data (or better). If the observed data is known to be in the right tail of the prior distribution, the probability of observing x or more events is:

$$\boldsymbol{P(X \geq x) = \int \Pr(X \geq x|\lambda)\, f_{prior}(\lambda) d\lambda} \qquad \textbf{Eq. 3-9}$$

While in this equation the "prior" refers to a generic data source under consideration for Bayesian update, the same comparison can also be made between one set of plant-specific data and another (for example, one system's motor-driven pump fails-to-start (FTS) data and the motor-driven pump FTS data across systems).

For example, when examining data for MOVs across the same plant, the analyst finds that for one system, the number of failures relative to the demands is a lot higher than it appeared to be for the other systems. One could pool the data for all the other systems, perform a Bayesian update, and then test the ability of the resulting posterior to predict the suspected outlier. Alternatively, the analyst could collect the data for all the other systems and test the experience for the potential outlier against the 'other systems' distribution first, before doing a Bayesian update. The parameters for beta or gamma could be calculated on a plant-specific basis (for example, using the Jeffreys simplified constrained non-informative distribution (SCNID) as was done in NUREG/CR-6928) and then the comparison could be made.

Knowing the outlier is in the right portion of the tail, if the tail probability $\Pr(X \geq x)$ is less than 0.05, then that is considered strong evidence that the data are inconsistent with each other. If the outlier is in the left portion of the tail, the test would be performed for $\Pr(X \leq x)$, with the same 0.05 criteria.

If inconsistency is determined, then this may indicate that the data should be considered separately. Some analysts consider whether the plant-specific data that differs is based upon more than one failure and if inconsistency was the result of only one failure, the inconsistency result was judged to be too uncertain and the data was retained as part of the same dataset. It should be recognized however that in the case of sparse data, a single failure may be the only information available and inconsistency is a moot point.

Often when compiling plant-specific data, the analyst will note that one component may be notably worse in terms of failure history than the others of a similar type (whether within or across systems). These insights are valuable beyond the data analysis alone and should be discussed with plant personnel to identify whether operational conditions or preferences are driving these differences.

To illustrate this process with an example, suppose we have a component which we have collected failure to run data from seven separate systems within the plant:

System	Failures	Hours
1	0	800
6	0	500
7	0	1250
3	1	1700
4	6	2000
2	0	2200
5	3	3200

For time-related data (gamma prior distribution and Poisson plant-specific data), the expression is the following (taken from section 6.2.3.5 of [13]):

$$\boldsymbol{P(X \geq x) = 1 - \sum_{k=0}^{x-1} \left(\frac{\Gamma(\alpha+k)}{k!\Gamma(\alpha)}\right) (t/\beta)^k (1 - t/\beta)^{-(\alpha+k)}} \qquad \textbf{Eq. 3-10}$$

Figures 3-7 and 3-8 below provide a graphic of the prior distribution, the posterior distribution where system 4 is excluded and the posterior distribution where the prior is only updated using system 4 data. We suspect based on visual comparison of the data that System 4 is an outlier and should be removed from the data.

The prior distribution based on generic data for this component is a Gamma distribution with parameters (1.5; 1,160). If the data is updated with all the data *except* the data from System 4, then the resultant distribution is a Gamma distribution with parameters (5.5; 10,800). The probability that the resultant posterior distribution predicts the experience of System 4 is 0.0017, indicating that the resulting distribution is inappropriate to model System 4.

When the test is applied using the original prior distribution we see that the probability is 0.065, which is not strong enough evidence by itself to indicate that the prior should not be used in an update of the data from System 4 to produce a posterior that is specific to System 4. The analyst would have to look at qualitative arguments to understand if the generic data can be used in this case.

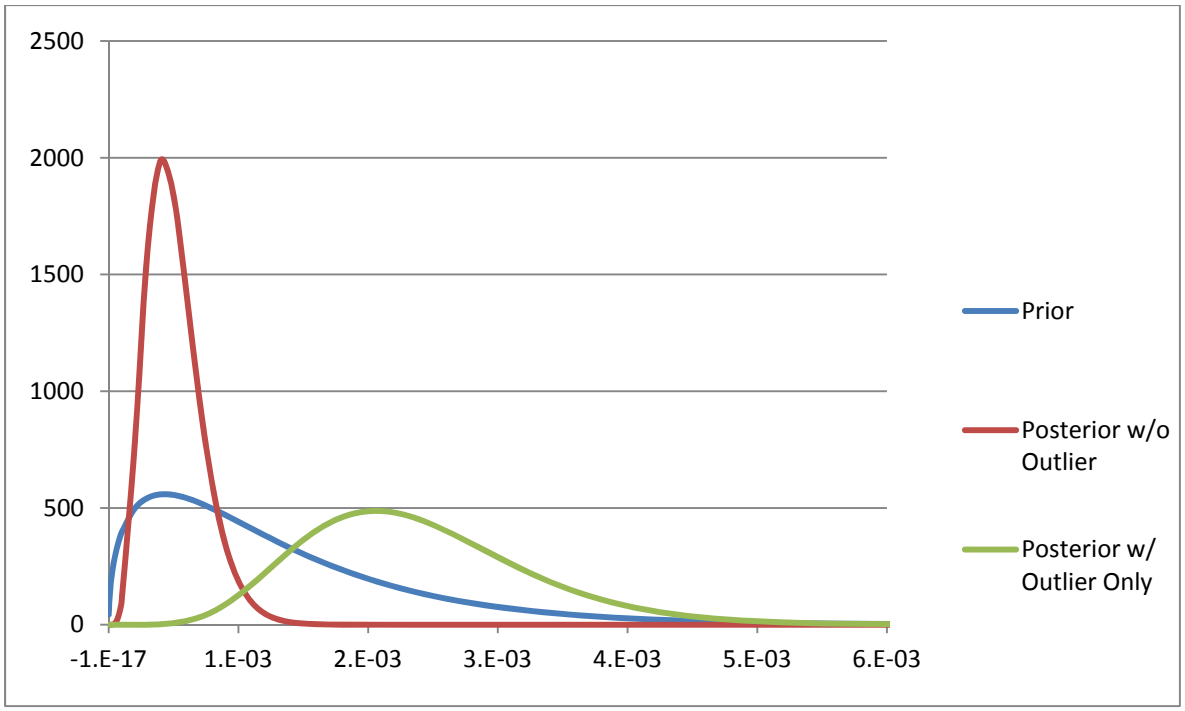

Figure 3-7
Example distribution comparison for outlier evaluation

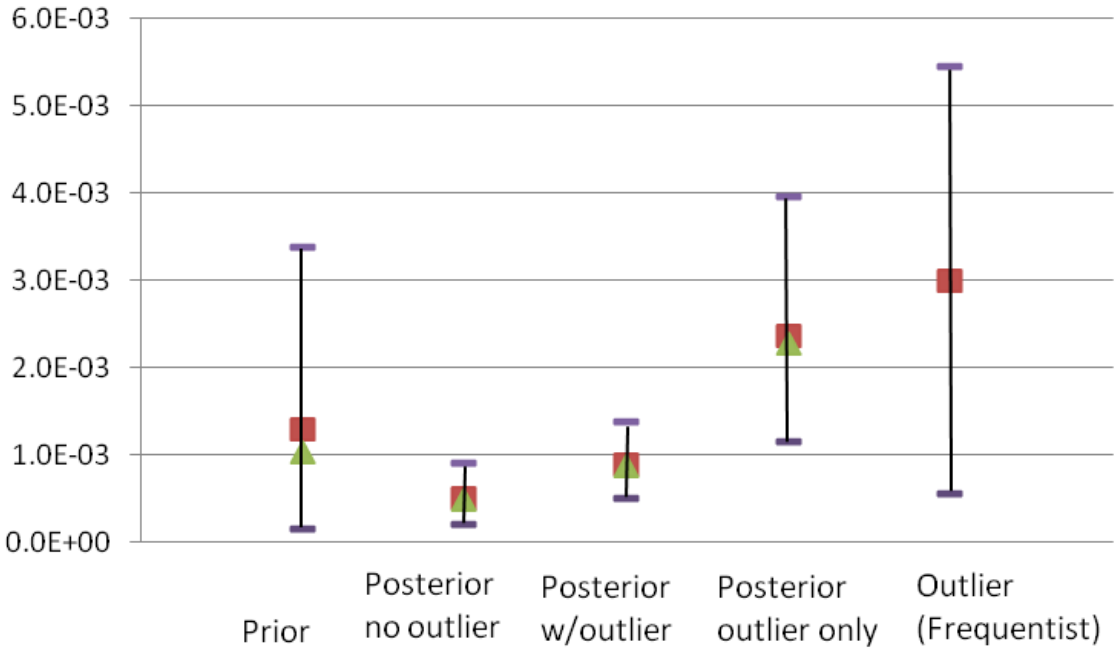

Figure 3-8
Example distribution comparison for outlier evaluation – alternate view

Calculations used to support the example:

The 5th, median and 95th percentiles in Figure 3-8 were evaluated using Microsoft EXCEL 2007 function "GAMMAINV(probability, α, β)," where "probability" was the percentile of interest. The 95% confidence interval for the failure rate based on just the outlier data ("likelihood") was estimated using the standard error as defined in NUREG/CR-6823 [13] Section 6.2.1.2.

Realizing that Equation 3-10 (inside the summation) is the **negative binomial distribution**, Microsoft EXCEL 2007 function "NEGBINOMDIST(f, α, p)," can be used to perform the statistical test and calculate $P(X \geq x)$.

where "f" is the value of k [which increments from k=0 -> (x-1), and x is the number of failures in the outlier being tested],

α is from the gamma distribution being tested,

and $p = 1 - \frac{t}{t+\beta}$, where t is the run time of the outlier and β is from the gamma distribution being tested.

The following formulas and associated values (Figure 3-9) were used to perform the statistical test by evaluating Equation 3-10.

	A	B
1		
2	**Alpha**	5.5
3	**Beta**	10800
4	**failures**	6
5	**time**	2000
6	**p=1-t/(t+B)**	=1-(B5/(B5+B3))
7		
8	**k**	**NegBinomDist**
9	0	=NEGBINOMDIST(A9,B2,B6)
10	1	=NEGBINOMDIST(A10,B2,B6)
11	2	=NEGBINOMDIST(A11,B2,B6)
12	3	=NEGBINOMDIST(A12,B2,B6)
13	4	=NEGBINOMDIST(A13,B2,B6)
14	5	=NEGBINOMDIST(A14,B2,B6)
15	**Pr(X≥x)=**	**=1-SUM(B9:B14)**
16		

	A	B
1		
2	**Alpha**	5.5
3	**Beta**	10800
4	**failures**	6
5	**time**	2000
6	**p=1-t/(t+B)**	0.84375
7		
8	**k**	**NegBinomDist**
9	0	0.427630752
10	1	0.334086525
11	2	0.156603059
12	3	0.057094865
13	4	0.017842145
14	5	0.005018103
15	**Pr(X≥x)=**	**0.00172455**
16		

Figure 3-9
Evaluating Equation 3-10 using MS EXCEL "NegBinomDist" function

3.6.3 Applying Engineering Judgment

Engineering significance is just as important as statistical significance. Engineering judgment should include the answers to questions such as [13]:

- Are there qualitative reasons that can explain the inconsistency (for example, a change in the maintenance program leads to increased reliability)? Note: it is easy to find justifications in hindsight, after seeing the data.
- Is the component risk significant? What are the consequences to including or excluding that data?

For example, in NUREG/CR-5750 [3] provides an example of engineering judgment compensating for lack of strong statistical evidence. Examining the evidence between 1987-1997 (5 events prior to 1987, three events between 1987-1993 and no events 1994-1997), "showed no statistical evidence of a decreasing trend in the SGTR frequency. This result is driven by the small size of the data population. A sensitivity calculation showed a trend would become statistically significant in the year 2001 if no other SGTR events occur up to that year. Although the limited data provided no statistical basis for a decreasing trend in SGTR frequency, there may be engineering reasons (for example, better inspection techniques, increased sleeving or plugging of tubes, and improved secondary system chemistry control) for observing no SGTR events from 1993 to1997."

Care should be taken when data is sparse – in this case any exclusion of data can have a large impact on the resultant distribution [43] and should only be done when there is a strong qualitative reason. Additionally, the analyst should beware of cognitive biases [41].

3.7 CAFTA Use of Bayesian Parameters

The EPRI CAFTA PRA software tool calculates posterior distributions using the Bayesian Update method for Lognormal, Beta and Gamma distributions. Lognormal distributions may have time-dependent or demand failure rates. Gamma distributions typically use time-dependent failure rates; beta distributions typically use demand failure rates.

The analyst has the choice of which distribution type they would like to select for the prior. For Gamma and Beta distributions, the update calculation is straight forward and done according to the formulas presented in section 3.3.1. If a lognormal prior is selected, CAFTA will find a Beta or Gamma distribution "equivalent" to the original log-normal.

CAFTA uses the concept of matching Moments to find an "equivalent" Beta or Gamma distribution. Specifics of how this is done can be found in the EPRI Knowledge Base article KB66 on Bayesian Calculation in CAFTA [44].

Bayes calculation parameters are input to CAFTA from the Bayes Data tab on the Edit Rate Data dialog. Bayes input parameters and calculated posterior distribution values are stored in the Type Code table of the database.

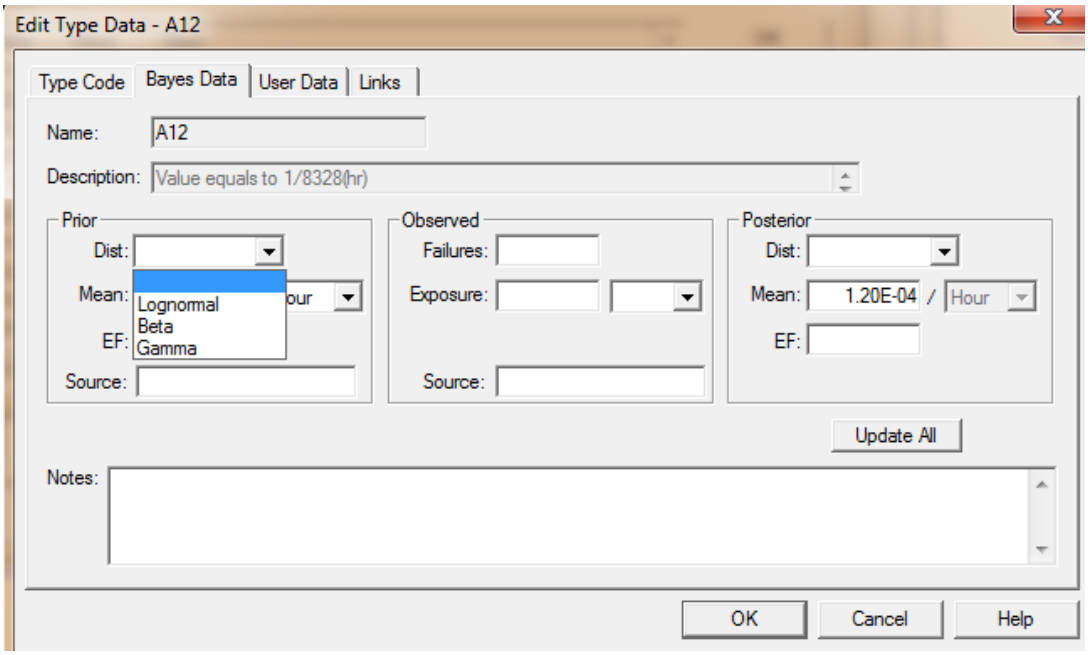

Figure 3-10
Screenshot of Bayesian calculations for CAFTA (v. 6.0)

NOTE: The selection of distribution type is important because if the user selects demands with gamma or time with beta, CAFTA will apply the same formulas, which will make no physical sense.

NOTE: There is a special case that needs to be considered in CAFTA for zero failures in the observed data (k = 0). This is specific to the case of using a lognormal prior and performing a Bayesian update using moment-matching to convert to/from a conjugate gamma distribution. In this case, the error factor is invariant even though the mean changes (potentially causing an overly narrow or skewed distribution). This is an artifact caused by the moment-matching conversion. To avoid this, the analyst can pick a gamma distribution as the input prior/output posterior distribution type. Alternatively, the analyst can use a lognormal distribution and assume a fractional failure (for example, ½ or 1/3 of a failure); this is conservative.

3.8 Standard and Regulatory Requirements

The use of a Bayes update process is explicitly recommended in Ref. [7] to combine evidence from generic and plant-specific data, for the conduct of internal events, at-power PRAs.

Regarding the evaluation of initiating events, Ref. [7] states in IE-C4, for all capability categories, that the analyst should provide justification for the selection of the prior distribution.

For component failure data, the DA requirements talk about the weighting of plant-specific vs. generic data in Bayesian updates, uncertainty estimation, and the selection of priors.

3.9 When Is an Update Needed?

Generally speaking, the Bayesian approach offers a statistical framework that naturally lends itself to an iterative process where prior information can readily be updated in light of new available data. Assuming that the generic prior and plant-specific evidence are compatible, the posterior distribution will offer a statistical representation of the uncertainty about the parameter under consideration that is informed by the latest plant-evidence covered by the data. Nevertheless, little plant-specific evidence may have accrued since the last Bayesian update, and the question arises on whether or when a new Bayesian update is warranted.

To answer this question, a possible approach consists of evaluating the merit of an update, based on an estimation of the change between the prior and posterior distributions. A simplified approach for an easy comparison can be done using conjugate distributions. Based on this comparison, the analyst can judge whether a Bayesian update is warranted. For example, if the plant-specific evidence reveals no failure recorded over an observation period representing 5 percent of the equivalent prior observation period, Equations 3-1, 3-2 and 3-3 show that α_1 will have the same value as α_0, while β_1 will be equal to 1.05 times the value of β_0. This will result in a new (posterior) mean failure rate equal to the initial failure rate decreased by a factor of 1/1.05, which corresponds to a relative decrease of approximately $1 - 1/1.05 = 4.8$ percent. The analyst might judge that this does not warrant a Bayesian update. In contrast, a failure recorded over the same period will likely be significant if the component under consideration is normally reliable. In such a case, a Bayesian update would be warranted to reflect the latest plant-specific information.

3.10 Peer Review Findings

Peer Reviews have been and continue to be conducted to evaluate the adequacy of Internal Events PRAs against the ASME/ANS PRA Standard guidance in the area of Data Analysis (DA). The following issues reflect findings that have been made in recent PRAs in the chapter topic area and recommended guidance based upon finding recommendations and PRA data practitioner experience.

1. Recommend best practices for choosing the time window for operation history for Bayesian updating. Can it overlap the generic prior data without being adjusted to remove that given plant's history?

   Recommended Resolution: It is possible that there is some overlap between the generic data and the plant-specific data (for example, overlap in data window such that the generic data includes some or all of the plant-specific data). In this case there is potential for double counting that can result in a potentially non-conservative reduction in the uncertainty. This double counting is usually negligible for most cases of interest. The exception is when the generic data is sparse and/or is dominated by data from the plant in question.

2. Updating with Zero Observed Failures per ASME/ANS PRA Standard SR DA-D1

   Finding: A Bayesian analysis was not done when there are no plant-specific failures. This is unacceptable for Category II or Category III. The discussion justifying not performing such updates in the DA Notebook is misleading because of the very small failure probabilities involved in the example given. Based on NUREG/CR-6928 parameters for distributions, with as few as 200 to 1000 demands, the posterior mean could drop by a factor of 2. It is not acceptable to skip performing a Bayesian update when zero plant-specific failures are observed.

   Recommended Resolution: Bayesian updating should be performed even when there are no plant-specific failures, unless there is good justification for not doing so. See Section 3.9.

3. Prior data versus Posterior bounds per ASME/ANS PRA Standard SR DA-A4

   Finding: Not Met CC II/III due to the lack of discussion and documentation relating to examination of inconsistencies between the prior distribution and the plant-specific evidence to confirm that they are appropriate. A review of the Update Spreadsheet in support of the Bayesian analysis reflects a single failure in which the posterior mean fell outside the uncertainty bound of the prior distribution.

   Recommended Resolution: Perform the checks on the posterior as described in Section 3.5. Additionally, if discrepancies are suspected, the analyst can conduct visual or statistical testing as discussed in Section 3.6 to examine the extent of the inconsistencies between prior and likelihood. The final conclusion should reflect a balance between the qualitative argument and the strength of the statistical or visual tests.

4. Initiating Event Uncertainty per ASME/ANS PRA Standard SR IE-D3

   Finding: A qualitative assessment of identified initiating event uncertainties is presented, but no basis provided for selection of uncertainty distributions. No technical basis is provided for conversion of uncertainty distributions to lognormal, other than to facilitate Bayes update.

   Recommended Resolution: Sections 2.3.4.4 and Table 3-1 provide information on selection of distribution types. Beyond a high-level qualitative check for appropriateness of the distribution (for example, are the bounds reasonable? Is the shape reasonable? Does it fit the confidence bounds?), there is no "data" that supports choice of one distribution over another. In most applications, the shape of the distribution is not a critical differentiator. The following additional discussion comes from [44].

   > There is no theoretical foundation for or against either the gamma or log-normal distributions, and there is little data for either choice, particularly if the shape is dependent on the grouping. The log-normal distribution has the advantage that it is easy to obtain the distribution parameters for the 5% and 95% values, whereas this is difficult for the gamma. On the other hand, the gamma distribution forms a conjugate prior when using the exponential model (that is, a gamma prior leads to a gamma posterior), and this simplifies Bayesian calculations, whereas, the log-normal is difficult to work with analytically. The choice between log-normal and gamma therefore becomes: "Do we just desire a distribution?" (the log-normal has easily obtained parameters) or "Will we perform Bayesian updating?" (the gamma is easier to work with analytically).

4
INITIATING EVENT DATA

4.1 Introduction

This section provides guidance to the analyst on how to collect data on initiating events and how to calculate initiator frequencies. This guidance focuses on calculating initiating events at-power; however, the concepts presented can be used to understand how initiating events can be calculated for LPSD.

One of the first tasks conducted in any PRA is the identification of initiating events. An initiating event is defined as an occurrence, or upset, which causes a plant disruption resulting in a challenge to one or more of the plant systems required to maintain stable cooling of the reactor core. In addition, the occurrence causes or requires a reactor trip, either automatically or by manual action, to prevent possible accident sequences leading to core damage or release of airborne fission products. The PRA then postulates and systematically examines accidents as a series or progression of events that follow an initiating event, or initiator.

Initiating events include human-caused disruptions and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds) [7].

The preferred measure for initiating events is annual frequency. A plant may experience several events per year or the equivalent of only one event in thousands of years.

Initiators are characterized as groups known as classes or categories. These initiating event classes are generally identified and modeled by the specific event that poses the most severe challenge to the plant. However, the frequency of these classes is estimated based upon the sum of all events that appear in a given class.

4.2 Methodology

Initiating event analysis for PRA follows the following steps:

- Data Collection – identify the most current events (SCRAMs) from current plant experience and obtain the most current generic data.
- List and Group Development/Update – use data to update existing list of initiating events from previous PRAs or develop a list from generic initiator data references, grouping by common plant impacts.
- Frequency Estimation – quantify frequency for each defined initiating event using generic and plant specific data as applicable.

4.3 Initiator List and Group Development

The initiating event analysis for PRA begins with the compilation of a comprehensive list of initiating events that might lead to core damage or radionuclide releases. Most plants already have a stable initiator list, so this guideline emphasize list update rather than list development from scratch. This part of the initiator identification process is primarily a systems analysis job, but the data analysts will have to interface closely with the systems analysts to understand what initiators are being added and what commensurate data will be needed.

The types of initiators that can challenge plant integrity (consistent with the minimal set of initiating events cited in the ASME/ANS PRA Standard [7]) are:

- Plant Transients – equipment and human-induced events that disrupt the plant and leave the primary system pressure boundary intact [45]. NUREG-5750 [3] includes the following definition of transients: "general transients are a combination of all reactor trip events that had no direct impact on mitigating systems' ability to remove decay heat."
- Loss of Coolant Accidents (LOCAs).
- Steam Generator Tube Rupture (SGTR) in PWRs.
- Interfacing System LOCAs (ISLOCA) – postulated events in systems interfacing with the reactor coolant system that could fail or be operated in such a manner as to result in an uncontrolled loss of core coolant outside the containment [7].
- Special initiators (for example, support systems failures, instrument line breaks; these initiators may result in either a transient or a LOCA type of sequence). Examples of special initiators for a PWR include:
  - Support systems
    - AC instrument buses
    - DC buses
  - Internal flooding or fire
  - Main Steam Line Break (MSLB) inside and outside containment

4.3.1 List Development

The development of the list of possible initiating events follows these guidelines:

- Use of generic industry lists/groups.
- Review of lists from comparable plants.
- Review of plant-specific trip reports such as Licensee Event Reports (LERs).
- Evaluation of each system to determine if a system failure causes an initiating event. This should include possible initiating events resulting from multiple failures if the failures are due to a common cause (for example, CCF of 2 DC Panels). Consider various system alignments that may influence the likelihood of an initiating event.
- Consideration of events that have occurred at conditions other than at-power unless it is determined they are not applicable to at-power conditions.
- Interviews with plant personnel (for example, operations, maintenance) to determine if any initiating events have been overlooked.

- Consideration of initiating event precursors in the plant experience.
- Inclusion of multi-unit site initiators such as Loss of Offsite Power (LOOP) and Loss of Instrument Air for shared systems.
- Inclusion of any initiating events that have been identified during peer reviews, PRA certifications, or self-assessments.

High-level initiator categories reflect the status of RCS integrity:

- Loss-of-coolant accidents
- Transients, with RCS integrity initially intact

Further breakdown reflects consideration of thermal-hydraulic performance based on similar trends and effectively the same success criteria.

4.3.2 Screening

Engineering judgment is used to qualitatively screen out initiators based on inapplicability to the plant-specific design or operation characteristics. Examples are provided in Table 4-1.

Table 4-1
Initiator screening examples

Initiating Event	Basis for Non-Inclusion
Very small LOCA/leak	Break sizes less than 0.0005 ft^2 are considered leaks rather than small LOCAs, since (as plant-specific thermal hydraulic analysis and plant experience with such leaks shows) the normal charging system can maintain RCS inventory so that RCS pressure and pressurizer level do not decrease. Any one of the three charging pump trains that is in service at the onset of the event can maintain the function. Very slight system depressurization may occur, but no automatic trip or safety injection would be generated (a manual plant shutdown to meet Technical Specification action requirements would be required, however). Therefore, this IE is not applicable as a separate initiator, but are combined with the normal transient/shutdown initiating event.
Stuck open: 2 or more safety/relief valves	Plant-specific thermal hydraulic calculations show that a single stuck open safety relief valve scenario provides results in terms of timing required to start injection systems and transfer suction supplies to the high head safety injection pumps that are as limiting as the multiple stuck open relief valve scenario. In addition, a single stuck open relief valve is a more likely occurrence than is multiple stuck open relief valves. Therefore, this IE is screened from the analysis.
Turbine bypass unavailable	Turbine bypass is represented by steam dump to the condenser at this plant. In addition to the condenser, steam dump to atmosphere is available through the Atmospheric Dump Valves (ADVs) and Safety Valves. However, plant trips involving unavailability of steam dump to the condenser are counted as Loss of Condenser Heat Sink initiating events. Therefore, this initiator is screened as a separate initiating event.

Screening can also be done on a quantitative basis if the frequency of the event is sufficiently low. ASME/ANS PRA Standard [7] supporting requirement IE-C6[3] provides screening criteria for initiators based on frequency and immediacy of reactor shutdown (requirements paraphrased below):

- Event frequency < 1E-7 per reactor year except for ISLOCA, containment bypass or reactor pressure vessel rupture.
- Event frequency < 1E-06 per reactor year where core damage is highly improbable (specifics identified in the standard).
- Event does not require plant shutdown until after initiator conditions have been resolved.

4.3.3 Grouping

Initiators are grouped so that events in the same group have similar effects on the plant's ability to safely shut down or have similar plant mitigation requirements. Initiating events with significantly different plant response impacts or different radionuclide release potential are grouped separately.

Groups should be defined so that all events included in each group share important attributes [9], such as:

- Impact on RCS integrity
- Similarity in plant thermal-hydraulic performance (temperature and pressure response)
- Same requirements for systems to maintain core cooling (that is, success criteria)
- Common operator actions expected for response
- Similar timing of events
- Similar potential end-states (high-pressure sequence, low-pressure sequence, and so on).

The representative event for the group should be a reasonable bound on the events in that group. Grouping is based on realistic analyses and is iterative, interfacing with the accident sequence analysis task of the PRA to ensure that the use of the bounding transient is not overly conservative. The development of mutually exclusive initiator bins therefore requires a tradeoff between the worst case for a given initiator category and differentiation based on plant mitigation requirements. If the bin is too big, the resulting frequency might be too conservative. The analyst should therefore look for balance between the frequency and the bounding nature of the events.

Grouping initiating events into general categories leads to a more manageable analysis, but still retains the identity of initiators that result from unique plant challenges, allowing for a realistic estimation of the CDF. The general categories include, but are not limited to, 1) transients, 2) LOCAs, and 3) special initiators.

[3] Screening criteria were identified as a cross-cutting issue by the ASME/ANS Subcommittee on Standard Maintenance. The resolution of this issue could very well change the wording of the SR and the screening criteria for initiating events could change in the future.

Table 4-2 shows the initiating event grouping from NUREG/CR-6928 [4] that is included in the U.S. NRC standardized plant analysis risk (SPAR) models and is used to structure NRC generic initiator data development.

Table 4-2
NUREG/CR-6928 [4] initiating event list

Initiating Event	Category
Large Loss-of-Coolant Accident at Boiling Water Reactors	LLOCA (BWR)
Large Loss-of-Coolant Accident at Pressurized Water Reactors	LLOCA (PWR)
Medium Loss-of-Coolant Accident at Boiling Water Reactors	MLOCA (BWR)
Medium Loss-of-Coolant Accident at Pressurized Water Reactors	MLOCA (PWR)
Loss of Vital AC Bus	LOAC
Loss of Component Cooling Water	LOCCW
Loss of Condenser Heat Sink at Boiling Water Reactors	LOCHS (BWR)
Loss of Condenser Heat Sink at Pressurized Water Reactors	LOCHS (PWR)
Loss of Vital DC Bus	LODC
Loss of Instrument Air at Boiling Water Reactors	LOIA (BWR)
Loss of Instrument Air at Pressurized Water Reactors	LOIA (PWR)
Loss of Main Feedwater	LOMFW
Loss of Offsite Power	LOOP
Loss of Emergency Service Water	LOESW
Partial Loss of Component Cooling Water System	PLOCCW
Partial Loss of Emergency Service Water	PLOESW
Steam Generator Tube Rupture	SGTR
Small Loss-of-Coolant Accident at Boiling Water Reactors	SLOCA (BWR)
Small Loss-of-Coolant Accident at Pressurized Water Reactors	SLOCA (PWR)
Stuck Open Relief Valve at Boiling Water Reactors	SORV (BWR)
Stuck Open Relief Valve at Pressurized Water Reactors	SORV (PWR)
General Transient at Boiling Water Reactors	TRAN (BWR)
General Transient at Pressurized Water Reactors	TRAN (PWR)
Very Small Loss-of-Coolant Accident	VSLOCA

4.3.4 List Update

According to ASME/ANS PRA Standard Requirement IE-A9, when performing a PRA update, the initiating event list needs to be reviewed against initiating event precursor events to ensure that no new initiating events need to be added. To meet Capability Category II, plant-specific operating experience only needs to be reviewed; to meet Capability Category III, industry operating experience also needs to be reviewed.

4.4 Initiator Frequency Calculation

Initiator frequencies are calculated either using a data-driven approach or a fault tree approach to estimate the frequency of special initiators when insufficient data exists either because it is a rare event or the initiator is so plant-specific that generic data cannot be applied. Development of support system initiator fault trees must still meet the ASME/ANS PRA Standard [7] systems analysis (SY) requirements for completeness and event screening per IE-C8, -C9, -C10 and -C11and can therefore involve a lot of work. However, this can be useful, particularly if the PRA model is to be used for Maintenance Rule a(4) (on-line maintenance) risk assessments.

4.4.1 Defining Initiator Event Frequency

4.4.1.1 Plant Availability Factor

The availability factor is the amount of time that the plant is able to produce electricity, estimated as the amount of time the generator is on-line ("at-power"), divided by the total time in that period.

The average plant availability factor for time window identified for the PRA can be obtained from plant reports (sometimes called Burn-up Reports) of the total time the generator was on-line, or from the (proprietary) RADS database available on the NRC operational experience website [21].

The total availability factor for the PRA database data time window can then be calculated as shown in the Table 4-3 example.

Table 4-3
Example plant availability factor calculation

Year	Hours Generator On-Line	Total Hours in Reporting Period	Availability (%)
2005	8450	8760	96.5%
2006	7500	8760	85.6%
2007	7357	8759	84.0%
Jan-08	695	744	93.4%
Total	**24002**	**27023**	**88.8%**

4.4.1.2 Calculating the Initiating Event Frequency: the Relationship Between Reactor Calendar Year and Reactor Critical Year

Note 1 to supporting requirement IE-C5 of the ASME/ANS PRA Standard [7] provides a detailed discussion on the relationship between *Reactor Calendar Years* and *Reactor Critical Years.* Due to continuing confusion between the concepts, the discussion here attempts to provide an alternate description of the same concepts.

The ASME/ANS PRA Standard [7] IE-C5 requires the initiating event frequency to be expressed per *Reactor Calendar Year* (also commonly expressed as per *Reactor-Year*, which is the terminology that will be used in the remainder of this document) in order to be consistent with the needs of Reg. Guide 1.174 (that is, for comparison to the quantitative acceptance guidelines). This represents the annual risk contribution to CDF/LERF from at power operations, and, therefore, reflects the time the plant is at power.

Some applications, however, require the analyst to consider the conditional probability of core damage/large early release given the plant is at power. One such example is a risk monitor, which uses PRA to assess the risk of the plant at a given configuration and operating state. For this application we consider initiating event frequencies in units of per *Reactor Critical Year*, or the annual frequency of the initiating event assuming the reactor is critical the entire year.

The relationship between the two metrics is:

$$F_{Calendar} = F_{Critical} * AF \qquad \textbf{Eq. 4-1}$$

where

$F_{Critical}$ = The initiating event frequency in units of per reactor critical year

AF = Plant Availability Factor

$F_{Calendar}$ = The initiating event frequency in units of per reactor-year (or per reactor calendar year)

One way to accommodate both applications is to represent the initiating event as a fault tree (Figure 4-1).

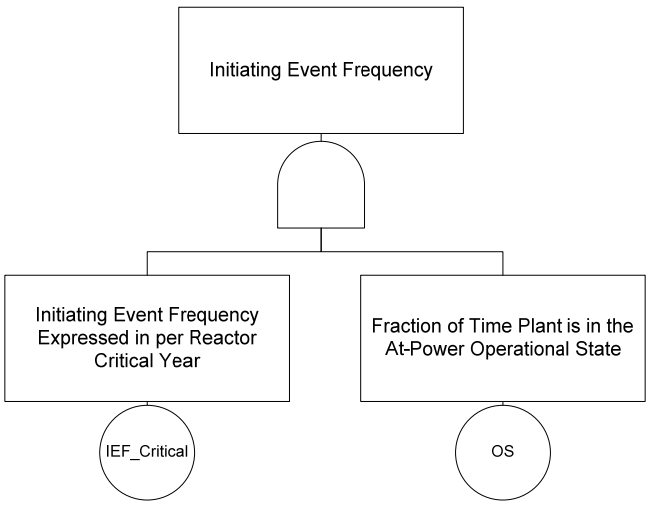

Figure 4-1
Initiating event frequency fault tree

Where the basic event IEF_Critical is the initiating event frequency expressed in per *reactor critical year*. The basic event OS is the probability that the plant is at-power. When the basic event OS is set to the plant availability factor, then the resulting initiating event frequency is calculated as per *reactor-year*, as required by the Standard. For the risk monitor application, when the plant is known to be at-power, the basic event OS can be changed to 1.0.

Calculating the Initiating Event Frequency Per Reactor Critical Year:

Generic data is generally reported in units of per *reactor critical year*. To calculate IEF_Critical the analyst needs to ensure the plant-specific data is also expressed in units of per *reactor critical year*. There are generally two categories of initiating events that will be calculated:

> Case 1: Events that can occur any time, regardless of plant operating state. An example of this type of event is a Loss of an AC or DC Bus.
>
> Case 2: Events that can only occur at a given plant operating state – in this case, at-power. An example of this type of event is Turbine Trip.

In calculating a frequency per *reactor critical year* is it helpful to think of the frequency expressed as the number of events / failure opportunities (in this case, expressed in years). Let us take for example a plant that is operating at 90% capacity for 10 years. In Case 1, if there are 3 events in 10 years, then the frequency of the event is 3/10 = 0.30 per year, because the event can happen anytime in that 10 year time frame, regardless of how much time the plant was in the at-power operating state. However, for Case 2, the failure opportunities are limited by the nature of the event (that is, can only happen while at-power), so the plant availability needs to be factored into the calculation. In this case, if there were 3 events in 10 years of operations, the "failure opportunities" would not be 10 years, because the plant was not at-power for the full 10 years and the event can only happen at-power. The number of years would actually be 90% of 10 years, which is 9 years. Therefore, the event frequency would be 3/9 = 0.33.

Calculating the Initiating Event Frequency Per Reactor-Year:

Some plants do not take the split-fraction approach illustrated in Figure 4-1, but rather calculate the initiating event frequency in units of *per reactor-year* and input that directly into the PRA as one basic event. In this case the frequency calculations for Case 1 and 2 are different that what was presented above. Because generic data is generally in units of *per reactor critical year*, the analyst must also ensure the generic data is also converted into *per reactor-year* prior to combining it with the plant-specific data; the plant's availability factor should be used along with Equation 4-1 to do this.

In calculating a frequency per *reactor-year* (a.k.a *reactor calendar year*) is it helpful to think of the frequency as the number of events that can happen while at-power in a given operational year. Let us take for example the same plant that has been operating at 90% capacity for 10 years. For Case 1, if there are 3 events in 10 years, then the failure rate is 3/10 = 0.30 events per year, BUT, because the plant is only at-power 90% of the time, the frequency of events that can happen while at-power is 0.9*0.30 = 0.27 events/reactor-year.

Case 2, however, is already limited by the nature of the event (that is, can only happen while at-power). So, if there are 3 events in 10 years, then the frequency of events that can happen while at-power is 3/10 = 0.30 events/reactor-year.

Summary

An analyst performing a PRA update should understand how their plant models initiating event frequencies and calculate the updated frequency using the appropriate method. Equation 4-1 provides the relationship between *reactor-year* (or *reactor calendar year*), availability factor and *reactor critical year*. Table 4-4 below provides a summary of formulas for how to calculate initiating event frequencies for Case 1 and Case 2 based on unit type.

Table 4-4
Initiating event frequency calculation

Initiating Event Cases	Units of Initiating Event Frequency	
	Per Reactor Critical Year	**Per Reactor Year**
Case 1	$F_{Critical} = \frac{n}{T}$	$F_{Calendar} = \frac{n}{T} * AF$
Case 2	$F_{Critical} = \frac{n}{[T * AF]}$	$F_{Calendar} = \frac{n}{T}$

where

Case 1 are events that can occur any time, regardless of plant operating state. An example of this type of event is a Loss of an AC or DC Bus.

Case 2 are events that can only occur at a given plant operating state – in this case, at-power. An example of this type of event is Turbine Trip.

n = the number of events in T years

AF = the plant availability factor

T = the number of calendar years in the data window

4.4.2 Data Driven Approach

For the data-driven approach at calculating initiating event frequencies, a plant-specific analysis is performed to determine frequencies for those initiators for which actual occurrences have been observed. Initiating event frequencies are generally considered to follow a Poisson distribution since they are based on the number of event occurrences over time and the Poisson addresses time-based failures. Events are considered to occur randomly in time with a constant occurrence rate (the initiating event frequency), meaning that there is an equal probability of an event occurring over any discrete period in time.

The Poisson distribution is very simple and the data required to estimate the parameter is the number of occurrences n in a total time t, expressed as $\lambda = n/t$. The statistical uncertainty associated with this estimate can be estimated using frequentist techniques such as those in NUREG/CR-6823 Section 6.2.1 [13].

However, because actual initiator occurrence is rare, it is unusual for a plant to have sufficient plant-specific data to quantify initiators. A Bayesian update approach is therefore generally used to combine generic data with the plant-specific data to obtain the benefits of both industry-wide and plant-specific experience. For initiating events, the Poisson-Gamma updating process can be readily used. In this case, the generic data in the form of a Gamma distribution would serve as the prior. The generic initiator data sources discussed in the next section provides industry information in terms of alpha and beta parameters for a Gamma distribution. The plant-specific information—or the likelihood function—should be expressed in the form of a Poisson distribution. Lognormal distributions have also been used in the past for initiating event. Section 3 provides more detail on the process and pitfalls of Bayesian updating using Gamma and Lognormal distributions.

The remainder of this section will discuss the inputs into the Bayesian update, including generic data and plant-specific data; for each data type, a discussion of sources and applicability is provided.

4.4.2.1 Generic Initiator Data

Generic data can be used to in the form of a prior distribution as described in Section 3 or can be used as-is for cases where there is little data (that is, initiators that are very rare events industry-wide). A summary of generic data sources for initiating events are provided in Table 4-5.

NOTE: when calculating the initiating event frequency in *per Reactor-Year*, the plant-specific availability factor should be applied to adjust the generic data. This is because the generic data is already normalized in the units of *per reactor critical year*.

Table 4-5
Generic initiator data references

Data Source Reference	Years of Applicability	Continuously Updated?	Description
U.S. NRC Reactor Operational Experience Results and Databases website [21]	FY1988-2012	Yes, yearly	Industry Average Parameter Estimates, Current Results, Detailed Data Sheets, Initiating Events. Generic BWR and PWR initiator frequency databased on operating experience as reported in Licensee Event Reports (LERs). The NRC operational experience website for the Initiating Event data http://nrcoe.inel.gov/resultsdb/InitEvent/UU9T9 provides current information updated yearly. The yearly summary includes the data totals in terms of number of events and reactor critical years and representative industry gamma and lognormal distribution parameters for each initiator frequency.
NUREG/CR-6928 [4]	Baseline periods with start years of 1988 to 1998, but all ending in 2002	No	Generic BWR and PWR initiator frequency data based upon nuclear plant experience. While this NUREG data source provides guidance and details on how the data is tabulated, the data in this source has been superseded by more current data available on the NRC operational experience website [21]. Informational note: NUREG/CR-6928 [4] may have assigned some events to more than one category as it includes both the initial plant fault and the functional impact (where applicable) in the data for development of the generic frequencies.
NUREG/CR-5750 [3]	1987 – 1995	No	Generic BWR and PWR initiator frequency data. While this NUREG data source provides guidance and details on how the data is tabulated, the data in this source has been superseded by more current data available on the NRC operational experience website [21]. Informational note: The LER data used for estimates in Appendix D has been categorized in two ways: Initial Plant Fault and Functional Impact. Appendix A of the document explains these categories in detail but the summary explanation is that each reactor trip has only one plant fault, but may have several functional impacts. The total of all initial plant fault counts is the same as the total of reactor trips.

Table 4-5 (continued)
Generic initiator data references

Data Source Reference	Years of Applicability	Continuously Updated?	Description
NUREG-1829 [46]	Based on expert elicitation	No	LOCA frequency estimates as a function of effective break size and operating time for separate generic BWR and PWR piping and non-piping passive systems. The NRC operational experience website [21] provides updates for some categories of LOCAs (for example, very small LOCAs); initiating event rates from NUREG-1829 should be used only when more current data is not available from [21]. Provides mean, median, 5th percentile and 95th percentiles of LOCA data in its Table 7.1 Total BWR and PWR LOCA Frequencies, by reactor type, LOCA size in gpm and effective break size in inches.
EPRI 3002000079 [22]	1970 through 2009	No (updated regularly, but not continuously)	Piping system failure rates for estimating internal flooding and/or high energy line break frequencies (with the exception of reactor coolant piping breaks). Section 6 of this source provides mean piping failure rates in reactor operating year-ft for various pipe sizes for non-safety-related service water system piping for PWRs and BWRs at sea, lake, and river sites. Mean piping failure rates are also provided for the following systems: fire protection, circulating water, feedwater and condensate (BWR and PWR), safety injection and recirculation, and component cooling water.
IAEA-TECDOC-719 [47]	1982-1992	No	Review of BWR, PWR, WWER initiating event categorization and data from a wide range of PRAs; includes data on rare initiators such as reactor pressure vessel rupture.

For most transients, generic data are used at face value and combined via Bayesian updating with plant-specific data to better reflect industry-wide experience. Generally, the generic frequencies do not need to be adjusted to remove any plant-specific events before performing the Bayesian update. This approach is considered acceptable due to the low number of plant-specific events and may be inordinately time consuming due to the difficulty in identifying the plant-specific events included in the generic initiator frequencies. Generic data are primarily used as-is for LOCA initiating event frequencies because there has been very little or no experience in the industry for these events. It should be noted that generic data for the reactor type being analyzed by the PRA (BWR, PWR) should be used.

Initiating event frequencies in NUREG/CR-6928, and subsequent updates provided on the NRC operational experience website, are appropriate for plant critical operation and are reported as events per reactor critical year (rcry) as shown below. The IE frequencies are characterized by gamma distributions, but lognormal parameters are also provided. The table below provides an example initiating event frequency as reported on the NRC operational experience website as an update to the data in NUREG/CR-6928. This distribution can be used as-is as a prior in a Bayesian update (see Section 3).

Table 4-6
Selected industry distribution of λ for LLOCA (BWR) as taken from 2010 update to the initiating event data sheet [21]

Source	5%	Median	Mean	95%	Distribution		
					Type	α	β
Ref. 5	1.90E-08	2.91E-06	6.78E-06	2.66E-05	Gamma	0.470	6.932E+04

Note – Percentiles and the mean have units of events/rcry. The units for β are rcry.

4.4.2.2 Plant-Specific Data

Occurrences

To tabulate the number of occurrences of each initiating event, all unplanned manual and automatic SCRAMs inside the data window of interest should be examined and binned into its relevant initiating event category. Initiating event occurrences collected from plant-specific operating experience should meet the following criteria, as cited in NUREG/CR-6928 [4]:

- Include an unplanned reactor trip
- Occur when the reactor is critical, and at or above the point of adding heat
- Are reported by a LER

The analysis of Loss of Offsite Power (LOOP) is discussed separately in section 4.5.

NOTE: The ASME/ANS PRA Standard contains specific requirements for ISLOCA frequency analysis under supporting requirement IE-C14.

Plant transient events are most often obtained from the following sources:

- Licensee Event Reports (LERs)
- Unit Transient Reports (UTRs)
- Condition Reports (CRs)
- Institute for Nuclear Power Operations (INPO) Generation Loss Events

The event documentation should be examined in detail to extract the cause and to classify the event. In some cases, only the initial plant fault that led to the plant SCRAM is considered when assigning events to the corresponding categories. Note that the generic frequencies for these transients obtained from NUREG/CR-6928 [4] and NUREG/CR-5750 [3] may have assigned some events to more than one category as it includes both the initial plant fault and the functional impact (where applicable) in the data for development of the generic frequencies. This means that the total count may exceed the number of SCRAMs.

Events that have occurred at conditions other than at-power operation (that is, during low power or shutdown conditions), and those resulting in an unplanned controlled shutdown that includes a SCRAM prior to reaching low-power conditions should be reviewed for applicability to at-power operation and if so, should be included in the initiating event data tabulation.

The following assumptions apply in evaluating initiating event data:

- The plant trips should include unplanned manual SCRAMs that otherwise would have eventually caused an automatic SCRAM.
- Planned trips are excluded from the analysis.
- Operating experience should be reviewed to identify any precursors to initiating events, as well as multi-unit site initiators.
- Data that are not considered to be applicable can be excluded, but a justification for this (for example, design or operational change) must be provided. (See Section 3.6 on model validation for information justifying data truncation.)

Plant operating experience should also be reviewed to identify precursors of initiating events. Precursor data are used to identify possible initiating events, but are generally not counted in the calculation of the initiating event frequency. The number of unplanned automatic and manual SCRAMs while critical is reported to the NRC for each reactor unit on a quarterly basis as part of the Performance Indicator program [21]. These events should also be discussed with plant personnel to clarify their impact in terms of plant response. Table 4-7 provides a list of plant-specific data sources.

NOTE: The ASME/ANS PRA Standard specifically requires that plant personnel be interviewed to determine if plant-specific initiating events have been overlooked. Documentation of these interviews is important for verifying that supporting requirement IE-A8 has been met.

Table 4-7
Plant-specific data sources

Data Source Reference	Years of Applicability	Continuously Updated?	Description
Licensee Event Report Search (LERSearch) [48]	1980 to present	Yes	Searchable on-line database of individual LERs. Searchable by several fields including date range, specific plant, reactor type or LER number
North American Electric Reliability Corporation (NERC) Generating Availability Data System (GADS) [49]	1978 to present	Yes, information is reported to GADS quarterly	Utilities are required to report Event, Performance and Design data to GADS. Unit time information that is reported includes planned, unplanned and maintenance outage hours
Institute of Nuclear Power Operations (INPO) INPO Plant Events Database [50]	1980 to present	Yes, events are reported to INPO	Utilities report Operating Experience and Condition Reports to INPO. OEs include SCRAMs with narrative discussion of what occurred. INPO reviews and categorizes events as Significant Events, producing SERs, SOERs and SENs.

Time Frame

In order to calculate the plant-specific failure rate, the total number of reactor critical hours over the data window is needed. This data is routinely collected by plants and is reported to the NRC and to the North American Reliability Council (NERC) Generating Availability Data System (GADS) [49] in terms of the number of hours of critical operation in the previous quarter.

The GADS database includes all reactor power perturbations and shutdowns since 1978, and mandatory GADS reporting started in January 2012 for all conventional generating units 50 MW and larger. The reactor critical hours for a calendar year are then summed from January through December and divided by 8760 hours to express the data in units of reactor-critical year.

An example of this process is shown in Table 4-8.

Table 4-8
Example reactor critical year calculation using GADS data

Year	Month												Total
	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	
1995	744	300	5.5	650	744	720	710	744	720	745	720	744	7546.5
1996	744	696	744	719	622.5	720	744	744	215.5	185.3	720	744	7598.3
1997	744	672	744	719	744	720	744	744	720	745	720	744	8760
1998	575.1	672	640	0	565.7	720	744	744	720	745	720	586.2	7432
1999	626	672	744	719	744	720	744	744	235.2	489	700	744	7881.2
2000	645.2	105	398	719	744	720	744	744	720	745	720	744	7748.2
2001	684.7	696	384	524.5	744	720	698.6	744	720	745	720	744	8124.8
2002	744	696	744	719	744	720	744	744	720	96.1	616.5	744	8031.6
2003	744	696	744	719	744	720	744	686.5	706.3	745	325.2	485.3	8059.3
2004	744	696	744	480	435.7	532.4	744	744	720	745	720	744	8049.1
2005	744	696	744	719	744	720	744	744	720	94.3	0	133.1	6802.4
2006	744	696	744	719	744	720	522	744	720	745	720	744	8562
2007	744	696	743	512.4	308	720	744	744	720	744	721	744	8140.4
2008	744	696	743	720	744	720	744	744	720	745	720	744	8784
TOTAL REACTOR CRITICAL HOURS FROM 1/1/95 – 12/31/08													**111519.8**
REACTOR YEARS (reactor critical hours/8760 hrs per year)													**12.73**

4.4.2.3 Data Window and Applicability

The initiator data analyst needs to establish the official timeframe for which data will be collected, otherwise known as the data window. The earliest date will depend upon the last data update that was performed. For example, if the previous data set included data collected through the end of December 2009, then the start date of the data window for the current data update project is 1 January 2010. The end date of the data window is usually the most current month for which the number of events and the reactor critical hours have been logged and documented. It may be wise to have the data window lag by one or two months from the current date to ensure that all information has been entered into the plant computer system.

Consistency in the data window across the entire PRA update used to be the convention, although some plants have chosen to select data windows for the different data elements (initiating events, component failure data, unavailability data) depending upon issues that would impact the continuity of the database. For example, start dates for data in NUREG/CR-6928 [4] vary by initiating event, depending upon the relative frequency of the event and whether a trend exists. The initiating event data window should be documented for reference in the PRA initiating event data notebook.

Both the generic data and the plant-specific data needs to be reviewed for applicability and inclusion into the data analysis. The generic data is usually taken as-is, but may be modified if there is an industry-wide trend that warrants an adjustment.

Plant-specific data should be examined to see if there are outliers that should not be included in the data set. In general, when considering if the data is applicable, the analyst should consider the likelihood of the initiator (frequent, sparse or not observed in the industry) and whether a trend exists. It may appropriate not to use older plant operating experience in calculating the reactor trip frequency due to improvements in plant performance or major plant modifications. However, for rare events, such as small break LOCAs, the use of a longer data window may be appropriate. In addition the reactor trip history should consider the occurrence of major plant modifications and upgrades.

One example of adjusting the data window shown in Figure 4-3 is taken from a reference plant: Data prior to 1987 shows a significant number of plant trips associated with a young nuclear industry. In comparison, the data after 1987 shows a significant reduction that can be attributed to significant improvements and changes made in industry, including replacement of the steam generators in 1984 with some break-in period in the two years that followed and other industry-wide improvements in maintenance and operation. NUREG/CR-6928 [4] and NUREG/CR-6890 [5] discuss major culture changes in the industry associated with this trend. This is consistent with culture changes that started in the early 1990s at the reference plant that emphasized nuclear production and efficiency, especially in view of potential industry electric grid deregulation. A number of programs can be directly attributed to the improvements in performance, including trip reduction programs, weeding out the plant work backlogs and workarounds, implementing a ‘fix-it-now’ program and teams, and maintenance rule implementation. In addition, operations staffs have become more seasoned and the industry as a whole communicates operations experience and lessons learned more effectively. Based on the improved performance since 1997, the plant in question chose to exclude prior years in the estimations of future performance, as reflected in the

initiating events data. The data range starting in 1997 is compared to the time windows presented in NUREG/CR-6928 [4] and NUREG/CR-6890 [5] for historical reference of the performance improvement trend. Figure 4-3 provides a graph of the general transient events over time at the reference plant; Figure 4-4 provides the same information over the industry (PWRs).

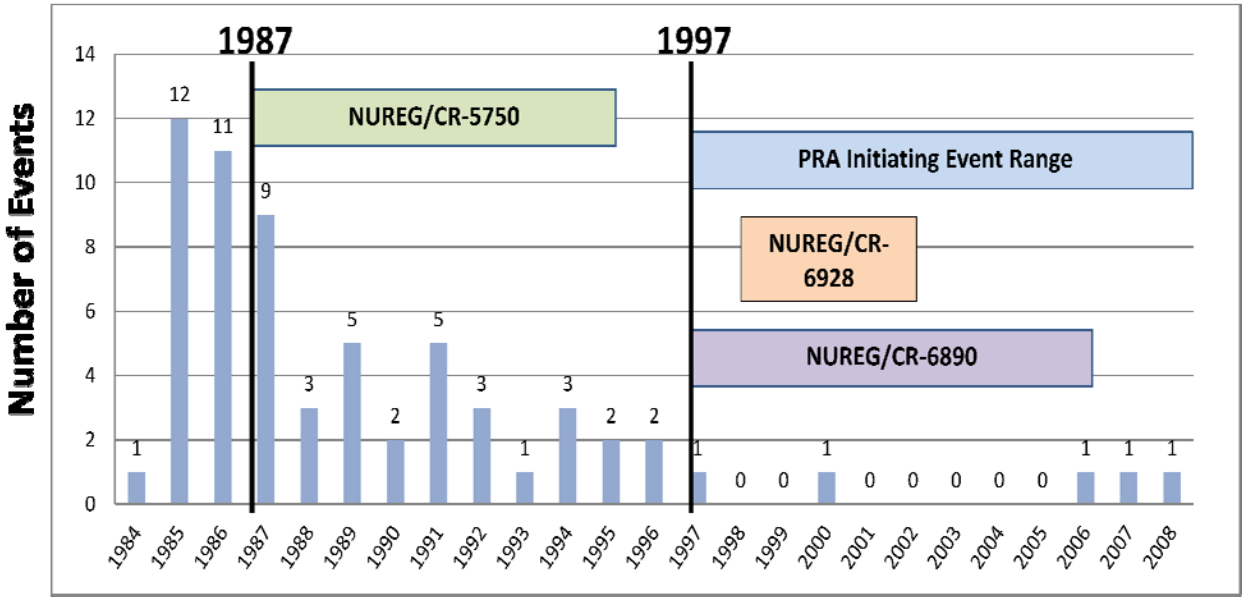

Figure 4-2
Example reactor trip history at reference plant

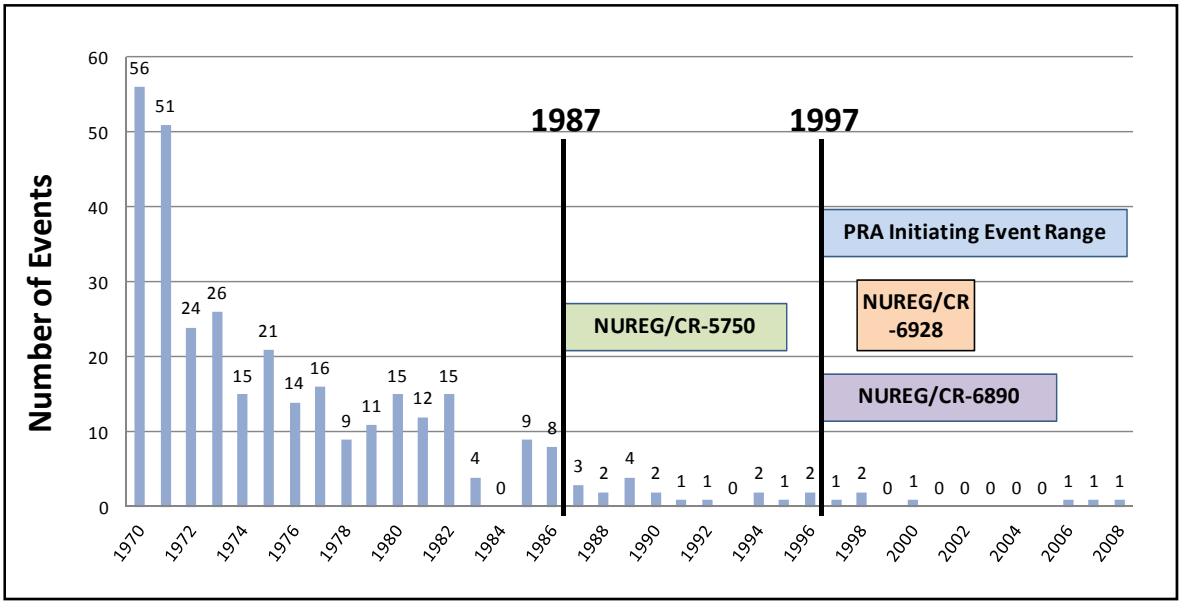

Figure 4-3
Example frequency of PWR initiating events (as compiled by the reference plant)

Some evaluations can be made on a heuristic basis, such as to remove the first few years of operation to address early burn-in failures, end of life (aging) failures, or to count experience accumulated after a major component replacement in a system. Even though judgment is involved in establishing the data window, if a case is being made for justifying one selection vs. another, the important issues that need to be considered for initiating events are:

- Operations status – major outages, frequency of maintenance, extended power uprate
- Equipment status – system upgrades and equipment replacements that could impact reliability, effects of aging or early burn-in

When performing this evaluation, care needs to be taken not to discard data where the data is very sparse or there is insufficient data to determine a trend; in these cases, the strength of the qualitative justification for discounting data needs to be much higher. Section 3.6 provides additional guidance on how to assess outliers. The Initiating Event Summary provided on the NRC operational experience website [21] provides some industry trending data for IEs. MSPI tracks trends and should be able to reveal the differences between data trends from one timeframe vs. another. INPO tracks industry wide trends and provides this data to its members [50].

Finally, when the calculations have been performed, transient and special initiator frequencies should be compared with the generic NUREG/CR-6928 [4] or NUREG/CR-5750 [3] frequencies, as well as any reactor type Owner's Group frequencies, to confirm that the values are reasonable and consistent. Any inconsistencies should be able to be explained and the explanations included in the Initiating Event Data Notebook for the PRA.

4.4.3 Fault Tree Approach

For cases where there is insufficient data or the initiator type is unique and plant-specific, or when PRA applications are anticipated that require that changes or impacts to support systems that can produce initiating events be accurately modeled, initiators can be quantified using fault trees, rather than via frequency calculations. In these cases, a fault tree is used to break the initiator down into the system and component level contributors, in the same way as the overall PRA model fault tree does. The component failure basic events for the initiator fault tree would be quantified as discussed in Section 5 and the overall initiator frequency entered into the PRA model, as coordinated with the PRA accident sequence analysis task.

Note that for risk monitor Maintenance Rule a(4) applications, for example, it is desirable to allow these initiating event frequencies to be calculated dynamically as the model is quantified so that it may reflect the actual plant configuration and component unavailability at the time of the analysis. In this case, rather than a summary-level basic event, the entire initiating event fault tree may be included in the PRA model, or other means may be provided to allow the fault tree-based initiating event frequencies to be dynamically solved and incorporated into the PRA model at run-time. When not being used for the risk monitor application, a baseline set of system alignments and annual average maintenance and testing unavailability values are used in these fault trees to obtain a static initiating event frequency for each calculation.

4.5 Loss of Offsite Power (LOOP)

Loss of off-site power is the simultaneous loss of electrical power to all unit safety buses (also referred to as emergency buses, Class 1E buses, and vital 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. LOOP is therefore an important contributor in almost every plant-specific PRA. When considering LOOP, there are generally four types of data that are needed:

1. LOOP initiating event frequency (events that can initiate an accident sequence)
2. Conditional probability of a LOOP given a reactor trip that occurred for another reason
3. Probability of power recovery as a function of time after loss
4. Conditional probability of a LOOP given certain maintenance activities (that is, adjustment factors for use in risk monitors)

There is currently no standard industry approach for calculating the above probabilities and frequencies for LOOP; future EPRI guidance is expected to address this, so specific guidance is not provided here. However, some background information is provided for context.

The LOOP initiator is defined by four categories of event types:

- Plant-centered (for example, failures of main or startup transformers, relaying, breakers, and so on)
- Switchyard-centered (may affect multiple units at a site)
- Grid failures
- Weather-related (may overlap with evaluation of external events)

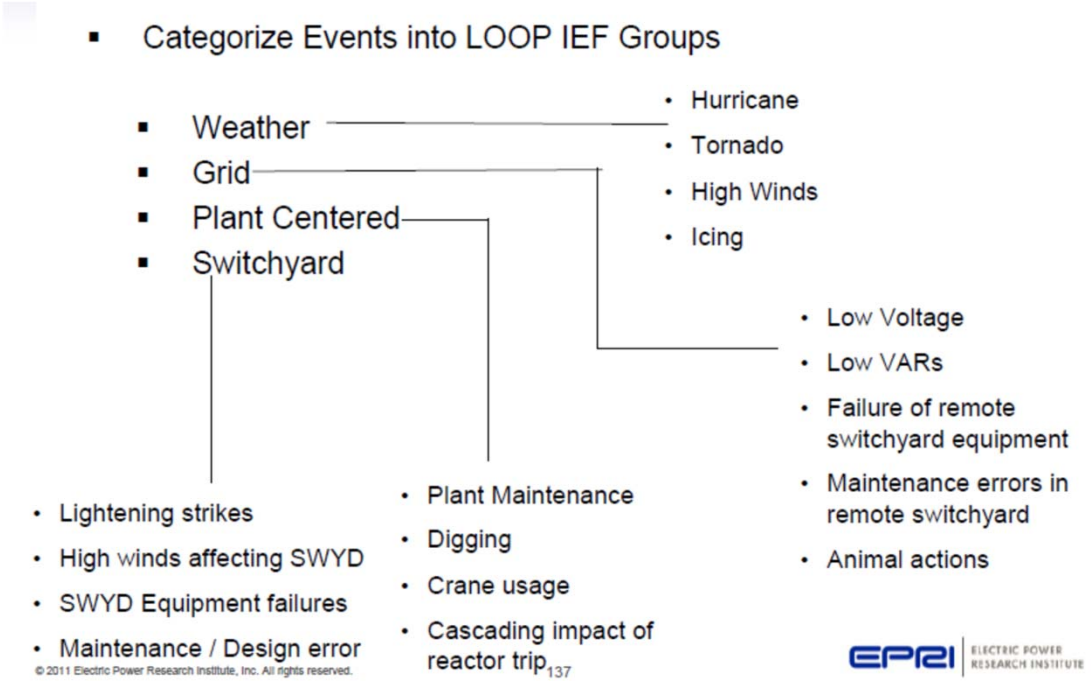

Figure 4-4
LOOP event categorization [9]

The two major sources of LOOP data are NUREG/CR-6890 [5] (and subsequent data updates on the NRC operational experience website [21]) and the EPRI LOOP report series [23–33] summarized in Table 4-9. The NUREG and EPRI reports report the same data, but use different classification schemes to categorize the LOOP data based on relevant characteristics; Table 4-10 summarizes the classification scheme used in the two sets of data.

Table 4-9
LOOP data references

Data Source Reference	Years of Applicability	Continuously Updated?	Description
NUREG/CR-6890 [5]	1986-2004	Updates available on website	LOOP data through 2011 available on website: http://nrcoe.inel.gov/resultsdb/LOSP/
EPRI 3002000697 [23]	2012	No	LOOP events for the year 2012 and event summaries for the ten-year period 2003 through 2012
EPRI 1025749 [24]	2011	No	LOOP data for 2011; limited overview data and analysis for the 10-year period 2002 through 2011
EPRI 1023147 [25]	2010	No	LOOP data
EPRI 1021508 [26]	2000–2009	No	LOOP data
EPRI 1013239 [27]	1996-2005	No	LOOP data
EPRI 1011764 [28]	2004	No	LOOP data for 2004; limited overview data and analysis for the 10-year period 1995 through 2004
EPRI 1009889 [29]	1994-2003	No	LOOP data
EPRI 1000158 [30]	1988-1999	No	LOOP data
EPRI TR-110398 [31]	1984-1997	No	LOOP data
EPRI TR-106306 [32]	1980-1995	No	LOOP data
NSAC-194 [33]	1980-1992	No	LOOP data

Table 4-10
NUREG and EPRI report LOOP classifications

Category	Description
NUREG/CR -6890 Classification	
LOOP-SD	LOOP occurs while a plant is shutdown.
LOOP-NT	LOOP occurs during critical operation, but the plant is able to continue without a plant trip.
LOOP-IE-I	LOOP occurs during critical operation; LOOP event causes a reactor trip.
LOOP-IE-C	LOOP occurs during critical operation; reactor trip causes a LOOP to occur.
LOOP-IE-NC	LOOP occurs during critical operation; reactor trip and LOOP both occur during the same transient, but are unrelated.
NUREG/CR-6890 data is further binned into the four LOOP categories of plant-centered, switchyard-centered, weather related and grid related.	
EPRI Classification	
Ia	No offsite power available to the safety buses for 30 minutes or longer.
Ib	No offsite power available to the safety buses for up to 30 minutes.
IIa	With the unit online, the startup/shutdown sources of offsite power for the safety buses become de-energized. During these events, the main generator remains online (connected to the offsite grid) and power for the safety buses is available from a unit auxiliary transformer.
IIb	With the unit online, the startup/shutdown sources of offsite power for the safety buses remain energized but in question. There is low or unstable grid voltage, or such a condition could result if the unit were to trip or tripped coincident with a LOCA and emergency safety feature actuation. During these events, the main generator remains online (connected to the offsite grid) and power for the safety buses is available from a unit auxiliary transformer.
III	The unit auxiliary source of power for the safety buses becomes deenergized or unavailable, but offsite power for the safety buses remains available, or can be made available, from a startup/shutdown source. Connection to this source may require a fast or slow automatic transfer, or manual switching from the control room. Category III does not include events in which a loss of power from the unit auxiliary source results from a unit trip. To fall in Category III, the loss of power from the unit auxiliary source must be the initiating event and must precede the unit trip. A Category III event is most often associated with a failure of main electrical power hardware that makes near-term availability of the unit auxiliary source of power for the safety buses unlikely.
IV	No offsite power available during cold shutdown because of special maintenance conditions that do not occur during or immediately following power operation.

LOOP initiating event frequency

The LOOP initiator frequency development process [9] can be summarized as follows:

1. Select relevant period of operating experience
   a. Operation since de-regulation of utility operations
   b. Most recent operating period (for example, 10 or 20 years)
2. Determine relevant mode of operation (at-power, shutdown)
   a. Some events would only have occurred during shutdown conditions
   b. At-power PRA should examine events to identify those that:
      i. Occurred at power operation
      ii. Would be relevant irrespective of operating mode
3. Review generic data for events that fit the period of interest and operating mode and examine for applicability to plant. Some data may need to be discounted based on:
   a. Unique configurations (for example, number of grid connections to switchyard)
   b. Unique weather conditions, for example:
      i. Relevance of ice storms to plants in Florida
      ii. Relevance of hurricanes to plants in the midwest
   c. Regional differences
      i. For example, was event of August 13, 2003 relevant to other regions of the country?
4. Categorize events according to plant-specific relevance
5. Categorize events as single-unit or site-wide
6. Calculate frequencies relevant to the plant under consideration
   a. Consider appropriate units (per reactor-year v. per reactor critical year)

When reviewing generic data for applicability to the plant under consideration, some events may need to be reclassified because of differences between the plant that experienced the event and the plant which the data is being calculated for. In some cases, to get the necessary detail to make the determination, the analyst may have to go back to the LER associated with a given entry. Below are two examples where events would have to be reclassified due to plant differences:

- At some plants, a single startup transformer is available to supply offsite power to plant auxiliaries in the event of a loss of the normal supply (for example, from the main generator via an auxiliary transformer). For example, Plant X has two startup transformers, which normally supply separate main power buses (buses A and B). In the event that power is not available from one of the transformers after a trip, the buses it was set to feed automatically transfer to the other transformer (either can supply all of the plant's auxiliary loads).

Therefore, events at other plants involving loss of offsite power due to loss of a single startup transformer were evaluated on a case-by-case basis to determine whether or not they could constitute actual losses of both startup transformers at Plant X. If it could be determined that at least one of the startup transformers should have been unaffected if the event were to have occurred at Plant X, the event was not considered to be a loss of offsite power.

- All offsite power to Plant Y is supplied through one switchyard. Events at other plants in which the normal offsite power supply was lost but a reserve source from another switchyard (or from another unit at the site) remained available were generally reassessed to be total losses of offsite power for Plant Y.

Conditional Probability of a LOOP Given a Reactor Trip

The second category of data of interest is the conditional probability of a LOOP given a reactor trip. There are potential dependencies between reactor trip and LOOP, for example, in some cases a reactor trip can produce a sufficient disturbance in the grid to cause a LOOP. This is why it is useful to derive a conditional probability using data when available.

To do so, the LOOP data needs to examined, and LOOP events where a reactor trip causes a LOOP to occur (LOOP-IE-C, in the NUREG/CR-6890 [5] nomenclature) should be parsed out and examined for relevance to the plant under consideration. This provides the numerator. The denominator requires the analyst to determine the relevant number of trips for each operating unit in the database. Note: low-power trips may be less likely to affect offsite power (for example, for power levels below ~15%, the main generators are not typically online at most plants). If these are included in the data, the conditional probability may be underestimated.

Probability of Power Recovery

Some data is available to inform the probability of power recovery within a defined timeframe of interest. The EPRI LOOP reports [23–33] provide some data on duration of the LOOP. If these data are used to construct or inform a distribution, the analyst should take care to understand which data are applicable to their plant site. For instance, if for a given event recovery was accomplished via a backup source for which no equivalent source exists at the plant being analyzed, the analyst should consider discounting that data point or using the duration associated with restoration of normal offsite power.

Use of Adjustment Factors for LOOP Probability in Risk Monitor Applications

Certain conditions can cause an increase or decrease in the probability of a LOOP over a particular time frame (that is, during periods of expected adverse weather, switchyard maintenance, and so on). For online risk management purposes it is useful to understand what these conditions are and to what extent they can affect the probability of a LOOP. For example, adverse weather conditions can increase the probability of a LOOP. Similarly, certain types of maintenance activities, particularly in the switchyard, can cause an increase in the probability of a human-induced LOOP. There is currently no standard industry approach at calculating adjustment factors for use in risk monitors. However, EPRI 3002000414 [34] provides a methodology for calculating adjustment factors for plant-centered and switchyard-centered LOOPs for various maintenance activity types.

4.6 Standard and Regulatory Requirements

RG 1.200 [8] cites the following Technical Characteristics and Attributes for Initiating Events Analysis:

- Sufficiently detailed identification and characterization of initiating events
- Grouping of individual events according to plant response and mitigating requirements
- Proper screening of any individual or grouped initiating events

A Note is also provided, as follows: "It is recognized that for those new reactor designs with substantially lower risk profiles (for example, internal events CDF below 10^{-6}/year) that the quantitative screening value should be adjusted according to the corresponding baseline risk value." However, no specific guidance is available on what that adjustment should be.

ASME/ANS RA-Sa–2009 [7] contains the following high level requirements (HLRs) in the area of internal Initiating Event analysis:

- HLR-IE-A – Identification
- HLR-IE-B – Grouping
- HLR-IE-C – Frequency Estimation
- HLR-IE-D – Documentation of the initiating event analysis shall be consistent with the applicable supporting requirements

Key points from the PRA Standard related to initiating event data have been highlighted in the chapter text in boxes.

4.7 Guidance per Findings and Experience

Peer reviews have been and continue to be conducted to evaluate the technical adequacy of Internal Events PRAs against the ASME/ANS PRA Standard in the technical element of data analysis. The following issues reflect findings that have been made in recent PRAs in the chapter topic area and recommended guidance based upon finding recommendations and PRA data practitioner experience.

1. EPRI Support System Initiating Events: Identification and Quantification Guideline

   From Westinghouse: Would it be defensible to adjust the alpha factors for a Support System Initiating Event (SSIE) CCF group by the allowed outage time for the initial failed component? The SSIE guideline only provides this option for the average repair time and most plants do not have enough data to support an average repair time calculation. Using the 8760 hour initiating event failure rate in an SSIE tree is too high and the results of just the CCF failure can be higher than industry average for loss of that system.

   Response: This issue will be addressed in what will ultimately be a new EPRI report addressing SSIE. Until new guidance is issued, EPRI 1016741 [51] is considered applicable.

2. Weighting of initiating event frequencies per ASME/ANS PRA Standard SR IE-C5

   Finding: Not met since the frequencies were not weighted by the fraction of time the plant was at power. SR requires that the initiating event frequencies be weighted by the plant availability.

   Recommendation: This SR has come under protest and scrutiny, but as it stands, it requires initiating event frequencies to be weighted by the availability factor and therefore should either be done or it will be assessed as not met. Section 4.4.1.2 provides guidance on how to perform this calculation and suggestions on how to incorporate it into the PRA.

3. Generic initiating event consideration per ASME/ANS PRA Standard SR IE-D2

   Finding: NUREG/CR-6928, the source for generic initiating event data, addresses Partial Loss of Service Water and Partial Loss of Component Cooling Water. However, the PRA does not address these potential initiators.

   Recommendation: Evaluate plant-specific events and generic experience and provide detailed justification for any initiators that are screened.

4.8 Research Areas Under Development

There are three areas of research under development relevant to initiating events:

- INL is investigating the impact of uncertainty (both aleatory and epistemic) on estimated probabilities of recovering from LOOP within a specified time window.
- EPRI is working on a guideline for estimating LOOP initiating event frequencies using industry data.
- EPRI is working on a revision to the 2008 SSIE identification and quantification guideline 1016741 [51].

5
COMPONENT FAILURE DATA

5.1 Introduction

This chapter covers the definition, collection, and calculation of component failure data. The main sources of component failure data are plant-specific data from actual operating experience and generic data that compiles information across plants and even across other industries. This chapter covers how and when they are used.

5.2 Data Definition

The purpose of component-level data analysis is to provide reliability information for logic model quantification at the appropriate level agreed upon by the systems and data analysts. To do this, it is necessary to clearly define component types, boundaries, and failure modes. The system analysis fault tree basic events identify the component and failure mode combinations requiring data, and the analysts' descriptions provide an understanding of the component operating environments. In response to these identified data needs, the data analysts compile data at the component failure mode level for input to the fault tree models. However, this is best achieved via an iterative process between the system and data analysts to ensure that all basic events are properly quantified with appropriate failure data estimates.

The methodology for component failure data development includes plant-specific data collection and analysis, including information on component failures (failure rate numerator), and the demands or run times experienced by the components (failure rate denominator). In addition, generic data is accessed from published data sources to supplement or complement the plant-specific data.

5.2.1 Component Boundary Definition

The boundary definition task is closely connected with the tasks of defining systems boundaries and fault tree construction. Therefore, this task is performed jointly with the system analysts.

A component boundary defines what is considered to be contained within the component type and what is not, so that the subcomponents and piece parts that can contribute to component failure are appropriately considered. It is necessary to define component boundaries to support the data analysis so that the data analysis and systems analysis are working from the same premises. The PRA model and the data collection should be coordinated so that the boundaries of the components are defined similarly. Component boundaries are often established based on the guidance in NUREG/CR-6928 [4] or NUREG/CR-6823 [13], and the generic data sources. It is necessary to ensure that the component boundary definitions used in the generic data sources are compatible with the boundary definitions used by the PRA team.

Failure to carefully define and observe component boundary definitions can result in system models that do not provide a true reflection of the system reliability. Boundaries must be set low enough that the PRA model is able to provide significant insights regarding individual components, but not so low that the ability to obtain accurate plant-specific and generic data for modeled components is compromised. When quantified, a system logic model (which may contain numerous individual component models) should provide results that align satisfactorily with the actual, observable reliability level of the system,

For example, all pieces of a motor-operated valve (MOV) are typically considered to be part of a single "component" when collecting reliability data even though the valve consists of various piece parts (for example, electric motor, gearbox, limit switches, torque switches, reversing contacts and coils, stem, disc, valve body, and so on) that may be separately identified in the plant maintenance records. PRAs typically do not model failures of every switch, relay, or contact in a control circuit of a pump because that type of detail is difficult to obtain from the plant data. Instead, failures of these components are included with actual failures of the pump to establish a pump failure rate.

The boundaries of a component generally include all subcomponents specific to the component. However, the component boundary does not include piece-parts that are shared with other components modeled in the PRA. For example, the component boundary for emergency-actuated valves commonly includes the valve control circuit. However, the components needed to generate the actuation signal that initiates multiple components modeled in the PRA are not included as part of that specific valve boundary. Similarly, a diesel generator boundary will typically include the fuel day tank, but the fuel oil transfer pumps are not included since they are required for operation of all the diesel generators (unless they are dedicated pumps, in which case they should be included in the component boundary).

An example of the component boundaries for the NUREG/CR-6928 [4] generic components is included in Table 5-1 and a visual representation of a component boundary from the OREDA Handbook [40] is shown in Figure 5-1.

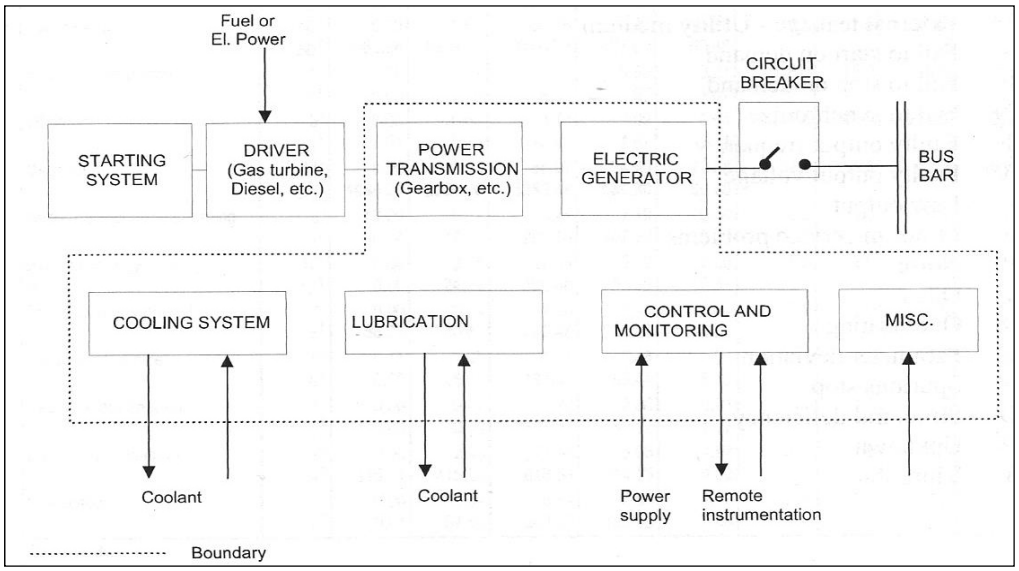

Figure 5-1
Component boundary diagram example

Table 5-1
NUREG/CR-6928 component boundary examples

Component Type	Component Boundary Definition
Air-Operated Valve (AOV)	The valve, the valve operator (including the associated solenoid operated valves), local circuit breaker, and local instrumentation and control circuitry.
Circuit Breaker	The breaker itself and local instrumentation and control circuitry. External equipment used to monitor under voltage, ground faults, differential faults, and other protection schemes for individual breakers are considered part of the breaker.
Electrical Bus	The bus component itself. Associated circuit breakers and stepdown transformers are not included.
Emergency Diesel Generator (EDG)	The diesel engine with all components in the exhaust path, electrical generator, generator exciter, output breaker, combustion air, lube oil systems, fuel oil system, and starting compressed air system, and local instrumentation and control circuitry. However, the sequencer is not included. For the SW system providing cooling to the EDGs, only the devices providing control of cooling flow to the EDG heat exchangers are included. Room heating and ventilating is not included.
Heat Exchanger	The heat exchanger shell and tubes.
Turbine-Driven Pump	The pump, turbine, governor control, steam emission valve, local lubrication or cooling systems, and local instrumentation and controls.

5.2.2 Component Type Identification and Grouping

Component types and failure modes are initially identified based upon a listing of the components considered to be likely to be encountered in the analysis. This list is compiled from expertise in database development and familiarity with general component requirements in a variety of facilities. As the fault tree modeling progresses, this list is augmented and tailored to the specific components included in the PRA models based on the plant design.

Correspondingly, it is necessary to develop an active component and failure mode coding scheme that is consistent with the fault tree model basic events, the needs of the fault tree models, as well as with standard plant naming conventions for equipment types.

Data analysts should coordinate the basic event naming conventions up front with the fault tree modelers to allow events to properly reflect the component types and failure modes and to allow the fault tree modeling software to properly access the data via the component failure mode coding scheme.

5.2.2.1 Component Type

Component type refers to the equipment category for which data is required by the logic model and at which data will be developed by the data analyst. Examples of such component types are motor-driven pumps, diesel generators, and heat exchangers. For certain complex components, a larger component type may be broken down by the system analyst in the logic model into constituent component types, including motive and passive equipment, not only to facilitate the data analysis but to evaluate the contribution of various subcomponents to the overall component failure.

NOTE: The ASME/ANS PRA Standard supporting requirement DA-B1 indicates that components should be grouped according to type and the detailed characteristics of their usage to the extent supported by data, including mission type (for example, standby, operating) and service condition (for example, clean versus untreated water, air).

The exception to this is identified in SR DA-B2, which states that outliers should NOT be included in component groups (such as valves that are never tested and unlikely to be operated with those that are tested or otherwise manipulated frequently).

To clarify further what is stated in the note box above, according to IEEE Std. 500-1984 [52], "The reliability of an item tends to increase as the applied stresses (such as electrical, mechanical, and environmental) decrease and vice versa." Consideration should, therefore, be given to the different stresses placed upon components from one system to the next that might require failure data to be calculated separately. For example, equipment that is primarily in standby is generally calculated separately from continuously operated equipment because of the difference in failure modes (failure to start versus failure to continue to run). But the conditions experienced by the equipment may also influence the failure causes and therefore the failure rate.

Environmental factors such as humidity, vibration, and external temperature can have an influence on a component's reliable performance and should therefore be treated separately when applying generic data.

Several published data sources, such as the Guidelines for Process Equipment Reliability Data by the AIChE [53], Offshore Reliability Data Handbook [40], the Savannah River Site Generic Database [54] and the Nonelectronic Parts Reliability Data book NPRD-95 [38] separate failure data on the basis of the medium exchanged, such as water, chemical process, oil, or gas, or the application environment from which the data were obtained.

5.2.2.2 Failure Mode

Failure mode is defined as an undesirable component state (for example, normally closed MOV does not open on demand because of valve mechanical damage that occurred before the demand itself) and characterizes the specific manner or method of failure of the component resulting in a loss of function. Failure modes are equipment specific and generally categorized as time or demand-based calculations. They can also be considered as sub-categories under the Severity classifications identified in Section 5.2.4. NUREG/CR-6823 [2] Section 5.2.3 provides guidance on the allocation of plant-specific events to each component failure mode of interest.

Examples of valve failure modes, originally developed during the In-Plant Reliability Database (IPRD) project (NUREG/CR-3154 [55], currently out of print, and data tables cited in [35]) are presented in Table 5-2.

Table 5-2
Valve failure modes (from Table 3, NUREG/CR-3154 [55])

Failure Mode Summary	Time/Demand Related
1 – Catastrophic	
A. Fails to Operate	Demand
a. Normally open – fails open	
b. Normally closed – fails closed	
B. Spurious Operation	Time
a. Normally open – fails closed	
b. Normally closed – fails open	
C. Plugged	Time
D. Leaks through (disabling internal leakage)	Time
2 – Degraded	
E. Improper Operation (operates out of specification)	Time
a. Premature operation	Time
b. Delayed operation (operates out of spec)	Time
F. Leaks through (debilitating internal leakage)	Time
3 – Incipient	
G. External Leakage	Time
H. Faulty indication and other failure modes	Time
I. Plugged (partial)	Time
J. Chattering	Time
K. Fails to Reclose	Time
L. Small external leakage/weepage	Time

5.2.2.3 Grouping and Outliers

The decision to include versus exclude events and failures that could be considered outliers requires some further evaluation of the available data both from a qualitative and quantitative standpoint. Some evaluations can be made on a heuristic basis, such as to remove the first few years of operation to address early burn-in failures, end of life (aging) failures, or to count experience accumulated after a major component replacement in a system.

NUREG/CR-6823 [13] Section 5.2.2.1 on Event Screening has the following advice:

> One consideration in the identification of plant-specific data is whether design changes have been made to the plant or its components that invalidate some of the historical data. For example, changing the type of flow controller could impact the operation of a particular turbine-driven pump. Thus, the total historical count of the turbine-driven pump events is not valid for the current condition of the plant. Typically, the turbine-driven pump data prior to the design change would be deleted from the data analysis. However, this has the undesirable impact of reducing sample size. Another approach is to investigate whether there is indeed a significant difference in the fraction of events before and after the design change. Not all the failures may be invalidated by the design change and so the historical data prior to the design change implementation may have partial validity and could be included in the data analysis.
>
> Consideration of design changes is one example of where censoring of data can and should be performed. Other reasons can be used for data censoring if they are well supported and valid. For example, it is not uncommon to eliminate data from the first year of plant operation since it represents failures that occurred during the plant break-in period. However, any data censoring should be approached carefully to avoid losing important information and biasing results (eliminating the first year of data actually makes the results less biased).

Graphs can be used not only for plotting reactor trip history, but for plotting failures by date of occurrence for a given component and noting the distribution of the failures along that timeline. Bunching of failures in the early and late stages may be indicative of burn-in and aging failures, but—as discussed in the excerpt above—should not necessarily be dismissed.

Decisions on which events or failures to include vs. exclude becomes particularly important when analyzing infrequent items such as initiating events or infrequently operated components, because the exclusion of a single data point could be statistically significant.

Decisions made to include vs. exclude data should be documented with a clear explanation and identified in a separate section of the Data Notebook as uncertainty contributors and sensitivity analysis topics to be carried forward to the Uncertainty/Sensitivity Analysis.

For example, if it is known that certain systems experience significantly different environmental conditions, such as extreme external factors (heat or radiation), or conduct different media of exchange (for example, borated versus clean versus salt water) or are safety related systems vs. non-safety (for MOVs), it is worthwhile to calculate component failure rates/probabilities at the system-level and compare them to a total component failure rate/probability across plant systems, and to generic data considered for use as prior distributions in a Bayesian update.

In general, as the analyst reviews maintenance and repair records to classify them for use in the PRA data set, it becomes apparent which equipment fails more frequently than others in its same type classification (for example, MOVs). Calculation of system-specific data and performing comparisons will allow the systems with notably different failure rates to be identified. NRC Maintenance Rule records system functional level trends, which could be due to more than just individual component level variability, but could provide insights to system-specific data differences. On-line industry wide databases such as RADS and EPIX provide the user with the ability to perform trend analyses.

If the difference between the system-specific and overall plant data (for example, the measured reliability of service water system MOVs vs. all MOVs plant-wide) is significant (two orders of magnitude apart), then grouping would misrepresent the distinct failure history of the individual system. If the individual system data are inconsistent with the generic prior, then conducting a Bayesian update with those values would be inappropriate. Comparisons between failure data can be made by visual comparison of failure distributions, engineering judgment or by statistical test. These comparisons are discussed in more detail in Section 3.6; particularly the example in Section 3.6.2 provides a simple method understand the effect of outliers in the update process and how a specific statistical test can be practically used to update a prior when the data suggests there might be an outlier.

Often when compiling plant-specific data, the analyst will note that one component may be notably worse in terms of failure history than the others of a similar type (whether within or across systems). These insights are valuable beyond the data analysis alone and should be discussed with plant personnel to identify whether operational conditions or preferences are driving these differences.

Significant differences in data warrant the development and quantification of a separate type code and failure mode to represent the unique plant-specific operational history. Further, a more appropriate prior should be selected for use in a Bayesian update. This may be a challenge since fewer generic data sources reflect the operating condition factors cited in PRA Standard SR DA-B1; therefore, it may be appropriate to use the plant-specific data by itself.

5.2.3 Basic Event Naming

PRA projects use a detailed and comprehensive basic event naming scheme. Component basic event names typically include coding for system identification, component type, failure mode and the equipment database label. For example, the BE name LPI-HTX-RP-E35A gives the system (LPI), component (HTX), failure mode (RP) and equipment ID number (E35A). Other events, such as human actions, common cause events, and initiating events also need to be easily distinguishable.

Conventions are required for the component type and failure mode, and depend upon the software being used. For example, Computer-Aided Fault Tree Analysis (CAFTA) [56] employs an alphanumeric code of user-defined length for the component type, called the Type Code (TC) and another alphanumeric code for the Failure Mode (FM). The placement of the TC and FM coding in the basic event naming scheme should be agreed upon by the data analyst and the systems analyst, and this needs to be reflected in the software so that it will grab the information it needs to populate the basic event with the appropriate data. Additional information such as,

system identification numbers and unit number (for multiple unit sites) may be included in the naming convention. Human actions, common cause events and initiating events have their own unique naming scheme. Documentation of the agreed naming scheme should be included in the PRA documentation.

The Systems Analysis Program for Hands-on Integrated Reliability Evaluations (SAPHIRE) [57] code limits both component type and FM codes to three characters each to be consistent with the input constraints and conventions of the SAPHIRE template database feature. This allows the same component failure data to be applied to all items in the model.

As the fault tree analysis progresses, it is possible that additional component types and FMs may be required by the systems analyst. Discussions between the data analyst and the PRA modeler are essential to ensure that the new component request is not actually a duplication of another component type. In addition, some negotiation may be needed since not all FMs are readily available in generic data sources.

The Component Type + FM list should:

- Form the basis for the component type and FM coding scheme to be used in the PRA
- Consider the PRA software being used and the constraints it places on the naming scheme and database
- Reflect the best compromise between the available data in generic data sources and the data needs of the PRA

5.2.4 Defining a Failure

Events are identified as failures if the component would not have been able to perform its mission as defined in the PRA. Degraded states in which the component would have been able to perform its function over the mission time are not considered failures. This is consistent with ASME/ANS PRA Standard SR DA-C4. System engineers should be consulted if it is not clear from the documentation whether the maintenance action reflects a degraded state or a failure.

Failure Severity

Severity has been divided into three categories [52, 53]:

1. Catastrophic (aka Complete or Critical) – A failure that is both sudden and causes termination of one or more fundamental functions.
2. Degraded – A failure that is gradual or partial.
3. Incipient – An imperfection in the state or condition of equipment such that a degraded or catastrophic failure can be expected to result if corrective action is not taken.

It should be noted that only catastrophic failures form the numerators of component failure rates, unless the degraded failure leads to the inability of a component to perform its function during the PRA mission time. Degraded failures can contribute to equipment unavailability if the component needs to be taken out of service for repair. Incipient failures are generally more difficult to identify and classify from repair records and are therefore addressed separately by the Human Reliability Analysis (HRA) through the identification and quantification of misalignment and miscalibration pre-initiator human failure events.

The following additional guidance for component failure data review and coding is excerpted from EPRI TR-100381 [58]:

1. If the cause of unavailability of a standby component is self-revealing at the time it occurs (for example, control room alarm), or occurs during a test, but is revealed at the end of a test and results in maintenance, the event is accounted for in the unavailability due to maintenance (see Section 6). If the failure is such that it could also occur while the component is performing its mission, it should be counted towards that basic event also.
2. Failures to start or run of standby equipment are characterized by the failure condition not being revealed before a test or an actual demand, and the failure being catastrophic (in the sense of preventing operation or preventing achieving a certain minimum performance level).
3. Failures, such as leaks of components such as pumps and valves, which are not serious enough to be failures of the pressure boundary by an accepted definition, would be included in the unavailability due to maintenance as their effect is to induce maintenance activity (see Section 6).
4. If the effect (for example, pump A fails) is the result of the failure of another component that is modeled explicitly, the event is associated with that component, not the pump.
5. If the failure is caused by the test itself, or can only occur under test conditions, it should not be considered if the test conditions are beyond those normally expected on a real demand.
6. If the failure is spurious and could not be repeated on a second test or subsequent tests, it could be included as a potential failure, but to a best estimate it is not a failure. In the same way, events which are instantly recoverable are not important failures. This is, of course, a function of the success criterion for the component in terms of the time window within which it has to operate.
7. Failures revealed by tests performed as part of troubleshooting are not, in general, valid failures. However, failures which are associated with different mechanisms from those for which repair was initiated, are candidate failures.
8. An event only reporting a degraded or failed state of a non-critical piece part (for example, failure of one air start motor of a diesel generator which has redundant air start motors) should be carefully excluded from the failure events if the diesel generator component boundary includes the redundant air start system.
9. An event reported as a failure to meet tech specs, but which would not result in a catastrophic failure in the PRA sense, should not be included, but may lead to a maintenance unavailability (see Section 6).

5.3 Data Collection

The best available information is plant-specific data that have been analyzed, evaluated, and distilled to a point estimate value. However, because of the nature of the data collection and evaluation, and the fact that failure of some components is rare, not all components can be characterized by such data. The PRA, therefore, takes advantage of generic data sources to supplement, complement, and compare to the plant-specific data.

5.3.1 Generic Data

Generic data sources are documents and databases containing industrial experience on component performance. Usually they are previous safety/risk analyses and reliability studies performed nationally or internationally, but they can also be standards or published handbooks. Generic data is generally used: 1) when plant-specific data are not available, 2) for comparison with plant-specific data against industry experience, or 3) as a prior for a Bayesian update with plant-specific experience. A generic database is constructed using a library of generic data sources of reliability data, primarily from nuclear power plants, but also from equipment used by the military, chemical processing plants, and other facilities.

The preference should be to use data from the NRC operating experience database website [21] that and captures the current industry-average performance for components and initiating events at U.S. commercial NPPs updates the data organized by the component type and failure mode categories cited in NUREG/CR-6928 [4]. For component types or failure mode s where data are not available from NUREG/CR-6928, alternative data sources can be used, such as those cited in Table 2-3.

The list of components and failure modes for which generic data should be collected is obtained from the PRA model basic event file (for example, the .RR file from CAFTA, or the .BEI file from SAPHIRE). Definitions of component types and failure modes should be clarified wherever necessary using the plant support systems and naming convention.

It is necessary to analyze the generic data to compare the relevancy of the component data from the generic data sources with the equipment in the plant models. The data source scope should be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter was appropriately addressed. For example, a separate source might be used for electronics data versus mechanical data, so long as its use is justified by the detail and the applicability of the information provided. In addition, the generic data component boundaries must match those from the PRA basic event components. Lastly, the quality of the data source is considered to be a measure of the source's credibility. Higher quality data sources are based on equipment failures documented by a facility's maintenance records. Lower quality sources use either abbreviated accounts of the failure event and resulting repair activity, or do not allow the user to trace back to actual failure events. Every effort should be made to use the highest quality data source available for each component type and failure mode.

Data are selected from the generic data sources using the following criteria:

- The component type and failure mode identified in the generic data source must match those in the PRA basic events specified in the fault tree. For every component modeled, a comparison is made between the modeled component and the component found in the data source to ensure its suitability. Also, every attempt should be made to match the failure modes.
- The generic data source must be widely available, not proprietary. This ensures traceability and accessibility. The more recent the information, the better.

- The operating environment is an important factor in the selection of generic data sources. The environment of a component refers not only to its physical state, but also its operational state. The operating conditions of a component include the plant's maintenance and testing policy. If either of these differ from the modeled facility's state, then the generic data should be reconsidered and usually rejected (unless no alternative exists, at which time, explicit caveats should be provided about the use of the data, with sensitivity cases run, as needed).

If data are available from more than one generic data source, then the analyst has the option to apply further criteria to select one source considering the similarity between the plant operating environment and that represented in each generic data source, as well as the nature of the statistics provided, to ensure data appropriateness. The guidelines for the generic data selection process are summarized as follows:

- Greater than zero failures is preferred (not always able to exclude on this basis).
- Include mean or median values, and some expression of uncertainty surrounding these values (either upper or lower bounds or lognormal error factor).
- Denominator greater than 1,000 hours or 100 demands.
- Data analyst's confidence in the applicability of the data on the basis of component design, driver/operator, size, component application, active versus passive service, materials/fluids moved (for example, water versus caustic versus viscous), component boundary, what is included and excluded in the component definition (for example, motor, electrical connections), failure modes, operating environment, physical (for example, heat, humidity, corrosive), and functional (for example, operation, maintenance, and testing frequency).

A comparison should be made between the data used in any previous analysis to that planned for use in the current update. Type codes for which there is a measurable difference in generic data (that is, factor greater than five) should be reviewed in detail. These differences can be due to changes from using demand data to time-related data. In other cases, there may simply be better generic data sources available. All changes should be reviewed and justified based upon a match between the plant failure code and the failure code of the generic data source used.

One notable change can result from using the failure rate for turbine-driven pumps failing to run (standby) from NUREG/CR-6928 data, which separates data for failure to start, failure to run during the first hour, and failure to run after the first hour. The experience shows that all the failures to run occurred during the first hour. If the failure to run during the first hour data was combined with the failure to start data, the data for failing to run after the first hour can be two orders of magnitude lower than the failure to run during the first hour (and two orders of magnitude lower than the failure to run data previously used).

The results from the generic data search should be summarized (such as in an Excel spreadsheet) and a full set of distribution parameters should be calculated for each component type/failure mode. For example, since SAPHIRE needs different parameters for different distributions, means and error factors (EFs) are included for lognormal distributions, means and beta parameters are included for beta distributions and means and alphas were included for gamma distributions.

5.3.2 Plant-Specific Data

Nuclear power plant equipment failures are primarily collected from:

- The Maintenance Rule (MR) Program
- The Equipment Performance and Information Exchange (EPIX) database maintained by the Institute for Nuclear Power Operations (INPO) [50]
- Data provided to the proprietary INPO Consolidated Data Entry (CDE) system [50]
- Plant maintenance work orders (MWOs)

5.3.2.1 Data Window

The data analysis needs to establish the official timeframe for which data will be collected, otherwise known as the data window. The earliest date will depend upon the last data update that was performed. For example, if the previous data set included data collected through the end of December 2009, then the start date of the data window for the current data update project is 1 January 2010. The end date of the data window is usually the most current month for which the number of failures and the component demands or run times have been logged and documented. This determination includes overall plant operational hour information for those components that operate whenever the plant is operating. Therefore, it may be wise to have the data window lag by one or two months from the current date to ensure that all information has been entered into the plant computer system.

Consistency in the data window across the entire PRA update used to be the convention, although some plants have chosen to select data windows for the different data elements (initiating events, component failure data, unavailability data) depending upon issues that would impact the continuity of the database. The component reliability data window should be documented for reference in the plant-specific PRA data notebook.

There may be cases, however, when different data windows should be identified for certain equipment. For example, if a particular pump was replaced with a newer or different design or was significantly modified at some point in time, the data window for that pump may be restricted to the period after the replacement or modification. For these cases, it is advisable for the analyst to plot the failure history on a timeline for the time period before and after the upgrade or replacement of major equipment to see if there is a significant change (this would be expected since the rationale for replacement was likely to improve reliability). The data window should then select the operating history accordingly to be consistent with the post-upgrade experience.

Some evaluations can be made on a heuristic basis, such as to remove the first few years of operation to address early burn-in failures, end of life (aging) failures, or to count experience accumulated after a major component replacement in a system. Section 3.6 provides additional guidance on methods to determine if trends or outliers exist and how to justify their inclusion or exclusion in the dataset.

Even though judgment is involved in establishing the data window, if a case is being made for justifying one selection vs. another, the important issues that need to be considered are:

- Operations status – major outages, frequency of maintenance
- Equipment status – system upgrades and equipment replacements that could impact reliability
- Impacts to reliability data for inclusion vs. exclusion

The Mitigating Systems Performance Index (MSPI) [59] trends system and equipment performance and should be able to reveal the differences between data trends from one timeframe vs. another. In addition, the plant risk monitor should be able to evaluate different system configurations, performance trends, and their potential risk impact.

5.3.2.2 Failures

General rules for failure counting are as follows.

If a component has a recordable failure, it is then taken out of service to correct the problem. If it is still under that work order, and the failure recurs during post-maintenance testing, then the problem would still get fixed under that work order and an additional failure should not be counted. If a failure occurs during post-maintenance testing that was not related to the reason for the maintenance, then it could be that the maintenance activity caused the problem, and again an additional failure should not be counted. If it was clearly a different problem that cannot be tied to the maintenance activity, and could have just as easily occurred during an actual demand (that is, system conditions during the post-maintenance test are similar to those that would be experienced by the failed component when in service and an actual demand occurs), then it should be considered a failure.

Component failure data can be gathered from the various sources discussed below. Although the data reported and therefore available from these sources is similar (if not the same), they are all cited here since different utilities and plants have different preferences for the systems they access or they (and their contractors) may find some sources to be more readily accessible than others.

Maintenance Rule

The Maintenance Rule, described in 10 CFR 50.65 [2], requires the licensee to "monitor the performance or condition of structures, systems, or components, against licensee-established goals, in a manner sufficient to provide reasonable assurance that these structures, systems, and components … are capable of fulfilling their intended functions."

The equipment categories that fall within the MR performance monitoring scope are:

1. Safety-related structures, systems and components that are relied upon to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure.

2. Non-safety related structures, systems, or components:
    a. That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs)
    b. Whose failure could prevent safety-related structures, systems, and components from fulfilling their safety-related function
    c. Whose failure could cause a reactor scram or actuation of a safety-related system

The MR functional failure (MRFF) records are based on the plant Corrective Action Reports (CARs) and Condition Reports (CR). While the failure information collected can primarily be based on information in the MR availability database, the PRA team should also review applicable MRFF reports, the plant level MR indicator database, and MSPI program reports [60, 61] that reflect the data provided to the INPO proprietary CDE system [50].

While the MR process identifies functional failures, it may not identify all PRA-relevant component failures that are either a) not functional failures or b) not within the MR equipment scope. For this reason, it is necessary to review the MWOs or other plant records to ensure that all PRA-relevant failures have been captured. For example, a failure where the air operator failed to open the valve may not be included in the MR database because the function remained intact since the valve was capable of being opened manually (assuming manual operation was allowed within the MR-credited function definition). From a PRA standpoint, the air operator causing the valve failure to function is a relevant component failure (and failure mode) that should be counted in the PRA database.

The MR data is a good source of finding historical failures of important equipment, and provides good descriptions of what happened and why, however, it is just one source that should be consulted among the many identified in this chapter.

An insight from the development of PRA databases is that it is very beneficial to coordinate data collection efforts with the plant Maintenance Rule Coordinator (or equivalent position). It is important for PRA Engineers to understand the data gathering perspective required for the MR program and for MR Coordinators to understand the PRA perspective, including the equipment scope and relevant failure modes modeled in the PRA. Documenting the capture of all MR equipment failures against the MWO reviews performed by the PRA data analysis staff provides valuable peer review documentation.

Equipment Performance Information Exchange (EPIX)

The EPIX System was developed in 1997 by INPO. The EPIX system is a web-based database that provides information on components important to nuclear plant safety and reliability. EPIX was developed to meet current and projected industry needs for component-level information exchange and to replace the Nuclear Plant Reliability Data System (NPRDS) and to support implementation of the MR and other industry programs. It contains failure and engineering data for key components in each utility's MR scope. EPIX also provides access to the retrieval of data reported to NPRDS from January 1973 through December 1996. EPIX is a proprietary database managed by INPO for exclusive use by its member organizations.

All operating US nuclear plants report data to EPIX. Components reported to EPIX generally include those that are within the scope of each plant's Maintenance Rule Program [2]. Demand and run hour information within EPIX include one-time estimates based on a review of plant experience over at least an 18-month period for all components, and quarterly non-test demands and run hours for a subset of the more important components. Events reported to EPIX include both catastrophic and degraded failures [4].

NRC staff accesses the EPIX database through the INPO website [50] for use in NRC's Reliability and Availability Data System (RADS) [62], Integrated Data Collection and Coding System, and Common Cause Failure Database to estimate PRA parameters. EPIX data are also used to update NRC Standardized Plant Analysis Risk (SPAR) models and to assist in developing and implementing the MSPI [60, 61].

EPIX is part of INPO's proprietary CDE system that collects data from all utilities to meet licensee reporting requirements for the Reactor Oversight Process (ROP), World Association of Nuclear Operators (WANO), and Monthly Operating Reports (MORs).

In EPIX components are linked to their subcomponents, supporting components, and piece parts and the database contains estimates of demands and run times for these components. For a selected set of components, it contains actual observed demands and run times [63].

Concerns have been raised in recent PRA peer reviews regarding the ability to use EPIX data as the only source to capture all the failures required to be included in the PRA failure rate calculations. Since at some sites EPIX reporting is limited to MR functional failures and critical component failures (post 2007), the use of EPIX alone is not sufficient to ensure that all PRA-relevant failures have been captured (see MR discussion above and MWO discussion below).

Reliability and Availability Data System (RADS)

RADS is a database and analysis code, developed by the Idaho National Engineering and Environmental Laboratory (INEEL) for the U.S. Nuclear Regulatory Commission (USNRC). The information covers 1997 through the present.

The code is designed to estimate industry and plant-specific reliability and availability parameters for selected components in risk-important systems and initiating events for use in risk-informed applications. The RADS tool contains data and information based on actual operating experience from U.S. commercial nuclear power plants. The data contained in RADS is kept up-to-date by loading the most current quarter's EPIX data and by yearly loads of initiating event data from LERs. The reliability parameters estimated by RADS are 1) probability of failure on demand, 2) failure rate during operation (used to calculate failure to run probability), and 3) time trends in reliability parameters [62].

Because EPIX data are proprietary, NRC provides the RADS database and the RADS analysis software, along with supporting technical documentation, only to nuclear power plant licensees who are members of INPO and NRC staff on request. The reliability parameters estimated by RADS are as follows:

- Probability of failure on demand
- Failure rate during operation (used to calculate failure to run probability)
- Maintenance out-of-service unavailability (planned and unplanned)
- Time trends in reliability parameters

Maintenance Work Orders (MWOs)

The data analyst should meet with the MR/MSPI recording/report team to discuss the components and failure modes that are modeled in the PRA vs. the failure modes reported via MR/MSPI to determine whether MR/MSPI are sufficiently complete for PRA data needs. If not, it may be necessary to obtain a data dump of the MWOs resulting in component unavailability, compare them against the MS/MSPI list, review those MWOs that are distinct to determine if a PRA-relevant failure occurred. If so, these failures should be included with the database and the MWO cited as a reference. Although the process of reviewing MWOs can be incredibly time-intensive, a "data dump" and high level review of the MWO failures against the MR/MSPI/ EPIX/RADS data (depending upon the source of preference) is recommended to ensure that all PRA-relevant component failures have been identified.

NOTE: The ASME/ANS PRA Standard supporting requirement DA-C5 indicates that repeated plant-specific component failures occurring within a short time interval should be considered as a single failure if there is a single, repetitive problem that causes the failures.

5.3.2.3 Equipment Run Time and Demands

To evaluate the failure probability of a component, the number of demands or run time experienced by the component must also be evaluated. Component demands and exposure time from all contributors should be included, including testing, automatic and manual actuations, and preventive maintenance.

The exposure time of a component is dependent upon whether the component is normally operating or is in standby. For components that are required to continuously operate during a particular plant mode, the operating time can be established by directly relating it to the time spent in that plant mode. For a component in a standby system, the operating time is generally given by the time the system is operated during testing or maintenance.

Methods to estimate equipment demands and run times should identify the components that are:

1. Operated at-power or during shutdown
2. Tracked by the plant process computer (PPC)
3. Tracked under the MR Program
4. Operated during surveillance tests
5. Included in preventive maintenance action(s)

Demands and run time for components like check valves at the suction and discharge of pumps (and configured in series with the pumps) should also be tied to pump operations as the operation of these components is typically not documented specifically in plant records or by the PPC. Control room and ex-control room operator logs are also a good source of information for major equipment start/stop times (not monitored by the PPC), Limiting Condition of Operation (LCO) entries, and other data that may be important in the development of the most complete and accurate set of demand and run time data.

The process for estimating the demands and exposure times for plant components is described in detail the following subsections. Discussions are provided for the methods used, including identification of components that are operated during normal plant operations or on a rotating basis, during shutdowns, tracked by the PPC data, operated during surveillance tests and during preventive maintenance.

Operating Equipment

The equipment operating status impacts the run time estimation.

Normally Operating Equipment: PRA equipment that runs continuously while the plant is at power should be identified. Using a run time based strictly on the number of hours the generator was on line during the data window introduces an element of non-conservatism to the calculated failure rates, unless plant operation depends on that one component and the plant cannot operate without it being in service (that is, an RCP or Rx trip breaker). For example, if there are two MFW pumps and the plant can operate at power with only one in service, then an investigation of periods where that condition occurred should be performed to obtain accurate run times for the equipment. Tables (spreadsheets) should be developed for normally operating components modeled in the PRA, including basic event name and description, Tag ID, and additional information about the component.

Operating Equipment on Rotation: Demands and run times during the data window must also be estimated for operating equipment that follows a normal rotation. PRA equipment that falls into this category generally includes the Instrument Air compressors, SW system pumps and Component Cooling Water (CCW) system pumps. A split-fraction approach may be sufficient, as long as the split fractions chosen are supported by the plant records.

If PPC data are available for the SW and CCW pumps, it is a better source of data than estimating rotation data.

Otherwise, equipment rotation demands and run time can be estimated based on discussions with operations personnel. In addition, Operations logs can be reviewed to confirm equipment rotation schedules and run times, although this is a time-consuming practice.

Shutdown Operating Equipment: Shutdown operating equipment includes the AFW system because it generally runs for a day following shutdowns and startups. The AFW shutdown and startup demands and run time can be split between the motor-driven pumps and trains, with each train assumed to run for 24 hours (or other appropriate duration) during each shutdown and startup. Such assumptions should be verified with operations.

Tables (spreadsheets) should be developed for components modeled in the PRA that operate when the plant is shutdown, including basic event name and description, Tag ID, and additional information about the component.

Plant Operating History

A review of plant operating history is required to identify the overall plant availability for the timeframe under study and to provide run time information for the normally running systems in the PRA study.

For systems that operate whenever the reactor is operating, reactor critical hour data can be used as run time. Reactor critical hour data is routinely collected by plants and is reported to the NRC (and is therefore available in the RADS database) and to the North American Reliability Council (NERC) Generating Availability Data System (GADS) [49] in terms of the number of hours of critical operation in the previous quarter.

The GADS database includes all reactor power perturbations and shutdowns since 1978; mandatory GADS reporting started in January 2012 for all conventional generating units 50 MW and larger. The reactor critical hours for a calendar year are then summed from January through December and divided by 8760 hours to express the data in units of reactor-critical years.

An example of this process is shown in Section 4 in Table 4-3.

The availability factor is the amount of time that the plant is able to produce electricity, estimated as the amount of time the generator is on-line, divided by the total time in that period. This factor is a measure of the plant's ability to operate and can be used to characterize the reliability of the plant.

The average plant availability factor for the data window identified for the PRA can be obtained from plant reports (sometimes called Burn-up Reports) of the total time the generator was on-line, or from the (proprietary) RADS database available on the NRC operational experience website [21].

The total availability factor for the PRA database data window can then be calculated as shown in Section 4 in the Table 4-3 example.

Components Tracked by PPC Data

PRA components are generally tracked at many facilities by the PPC system. This is not a foolproof source of data, but it is based on plant-specific operational records.

The PPC collects data every time an event occurs (that is, pump starts or stops) and at regular data collection intervals, such as every eight hours. These data can be used for pump, valve and breaker demands, as well as pump run time. Most PPC points of this type are calibrated via Technical Specification surveillance or by preventive maintenance (PM) and calibration sheets.

Care should be taken, however, in using plant computer data because it is difficult to distinguish between tests and actual actuations. One way to address this is to plot the actuation data by duration and see where it tapers to determine where the real actuations are and also look at the periodicity of the data to see if there are pulses. This method is at least conservative; use of raw computer data without additional scrutiny can be non-conservative.

For data values downloaded to a spreadsheet, it is often useful to create a macro to filter out spurious data points by querying the data for a change state position (for example, "started" or "opened"), and discarding all archived error messages (for example, "shutdown" and "I/O timeout"). The macro then looks at the previous data point and, if the state has changed, tallies this as one demand event. The cell counted can also be color coded to facilitate visual checking of the data for accuracy and erroneous counting of non-change events if any were to occur. This approach eliminates counting of change state positions if no change had actually occurred.

The data should also be visually reviewed to ensure that additional demands from post-maintenance testing were not counted. In cases where demands are identified in a short time interval, a check can be performed against PM actions to make sure none are associated with additional post-maintenance testing.

Procedure Reviews, MSPI, and Maintenance Rule Data

Procedure Reviews: Current surveillance procedures are used to calculate the component detection intervals, and demand and run time data. This is done to reflect the current plant operational practices and, therefore, the state of the plant as modeled in the PRA. Procedures should include those reviewed in the previous plant-specific data analysis, those identified on the System Responsibility Matrix or other plant tool that correlates operations and testing procedures applicable to PRA-related systems, those listed in the MSPI Basis Document, and those identified during discussions with system engineers and operations personnel.

For each procedure reviewed, the PRA components that were exercised during the test should be identified, along with the relevant piping and instrumentation diagrams (P&IDs) to identify additional components (for example, check valves) that are exercised during the test. Similarly, the MSPI basis document, and Operations narrative logs should also be reviewed concurrently with the procedure reviews to determine demand and run time estimates. This information should be discussed with operations personnel and system engineers for verification.

The result of this effort is a listing of components exercised during each surveillance procedure. Next to each component ID, the type of operation (for example, start, open) and a demand or run time should be indicated, as well as a reference to the applicable section and page number of the procedure. Components exercised upstream and downstream of the identified component are given the same procedure section and page reference.

To estimate the total number of demands or run time over the data window, the frequency of the procedure is identified and a simple data lookup function can be used. Most procedures are performed on a monthly, quarterly or refueling basis, so simple calculations can be made to estimate the total number of times each procedure is implemented during the data window.

A Procedure Review worksheet such as that shown as Table 5-3 should be developed to log component demands and run times for each procedure reviewed, preferably associated with the basic event name.

MSPI Basis Document Review: As previously mentioned, the ROP MSPI program **data** should be reviewed in conjunction with the procedure reviews. The MSPI program monitors the performance of selected systems based on their ability to perform risk significant functions as defined in NEI 99-02 [59]. It is comprised of three elements: 1) system unavailability, 2) system unreliability, and 3) system component performance limits. The MSPI is calculated separately for each of the following monitored systems:

- Emergency AC Power System
- High Pressure Safety Injection (HPSI)/High Pressure Injection (HPI)/High Pressure Coolant Injection (HPCI)
- Heat Removal System – Auxiliary Feedwater (AFW)/Reactor Core Isolation Cooling (RCIC)
- Residual/Decay Heat Removal System – Decay Heat Removal (DHR) system, Residual Heat Removal (RHR) system, Containment Spray
- Cooling Water Support Systems – Service Water system and Component Cooling Water (CCW) system

Further information regarding data collection using MSPI information is provided in Section 6 of this report.

MR Database Review: As part of the MR availability database, EDG starts, loads, and run times are tracked. These data are used to calculate EDG start, loads, and run time.

The "History" table in the MR availability database contains all of the entries for the components in the database. A query can then be run on the data to filter on the EDGs and then sort for the applicable date range. These data include the demand for the component (that is, start or load); the date of the demand; the start and end time for the demand; and if the demand was planned, unplanned, or from a fault exposure. The results should be exported into a spreadsheet and the total number of starts, loads, and run time calculated.

Table 5-3
Example procedure review worksheet

Frequency	Number of Tests	Component	FC	Mode	Demands	Run Hours	FSAR ID	Total Demands	Total Run Time (hrs)	Notes
Refueling	2	P-18A	ME	Start	1		CSP-PMME-P-18A	2	0.0	Section 8.3.1, Page 9
	2	P-18A	MG	Run		1.0	CSP-PMMG-P-18A	0	2.0	Section 8.3.1, Page 9
	2	CKV-2125	MA	Open	1		CSP-CVMA-CK-2125	2	0.0	Section 8.3.3, Page 9
	2	CKV-2125	MD	Remain Open		1.0	CSP-CVMD-CK-2125	0	2.0	Section 8.3.3, Page 9
	2	CKV-2115	MA	Open	1		CSP-CVMA-CK-2115	2	0.0	Section 8.3.3, Page 9
	2	CKV-2115	MD	Remain Open		1.0	CSP-CVMD-CK-2115	0	2.0	Section 8.3.3, Page 9
	2	CKV-2213	MD	Remain Open		0.5	ESS-AVMD-CV-2213	0	1.0	Section 8.3.4, Page 10
	2	P-29A	ME	Start	1		LPI-PMME-P-29A	2	0.0	Section 8.5.9, Page 14
	2	P-29A	MG	Run		1.0	LPI-PMMG-P-29A	0	2.0	Section 8.5.9, Page 14
	2	P-18C	ME	Start	1		CSP-PMME-P-18C	2	0.0	Section 8.5.10, Page 15
	2	P-18C	MG	Run		1.0	CSP-PMMG-P-18C	0	2.0	Section 8.5.10, Page 15
	2	P-18B	ME	Start	1		CSP-PMME-P-18B	2	0.0	Section 8.5.11, Page 16

Table 5-3 (continued)
Example procedure review worksheet

Frequency	Number of Tests	Component	FC	Mode	Demands	Run Hours	FSAR ID	Total Demands	Total Run Time (hrs)	Notes
Refueling	2	P-18B	MG	Run		1.0	CSP-PMMG-P-18B	0	2.0	Section 8.5.11, Page 16
Mode 5-3	9	P-18A	ME	Start	1		CSP-PMME-P-18A	9	0.0	Attachment 1, Step 3.2, Page 5
	9	CKV-2133	MA	Open	1		ESS-CVMA-CK-2133	9	0.0	Attachment 1, Step 3.2, Page 5
	9	CKV-2232	MA	Open	1		ESS-CVMA-CK-2232	9	0.0	Attachment 1, Step 3.2, Page 5

Preventive Maintenance Activity Data

Demands and run time are also estimated for PM activities performed on components modeled in the PRA. Most plant computer systems contain a function for tracking PM activities by individual component and equipment groups. PM activities are also coded by the frequency with which they are performed. It may be necessary for the data analysts to confer with the plant Information Technology department to request or learn how to request PM activity data properly from the various PM data systems.

Once the PM information is compiled, PM calculations must be performed. Calculations may need to be done differently for equipment whose demands and run times are based on PPC data versus other sources. For example, if there is a PM that occurred every six years and the PRA update data window is three years, a PM frequency of 0.5 is assigned.

All PMs longer than the data window should be evaluated this way, then summed. In addition to demands, PM run times must also be estimated. PM run times are generally based on discussions with system engineers and searches on the Operations Logs.

For components in which demands and run times must be estimated by other methods (for example, procedure reviews, equipment rotation, and so on), PMs can be counted using an equivalency based on the data window. For example, a 365-day PM (that is, yearly) is assigned three demands for a three-year data window; similarly, for a 548-day PM (that is, refueling outage), two demands would be assigned.

All PM-related demands are then summed to obtain a total number of PM demands, as are the run times.

Detection Intervals

Equipment detection intervals must be determined to support standby failure rate calculations.

The list of standby failure basic events is obtained from the PRA model. This list should be reviewed by the data analyst and plant staff to ensure that the basic events represent standby components, that is, components that are typically not used until tested or needed.

Then, several different evaluations should be performed in determining the detection interval:

- PM Actions – Based on a compilation of current plant PMs (as described previously), the shortest surveillance interval should be identified for each component. Components would be demonstrated or tested during a PM, so the detection interval should be based on the most frequent PM.
- Procedural Demonstrations – Successful operation of many components is demonstrated during testing. The testing frequency for components is identified during the procedure reviews to estimate component demands and run time (described previously). Procedure demonstrations are included where testing would verify the component failure code depicted by the basic event.

- Operational Demonstrations – Successful operation of some components is demonstrated during plant events such as hot or cold shutdowns, or refueling outages. Components that are used during hot shutdowns are assigned a detection interval based on plant operating history and the number of hot shutdowns over the data window. The hot shutdown interval is the number of hours between hot shutdowns. Similarly, components that are demonstrated to be operable during cold shutdowns are assigned a detection interval based on the number of cold shutdowns divided by the hours in the total data window. The final detection interval included was for components demonstrated during refueling outages. These components are assigned a detection interval based on an 18-month refueling outage schedule. Operational demonstrations were reviewed with operations personnel.
- Operator Checks – Several components are checked by operators performing daily rounds. The equipment inspection and round guidelines (Narrative Logs, Rounds, Operating) often provide several different daily round sheets (for example, Feedwater system). Components on these sheets if checked per shift are assigned an interval of 12 hours.

The detection interval for each basic event is chosen based on the most frequent option described above. The detection intervals for components checked by operators and demonstrated during hot shutdowns, cold shutdowns and refueling outages are also reviewed with operations personnel to verify that the component status would be confirmed. Plant drawings, specific functions, and indications for the components should also be reviewed to confirm the status of the component.

While detailed data systems now exist for recording demand and run time information, the development of exposure data may still involve judgments and assumptions on the part of the data analyst. Although the magnitude of error or the range of uncertainties associated with the exposure data are typically small compared with those of the failure data, there are cases where the combined effect of uncertainty about the exposure and failure has a significant impact on the estimate of the failure rate. The data analyst should note these uncertainties as candidates for PRA sensitivity analysis.

5.4 Data Calculation

For the calculation of plant-specific failure rates, the data analyst has the option of using a classical (frequentist) or Bayesian approach. The frequentist approach calculates maximum likelihood estimates (MLEs), which are failures/demands (or hours), using the failure information, and demand or run time information gathered from plant records.

The beta and gamma distributions are commonly used to express the reliability of a component. Beta distribution applies to probability upon demand types of inputs (Failure to Start, Failure to Open/Close, and so on), while the gamma distribution applies to time-based rates (Failure to Run, initiating event frequencies, and so on). Section 2.3.4.4 provides the formulas for the beta and gamma distributions, and section 3.3 describes how they are used in Bayesian updating. Chapter 6.2.1 of NUREG/CR-6823 [13] provides further information on beta and gamma distributions and Frequentist or Classical estimation methods.

NOTE: The ASME/ANS PRA Standard supporting requirement DA-D8 indicates that if modifications to plant design or operating practice lead to a condition where past data are no longer representative of current performance, the use of old data should be limited and either use generic data, if appropriate, or evaluate the extent to which the old data can be used.

Alternatively, generic data can be updated with plant-specific experience using Bayesian updating. For the Bayesian updating, generic data is used as the prior and the data as updated by the plant-specific failures and exposures form the posterior. Further information on the Bayesian updating process is provided in Section 3.

NOTE: It is not uncommon to see zero failure occurrences in a plant-specific data set since complete or catastrophic failures of key components are rare due to improved maintenance and surveillance testing practices. The treatment of zero failures depends upon whether the analyst chooses a frequentist or Bayesian approach, as discussed previously.

If the plant data is to be used "as-is" in a Frequentist calculation, then some estimation must be used for the numerator to permit a failure rate to be calculated when there are zero failures in the plant experience.

A one-third failure estimator has been documented [64]. In this approach, the failure rate would be calculated as:

$$\lambda_{mean} = (1/3)/\text{denominator} = (0.33333)/\text{denominator}$$

A comparison of the one-third failure estimator against four other approaches [65] found that it consistently yielded the lowest estimates for failure probability. However, the use of the one-third estimator continues to be controversial since some PRA data analysts have found it instead to be extremely conservative in cases where the experience is limited and the actual component failure probability or rate is very small. Their argument is that given just the experience data (and no failures), there is no specific idea how close the component might be to experiencing its first failure. However, this description is retained for historical purposes.

Alternatively, a Bayesian updating approach can be used. If no generic data is available, a Jeffreys non-informed prior, which is essentially a 0.5 failure estimator or "half-failure" approach, can be used. If generic data is available, then an informative distribution can be developed and the plant-specific zero failures will be statistically combined with generic data to develop the failure rate without need for additional assumptions (that is, zero failure can be use "as-is"). Bayesian updating is further discussed in Section 3.

5.5 Special Considerations for Use in Risk Monitor

Risk-Informed Technical Specification Initiative 5b provides a risk-informed method for licensee control of Surveillance Frequencies. In order to be able to support this application of PRA, the data must properly reflect the component reliability as a function of surveillance frequency so the analyst can assess the impact of a reduced frequency on overall risk.

Figure 5-2 below provides a graphical illustration of how failure probability is often modeled as a function of surveillance frequency. This figure shows a model assuming a constant failure rate and perfect testing (that is, testing is 100% effective at catching and correcting incipient failures). The probability of a time-related failure (for example, standby-stress failure characterized by a

failure rate) increases as the time period increases unless there is an intervention. When there is regular testing, the time frame "resets" after every test, thus reducing the average failure probability (for example, the risk is limited by the test interval, or "test-limited"). The longer the test interval, the higher the average failure probability.

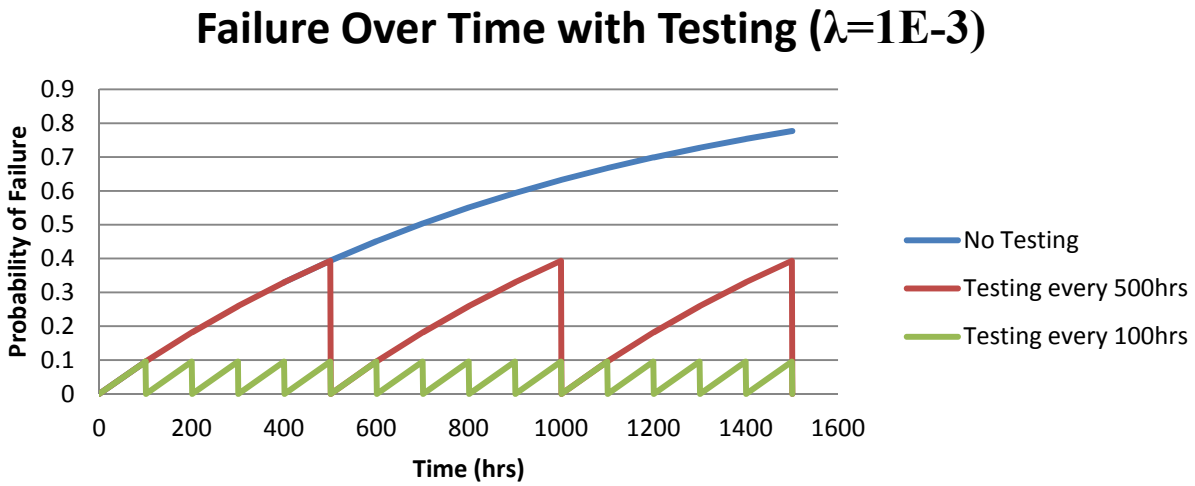

Figure 5-2
Example failure as function of surveillance frequency

The industry guidance document for Risk-Informed Technical Specifications Initiative 5b, NEI 04-10 [66] provides the following guidance (emphasis added):

> In general, the failure probability values of components used in PRAs consist of a time-related contribution (that is, the standby time-related failure rate) and a cyclic demand-related contribution (that is, the demand stress failure probability). The risk impact of a proposed STI adjustment shall be calculated as a change of the test-limited risk (see Regulatory Guide 1.177 [67], Section 2.3.3). Since the test-limited risk is associated with failures occurring between tests, the failure rate that shall be used in calculating the risk impact of a proposed STI adjustment is the time-related failure rate associated with failures occurring while the component is in standby between tests (that is, risk associated with the longer time to detect standby-stress failures). Therefore, caution should be taken in dividing the failure probability into time-related and cyclic demand-related contributions because the test-limited risk can be underestimated when only part of the failure rate is considered as being time-related while this may not be the case. Thus, if a breakdown of the failure probability is considered, it shall be justified through data and/or engineering analyses. When the breakdown between time-related and demand-related contributions is unknown, all failures shall be assumed to be time-related to obtain the maximum test-limited risk contribution.

To properly capture the increase in failure rate that occurs with an extended surveillance frequency, the analyst must express the standby failure as a function of time. Current practices often express failure of standby equipment simply as a demand-type failure (for example, failure to run) or may split the failure into two components: 1) failure during standby (time-related) and

2) failure on demand. When splitting the failure into two components, it may be difficult to determine the relative contributions to the overall failure probability. Therefore, NEI 04-10 recommends all failures be treated as time-related and only calculating a failure rate for standby components, unless a strong justification is available to do otherwise.

This report does not provide any guidance on how to justify splitting the failure into the time-related and demand-related pieces as there is no generally accepted method for this. However, there have been some recent efforts in industry to address this. Reference [68] provides one approach based on attempts to trend component failure data from EPIX/RADS (1997-2011) in order to generate test-interval-specific demand failure probabilities for specified components and failure modes.

5.6 Standard and Regulatory Requirements

RG 1.200 [8] cites the following Technical Characteristics and Attributes for Parameter Estimation:

- Estimation of parameters associated with initiating event, basic event probability models, recovery actions, and unavailability events using plant-specific and generic data as applicable.
- Estimation is consistent with component boundaries.
- Estimation includes a characterization of the uncertainty.
- A Note is also provided, as follows: It is recognized that for those new reactor designs with substantially lower risk profiles (for example, internal events CDF below 10^{-6}/year) that the quantitative screening value should be adjusted according to the corresponding baseline risk value.

ASME/ANS RA-Sa–2009 [7] contains the following HLRs in the data analysis technical element:

- HLR-DA-A – Definition
- HLR-DA-B – Grouping
- HLR-DA-C – Generic and plant-specific data consistency with the parameter definitions of HLR-DA-A and the grouping rationale of HLR-DA-B
- HLR-DA-D – Parameter estimates based on generic and plant-specific evidence, integrated using acceptable methods and accompanied by a characterization of the uncertainty

In addition, the following SRs from other areas of the PRA Standard apply to and interface with the component data analysis task:

- SY-A8 – Component boundary definition and data that matches these boundaries. Model subcomponents separately that are shared by another component or affect another component.
- SY-A14 – Failure modes.
- SY-A15 – Screening criteria for contributors to system unavailability and unreliability.

5.7 Guidance per Findings and Experience

Peer reviews have been and continue to be conducted to evaluate the technical adequacy of Internal Events PRAs against the /ASME/ANS PRA Standard guidance in the technical element of data analysis. The following issues reflect findings that have been made in recent PRA peer reviews in the chapter topic area and recommended guidance based upon finding recommendations and PRA data practitioner experience:

1. Demand Estimation per ASME/ANS PRA Standard SR DA-C6

   Finding: Surveillance tests were estimated. However, other demands (maintenance related, operational, other) were not evaluated. When MSPI demands (which count all of these types of demands) were compared with demands estimated only from surveillance tests, the overall demands (from MSPI) were 20 to 75% higher. Therefore, the demand estimates are low and conservative but may not be realistic.

   Recommended Resolution: Consider all sources of component demands, whether from planned or unplanned maintenance, operation, or surveillance testing to ensure complete accounting of challenges placed upon components.

NOTE: Demands should not be counted if the failure was not counted. If a component has a recordable failure, it is then taken out of service to correct the problem. If it is still under that work order, and the failure recurs during post-maintenance testing, then the problem would still get fixed under that work order and an additional failure should not be counted. If a failure occurs during post-maintenance testing that was not related to the reason for the maintenance, then it could be that the maintenance activity caused the problem, and again an additional failure should not be counted. If it was clearly a different problem that cannot be tied to the maintenance activity, and could have just as easily occurred during an actual demand (that is, system conditions during the post-maintenance test are similar to those that would be experienced by the failed component when in service and an actual demand occurs), then it should be considered a failure.

2. Data Categories per ASME/ANS PRA Standard SR DA-C7

   Finding: Planned maintenance activity, unplanned maintenance, and operational contributions to demands (and run hours) were not counted.

   Recommended Resolution: Consider all sources of component demands, whether from planned or unplanned maintenance, operation, or surveillance testing to ensure complete accounting of challenges placed upon components (see Note above).

3. EPIX Data Application per ASME/ANS PRA Standard SR DA-D1

   Finding: EPIX data alone is not sufficient to meet this requirement. There is no problem with the generic data or the Bayesian updating process used. The issue is the calculation of "realistic parameter estimates" using plant-specific data since only EPIX/MR information was used.

Recommended Resolution: Discuss with the engineer responsible for EPIX/MR data collection the exact nature of the information included and compare to the PRA and PRA Standard requirements to ensure full data capture. Augment with repair records/MWOs as necessary to complete the database.

4. Definition of Failure Modes per ASME/ANS PRA Standard SR DA-A2

   Finding: No definition or criteria for the definitions of failure modes, and success criteria were identified in the review of the data analysis package. The criteria to establish the definitions of structures, systems and components (SSC) boundaries, failure modes, and success criteria in a manner consistent with corresponding basic event definitions in systems analysis are required per the SR. In this case, SSC boundaries were discussed and examples provided. However, there was no similar documentation for the failure modes and success criteria.

   Recommended Resolution: Define component failure modes per 5.2.2 of these guidelines and correlate these modes to the success criteria and basic event definitions in the systems analysis (as determined in the analysis and documented in the PRA Systems Analysis notebook).

5. Prior data versus Posterior bounds per ASME/ANS PRA Standard SR DA-A4

   Finding: Not Met CC II/III due to the lack of discussion and documentation relating to examination of inconsistencies between the prior distribution and the plant-specific evidence to confirm that they are appropriate. A review of the Update Spreadsheet in support of the Bayesian analysis reflects a single failure in which the posterior mean fell outside the uncertainty bound of the prior distribution.

   Recommended Resolution: Evaluate the posterior data in relation to the uncertainty bounds of the posterior and prior uncertainties to address discrepancies and document the issue such that the discrepancies (if they exist) can be explained or resolved. See Sections 3.5 and 3.6 for more guidance on visual and statistical tests that can be used for this check. Any tests performed should be documented.

6. MR versus PRA Failure Definitions per ASME/ANS PRA Standard SR DA-C4

   Finding: For MRFFs and unavailability events, the reviewer was unable to find system or component specific definitions of these MR performance criteria. The applicable procedure states that the PSA should be considered as an input into MR performance criteria development. No evidence was found that MRFF and unavailability definitions have been compared to definitions or scoping in PSA. Events may be screened out from the PSA analysis that should not be.

   Recommended Resolution: Evaluate MRFF and unavailability definitions compared to definitions or scoping in PSA to ensure consistency.

NOTE: The analyst should check the MR data to ensure that it is consistent with the PRA, per the peer review comment.

7. MR Data use per ASME/ANS PRA Standard SR DA-C3

   Finding: The applicable PRA procedure states that "A failure would be counted if a component tripped for no apparent cause and was later restarted with no corrective activity. This type of event may not be counted as a MR functional failure ..." However, this type of failure would be screened-out by the failure identification process that starts with MRFFs.

   Recommended Resolution: Suggest providing alternate method to identify failures other than MR data, or validating that all modeled failures that will be used for plant-specific updates are included in functional failure definitions. No examples of missed failures have been observed.

8. Component Boundary Definition per ASME/ANS PRA Standard SR DA-A2

   Finding: No boundary definition is defined for heating, ventilating, and air conditioning (HVAC) air handling units or coolers. The AFW coolers are modeled as separate fans and heat exchangers. These are more appropriately grouped as an air handling unit per NUREG-CR-6928. Alternately, define these explicitly as separate components.

   Recommended Resolution: Ensure all boundaries are defined appropriately and modeled consistently with their definitions, or explain deviations. Adjust modeling as appropriate.

9. Standby Component Demands per ASME/ANS PRA Standard SR DA-C6

   Finding: In practice, computer point data are used for estimating demands on standby components, where the data points exist. According to the applicable PRA procedure, estimates of operation based on normal operating practices, surveillance procedures (SPs), and system engineer input were used for the remaining AOVs and MOVs, batteries, battery chargers, air compressors, dedicated shutdown diesel generator, diesel-driven fire pump, motor-driven fire pump, and deepwell pumps. There is no evidence that demands from post-maintenance testing are excluded. No unusual number of demands as multiple demands in an hour is excluded.

   Recommended Resolution: Review and exclude post-maintenance testing demands and count multiple demands in an hour as single demands (see Note above).

10. Test Procedure Use per ASME/ANS PRA Standard SR DA-C10

    Finding: It is not clear from the written discussion that the test procedures were indeed reviewed to determine that each test included all sub-components within the component boundary. Discussion with PRA personnel indicated that test procedures were indeed reviewed for this topic and pointed the reviewer to the system notebooks for additional information on test procedures. The appropriate section of each system notebook lists the test procedures that impact the availability of various equipment, but it does not list all the subcomponents within the component boundary.

    Possible Resolution: Add a brief discussion to the data notebook that explains how the test procedures were reviewed to determine which tests resulted in valid demands.

6
UNAVAILABILITY DATA

6.1 Introduction

In the PRA context, unavailability is the probability that a system, train or component (SSC) is not capable of supporting its function as modeled in the PRA due to being out of service for maintenance or testing, rather than due to an active or passive failure. From the PRA database perspective, this unavailability relates to the fractional time the SSC spent annually in test and maintenance. Unavailability basic events are documented in the PRA system notebooks and are quantified by the data analyst using total operating hours in the applicable plant modes for each system and combining this information with the downtime data by system and train.

6.2 Data Definition

The scope of unavailability data collection is determined by those components identified in the PRA by the systems analysts and explicitly included in the fault tree models.

Unavailability is considered in two cases, as cited in NUMARC 93-01 [69]:

1. Maintenance activities

   Equipment out of service (for example, tagged out) for corrective or preventive maintenance is considered unavailable. Support system unavailability may be counted against either the support system, or the front line systems served by the support system. The treatment of support system unavailability for the maintenance rule should be consistent with its treatment in the plant PSA. Performance criteria should be established consistent with whichever treatment is chosen.

2. Testing

   SSCs out of service for testing are considered unavailable unless the test configuration is automatically overridden by a valid starting signal, or the function can be promptly restored either by an operator in the control room or by a dedicated operator stationed locally for that purpose. Restoration actions must be contained in a written procedure, must be uncomplicated (a single action or a few simple actions), and must not require diagnosis or repair. Credit for a dedicated local operator can be taken only if (s)he is positioned at the proper location throughout the duration of the test for the purpose of restoration of the train should a valid demand occur. The intent of this paragraph is to allow licensees to take credit for restoration actions that are virtually certain to be successful (that is, probability nearly equal to 1) during accident conditions.

Plant-specific Maintenance Rule (MR) information is the primary source for this data for risk-significant (High Safety significant) equipment. For all other PRA modeled equipment, another means of determining average unavailability will still need to be developed from the sources identified below.

6.3 Data Collection

This section discusses the timeframe for which the unavailability data should be collected (data window) and the sources for this information.

6.3.1 Data Window

The data analysis needs to establish the official timeframe for which data will be collected, otherwise known as the data window. The earliest date will depend upon the last data update that was performed. For example, if the previous data set included data collected through the end of December 2009, then the start date of the data window for the current data update project is 1 January 2010. The end date of the data window is usually the most current month for which the maintenance and test actions and the component outage times have been logged and documented. This determination includes overall plant operational hour information for those components that operate whenever the plant is operating. Therefore, it may be wise to have the data window lag by one or two months from the current date to ensure that all information has been entered into the plant computer system.

Consistency in the data window across the entire PRA update used to be the convention, although some plants have chosen to select data windows for the different data elements (initiating events, component failure data, unavailability data) depending upon issues that would impact the continuity of the database. The component reliability data window should be documented for reference in the Plant-Specific PRA data notebook.

The maintenance data window should be long enough to capture infrequent maintenance (for example, 5-year equipment refurbishments) but short enough and recent enough to represent current plant practices.

Some evaluations can be made on a heuristic basis, such as to remove the first few years of operation to address early burn-in failures, end of life (aging) failures, or to count experience accumulated after a major component replacement in a system.

Even though judgment is involved in establishing the data window, if a case is being made for justifying one selection vs. another, the important issues that need to be considered are:

- Operations status – major outages, frequency of maintenance
- Equipment status – system upgrades and equipment replacements that could impact reliability
- Impacts to reliability data for inclusion vs. exclusion

MSPI trends system and equipment performance and allows the user to identify the differences between data trends from one timeframe vs. another. In addition, the plant risk monitor allows the user to evaluate different system configurations, their availability trends,and their potential risk impact.

6.3.2 Maintenance Rule (10 CFR 50.65)

The preferred source for unavailability data is the Plant MR Program data, specifically the MR availability database. The MR described in 10 CFR 50.65 [2] requires the licensee to "monitor the performance or condition of structures, systems, or components, against licensee-established goals, in a manner sufficient to provide reasonable assurance that these structures, systems, and components … are capable of fulfilling their intended functions."

The advent of data collected to demonstrate compliance to 10 CFR 50.65 has created a resource for use in the characterization of on-line maintenance unavailability that reflects current plant performance and practices. Guidance for collection of MR unavailability data closely matches the requirements for use in PRAs. For example, only outages during critical operation are considered (including overhaul outages); outages resulting from support system unavailability are not included. However, this can be a problem for multiple unit sites that share equipment important to plant risk (for example, emergency diesel generators and crosstie-able electrical buses, auxiliary feedwater pumps, service water systems, instrument air systems, chilled water systems, and so on). In this case, such systems and equipment should be identified and the MR unavailability data collection either verified to accurately represent availability for the modeled unit, or a separate data collection effort to capture unavailability during these opposite unit outage periods should be developed.

Unavailability is counted from the time the component or train is removed from service until it is restored to service.

Searches of the MR availability database can be performed on unavailability for equipment tag IDs from the PRA model. It is important to identify equipment "unavailability" because the database may also include "inoperability." The MR identifies "unavailability" as the time when the equipment is not able to perform its intended function. "Inoperability" can also include administrative time during which the equipment is capable of performing its intended function or Technical Specification related downtime.

As a cross-check, there are Limiting Condition of Operation (LCO) log type applications used by plants to track what action statements they are in at any given time and when the clock "runs out" on them, and they provide historical information on important equipment.

The MR availability data as shown in Tables 6-1 and 6-2 is generally provided as unavailability hours per month by train for a given system.

The equipment in each train is considered to be impacted similarly in terms of unavailability, so the downtime hours are allocated accordingly by component. However, if unavailability from the MR program is supplied at the train level, it should not be applied to more than one SSC (that is, one basic event) in the PRA representing the unavailability of the train as a whole.

Table 6-1
Example #1 – Maintenance Rule unavailability data

Month	Period Hours Applicable Modes	Planned Downtime Hours	Forced Downtime Hours	Total Downtime Hours
Nov-95	720	0.00	0.00	0
Dec-95	744	0.00	0.00	0
Jan-96	744	20.20	0.00	20.2
Feb-96	696	0.00	0.00	0
Mar-96	744	0.00	0.00	0
Apr-96	720	0.00	0.00	0
May-96	744	0.00	0.00	0
Jun-96	720	0.00	0.00	0
Jul-96	744	0.00	0.00	0
Aug-96	744	20.30	0.00	20.3
Sep-96	720	1.80	8.40	10.2
Oct-96	744	8.65	0.00	8.65
Nov-96	720	6.65	0.00	6.65
Dec-96	744	0.00	0.00	0
Jan-97	744	144.00	0.00	144
Feb-97	672	0.00	0.00	0
Mar-97	744	0.00	0.00	0
Apr-97	720	0.00	0.00	0

Table 6-2
Example #2 – Maintenance Rule unavailability data

Time	Period Hours	A Train Unavailability Hours	B Train Unavailability Hours
Feb-01	672	0	3.6
Mar-01	389.5	0	0
Apr-01	544.9	0	0
May-01	744	0	0
Jun-01	720	0	0
Jul-01	744	0	0
Aug-01	744	0	0
Sep-01	720	0	0
Oct-01	744	0	0
Nov-01	720	0	0
Dec-01	744	7.85	0
Jan-02	744	0	13.3
Feb-02	672	3.55	0

6.3.3 Other Maintenance Data Sources

6.3.3.1 Mitigating System Performance Index (MSPI)

The MSPI program data can be useful as a second/sanity check on the numbers and sources of information for the unavailability data collection effort, however, the equipment unavailability covered by MSPI is probably also risk-significant and already monitored by the MR program.

The MSPI program monitors the performance of selected systems based on their ability to perform risk significant functions. It is comprised of three elements: 1) system unavailability, 2) system unreliability, and 3) system component performance limits.

Specifically, the MSPI program monitors unavailability performance of pumps, EDGs, and selected valves in five types of mitigating systems: emergency AC power, High Pressure Safety Injection (HPSI)/High Pressure Injection (HPI)/High Pressure Coolant Injection (HPCI), heat removal [Auxiliary Feedwater (AFW) or Reactor Core Isolation Cooling (RCIC)], residual/decay heat removal, and cooling water support [Service Water (SW) and Component Cooling Water (CCW) systems]. Component unavailability baselines are required for EDGs; motor-driven pumps (MDPs), turbine-driven pumps (TDPs), and diesel-driven pumps (DDPs), respectively; and motor-operated/air-operated valves (MOVs/AOVs) [2].

The following definitions of the terms related to the data elements of interest are included in NEI-99-02 [59]:

> Unavailability is the ratio of the hours the train/system was unavailable to perform its monitored functions (as defined by PRA success criteria and mission times) due to planned and unplanned maintenance or test during the previous 12 quarters while critical to the number of critical hours during the previous 12 quarters. (Fault exposure hours are not included, and unavailable hours are counted only from the time of discovery of a failed condition to the time the train's monitored functions are recovered.)
>
> Unreliability is the probability that the train/system would not perform its monitored functions, as defined by PRA success criteria and mission times, when called upon during the previous 12 quarters.

The MSPI for each system is the sum of the Unavailability Index (UAI) due to unavailability for the system plus Unreliability Index (URI) due to unreliability for the system during the previous 12 quarters.

$$MSPI = UAI + URI \qquad \textbf{Eq. 6-1}$$

Unavailability is monitored at the train level for the purpose of calculating UAI, counted from the time the component or train is removed from service until it is restored to service.

Plant data for the UAI portion of the index includes:

- Actual train total unavailability (planned and unplanned) data for the most recent 12 quarter period collected on a quarterly basis
- Plant-specific baseline planned unavailability
- Generic baseline unplanned unavailability

Further information on the calculation of UAI is provided in Appendix F, Section F.1.3 of NEI 99-02 [59].

While the fact that the plant must collect and provide this train level unavailability information on a quarterly basis is useful, equipment unavailability information that is more directly relevant to the PRA unavailability data needs is usually available from the MR database (see Section 5.3.2 above).

Therefore, the MSPI unavailability information is primarily used by PRA database developers to:

- Verify the unavailability hours by system for those systems reported to MSPI.
- Provide a sanity check of unavailability basic events that should be retained in the PRA model.
- Obtain the list of surveillance test and preventive maintenance procedures included in the MSPI Basis Document. This indicates the documents that need to be reviewed to calculate the demands and run times related to test and non-test operation. Design basis documents and engineering support documents are also good sources of information.

An example of an MSPI Basis Document summary is shown in Table 6-3. However, since the MSPI data may not cover the entire data window for which PRA data is required, the listing of procedural references can be used to identify the history of demands and run times for the components of interest to the PRA.

Table 6-3
Example MSPI basis document surveillance test and preventive maintenance data

Reference (Surv Test or Preventive Maint Activity)	Test or Operation Non-Test	Frequency	Comments	P-14B Start Demands in 18 Months	P-14C Run Hours in 10 Months
QP-22	Test	Quarterly	Pump IST Performance Test. Test initiates 1 start of each pump each quarter.	5	5
QP-8	Test	Quarterly	Test initiates 2 starts per pump each test. During Refueling Outage, AB-5F/5G fulfills requirements of this test.	8	8
AB-5F/5G	Test	Refueling Outage	Sequencer Test starts all 3 pumps.	1	1
X-514	Test	Refueling Outage	Pump performance test.	3	3
YV-823	Test	Refueling Outage	Service Water System Flow Balancing initiates one start of each pump. In most cases, flow adjustments required and results in 2 pump starts.	3	3
			TOTAL ESTIMATE IN 18 MONTH PERIOD (TEST)	**20**	**20**
Equipment Rotation	Oper NT	Most Times Monthly	Monthly except for summer when all three pumps operate. With 2 pumps normally in service, pump rotation requires only 1 pump start.	6	10055
X-OPS896	Oper NT	As required	Pump oil change as required (assumed twice in 18 months).	2	2
SWP-218/219/220	Oper NT	As required	Pump packing replacement (assumed three times in 18 months).	3	3

Table 6-3 (continued)
Example MSPI basis document surveillance test and preventive maintenance data

Reference (Surv Test or Preventive Maint Activity)	Test or Operation Non-Test	Frequency	Comments	P-14B Start Demands in 18 Months	P-14C Run Hours in 10 Months
SW443	Oper NT	2 Years	Standby Start Calibration of all three pumps.	1	1
Basket Strainer Cleaning	Oper NT	As required	On average, assume one basket strainer cleaning each month.	18	18
Pump Cycling to Clear High Basket Strainer DP	Oper NT	As required	Assume each pump cycled once per month to clear high DP except in fall when pumps will be cycled twice per month.	21	21
			TOTAL ESTIMATE IN 18 MONTH PERIOD (Oper NT)	**51**	**10100**

6.3.3.2 Test Related Unavailability Data

The data analyst should verify that test-related unavailability is being reported in the MR or MSPI downtime data that is used. If not, as would be the case for many PRA-modeled components that are not in-scope or considered risk-significant in the MR, information on equipment unavailability due to testing can be obtained or derived from the plant Technical Specifications and maintenance records.

The following types of testing should generally be considered in terms of their potential impact on system unavailability:

1. System logic tests to ensure proper response to appropriate initiating signals
2. System flow and operability tests to verify that components, such as pumps and valves are in fact operable
3. System tests performed after discovering that a complementary safety system is unavailable, generally called tests after failure

It is usually not necessary to consider each hardware element individually since testing schemes are mostly performed at the subsystem level.

However, it is particularly important to evaluate the testing performed on redundant portions of a system and the constraints of the Technical Specifications should be understood, evaluated, and properly addressed in the fault tree. A thorough understanding of the testing impact on system hardware and operational preferences is important for completeness of the data analysis and provides crucial insights into the overall system operability.

6.3.3.3 Operator Logs or Other Estimation Techniques

For equipment that is not included in the MR availability database or the MSPI data set, the real time plant computer operating data or Operator Log searches should be performed by equipment ID number for data window timeframe. Equipment should be considered out of service when the associated breaker is disconnected, or if the equipment is logged as “out-of-service” or “equipment status not available.” In many cases, this information is provided by identifying one or more tag-ins and tag-outs, and should be discussed with System Engineers and Operations personnel. Using these times may be a slightly conservative because the repair may be completed before the component is declared tagged in. For single unit sites, equipment outages during refueling outages should not be counted as out-of-service time and maintenance performed during shutdowns is not included in the determination of component unavailability during power operation. However, for multi-unit plants, credit can be taken in the PRA for successfully providing a support function for an operating unit when the unit normally associated with the SSC is shut down and this should be factored into the unavailability estimate, as discussed in the footnote in section 6.4.

EPRI TR-100381 [58] provides the following guidelines for allocating unavailability due to test or maintenance:

1. If the cause of unavailability of a standby component is self-revealing at the time it occurs (for example, control room alarm), or occurs during a test, but is revealed at the end of a test and results in maintenance, the event is accounted for in the unavailability due to maintenance. If the failure is such that it could also occur while the component is performing its mission, it should be counted towards that basic event also.
2. Failures, such as leaks of components such as pumps and valves, which are not serious enough to be failures of the pressure boundary by an accepted definition, would be included in the unavailability due to maintenance as their effect is to induce maintenance activity.
3. An event reported as a failure to meet tech specs, but which would not result in a catastrophic failure in the PRA sense, should not be included, but may lead to maintenance unavailability.
4. Problems arise when a component is taken out for maintenance because it is in a degraded state, but not yet failed. If the degraded failure is revealed in short test duration, could we be sure the component would have succeeded in its mission? In this case, some judgment has to be applied in extrapolating the rate of degradation to the mission time.

NOTE: The ASME/ANS PRA Standard supporting requirement DA-C13 indicates that when reliable estimates for the start and finish times are not available, knowledgeable plant personnel (for example, engineering, plant operations, and so on) should be interviewed to generate estimates of ranges in the unavailable time per maintenance act for components, trains, or systems for which the unavailabilities are significant basic events. Ref. [14] provides a structured interview technique for obtaining this information and a way to account for individual biases.

6.4 Data Calculation

The equation used to calculate unavailability is:

$$\frac{\text{Planned unavailable hours + unplanned unavailable hours}}{\text{Required operational hours}^{4}} \qquad \textbf{Eq. 6-2}$$

[4] Required operational hours are the number of hours that the SSC serves a safety function. The safety function (and the need to count required hours), may be necessary at all times, or may be dependent on reactor mode, criticality, fuel in the reactor vessel, or other factors. The degree of redundancy for SSCs performing a safety function may vary based on factors as described above, and the determination or required operational hours may take this into account. However, determination of required operational hours should include consideration that an SSC may be used for establishment of backup success paths or compensatory measures. Required operational hours may include times beyond those for which SSC operability is required by Technical Specifications. [68] For multi-unit plants, credit is taken in the PRA for successfully providing a support function for an operating unit when the unit normally associated with the SSC is shut down.

Another way of characterizing unavailability is the following:

$U = \frac{T_{oos}}{T_{Total}}$	Component unavailability due to test and maintenance; probability that the component is down for test and maintenance at a random point in time when demanded to perform its function
T_{OOS}	Component-hours out of service for test and maintenance and unable to perform its function
T_{Total}	Component hours of time during which the out of service time is collected

Some additional items to note regarding test unavailability:

- Frequency and duration of testing is typically available from plant surveillance procedures.
- Only address testing that makes equipment unavailable.
- Typically, testing when equipment is automatically reconfigured on safety demand can be omitted from unavailability calculations.

T_{Total} can also be considered the time that the component is "required" to operate (also required time). Required times for each component should be adjusted to distinguish between those components that are required to be operable at all times and those that are only required when the reactor is critical. For example, at some plants, the RHR pumps are only considered to be required and operable in the at-power PRA model when the reactor is critical. In that case, the time during cool-down, time during refueling when the reactor is de-fueled, or time during plant shutdown would not be included.

Note that it may be desirable to include some unavailability terms in the PRA model only for use in the online risk monitor model (for example, equipment out-of-service (EOOS) monitor) even though there is no expected unavailability for these components.

If the actual outage time of a component during the data period is zero, then a basic event for this unavailability is probably not needed. However, for completeness the minimum unavailability of a PRA modeled component can be estimated with a placeholder assumption using the following equation:

$$Minimum\ Availability = \frac{1\ hour}{365\ {}^{days}/_{year} * 24\ {}^{hours}/_{day}} * \frac{0.5}{20\ years} = 2.85E-06$$

where the example presumes that the minimum estimated outage time due to test or maintenance is 0.5 hours and the plant has been in service 20 years.

Regarding uncertainty for unavailability estimates, NUREG/CR-6928[4] states that component or train UAs are characterized by beta distributions and for their unavailability calculations, the simplified constrained noninformative distribution ($\alpha = 0.5$) was used (see Section 3 for further information).

6.5 Coincident Unavailability

Coincident maintenance unavailability is associated with simultaneous maintenance for redundant equipment, both intrasystem and intersystem. Coincident unavailability is a result of a planned, repetitive activity and can arise for systems with installed spares.

The ASME/ANS PRA Standard [7] includes specific SRs for this data category, namely:

- SY-A20: Include simultaneous planned redundant equipment unavailability.
- DA-C14: Calculate planned repetitive coincident redundant equipment unavailability.

Some plants may have more redundancy than required by Technical Specifications, also known as "installed spares". For example, there may be a third train that is out of service for extended periods of time coincident with one of the other trains, but is still in compliance with tech specs.

An example of intersystem unavailability would be taking multiple components out of service on a train basis (such as AFW train A and HPI train A at a PWR, or RHR train A and LPCS train A at a BWR).

The ASME/ANS PRA Standard Supporting Requirement DA-C14 covers only planned repetitive maintenance activities. Development of unavailability estimates for unplanned emergent work in conjunction with normal on-line maintenance is not required by the standard. Similarly, development of unavailability estimates for planned but not repetitive coincident maintenance unavailability configurations is also not required. Plant experience shows that in most cases, only one piece of equipment from a train is removed from service at a time.

The PRA data analyst can confer with the plant Risk Monitor analyst (see Section 2 for a discussion of Risk Monitor vs. PRA) to identify any plant-specific maintenance practices that could result in coincident unavailability.

Another means for evaluating coincident unavailability is to review the MR unavailability data to identify any coincident events for each train. For any coincident unavailability instances that are initially identified, discussions with plant maintenance personnel are recommended to clarify whether the cases are actually coincident or not.

A review of unavailability data for one plant showed that there was limited, repetitive coincident unavailability; most cases involved only two components, and occurred only once in a three-year data window.

There are, however, a few cases in which plant experience has shown that two components from the same train were recurrently removed from service at the same time. In these cases, coincident unavailability was modeled. Coincident unavailability includes only the time that both components are simultaneously unavailable. If one component is unavailable for an extra hour, that hour is used in the individual unavailability.

Once coincident unavailability is calculated, the times are subtracted from the individual unavailability values to avoid double counting. This is usually a negligible effect on individual train unavailabilities.

6.6 Standard and Regulatory Requirements

ASME/ANS RA-Sa–2009 [9] contains the following supporting requirements in the technical element of component data analysis that are relevant to maintenance unavailability data:

- DA-C11 – Include maintenance and test duration data that could leave equipment unable to perform its PRA modeled function when demanded.
- DA-C12 – Count support system unavailability that causes front line component availability against the support system (not the frontline system).
- DA-C13 – Assess outage durations of equipment for various activities (test and maintenance), but only at power for maintenance. Identify shared systems for multi-unit sites and associated tech spec requirements. Use operator interview data when accurate start and finish times are not available from plant process data.
- DA-C14 – Evaluate redundant equipment coincident availability.

In addition, the following Supporting Requirements from other areas of the standard apply to and interface with the maintenance unavailability estimation:

- SY-A19 – Include out-of-service unavailability for components in the system model, unless screened.

6.7 Guidance per Findings and Experience

Peer Reviews have been and continue to be conducted to evaluate the technical adequacy of Internal Events PRAs against the ASME/ANS PRA Standard guidance for the technical element of data analysis. The following issues reflect findings that have been made in recent PRAs in the chapter topic area and recommended guidance based upon finding recommendations and PRA data practitioner experience.

1. Maintenance Unavailability during Power Operation per ASME/ANS PRA Standard SR DA-C13

   Finding: Other than firewater, the two units do not share anything, so the multi-plant site issues are not relevant. MR data are used. MR counts unavailability while the plant is down, if that system is required to be operable during shutdown. Inclusion of shutdown data may bias the results, especially for EDGs, where the shutdown unavailability value is approximately five to 10 times the at-power value.

   Recommended Resolution: Per the PRA Standard, include only outages occurring during plant at-power by reviewing MR data to remove unavailability during shutdown.

2. Operator Interviews for Maintenance Unavailability per ASME/ANS PRA Standard SR DA-C13

   Finding: PRA Appendix D1, Section 3.7 says “If no Maintenance Rule or plant records were available for a particular component, generic data from NUREG/CR-6928 were used to estimate unavailability.” This is conservative so it meets Capability Category I, but no operator interviews were performed, so Capability Category II is not met.

Plant response: The MR Coordinator and/or the appropriate system engineers were queried regarding the systems for which MR availability was not monitored. Based on the inability of the plant personnel to provide reliable estimates, generic data were applied to these system components. These interviews, however, were admittedly not well documented.

3. Inter-system Coincident Maintenance per ASME/ANS PRA Standard SR DA-C14

   Finding: No intersystem coincident maintenance analysis was found to be performed. This may be important, particularly on an accident sequence functional requirement.

   Recommended Resolution: Perform an intersystem coincident maintenance analysis by reviewing the quarterly maintenance schedule, interview scheduling personnel, and reviewing EOOS entries. If coincident maintenance is found of consequence, add new basic events to model and revise documentation as appropriate.

7
COMMON CAUSE FAILURE (CCF) DATA

7.1 Introduction

A common cause failure (CCF) occurs when two or more components fail or enter a degraded state due to the same cause and at the same time or in a short interval of time in relation to the component mission time. CCFs are a special class of dependent failures that are emphasized in developing and quantifying PRA models due to their high level of risk significance.

Historically, multiple component failures usually occur because of the failure of something else that impacts them. CCF modeling is therefore performed because of a lack of knowledge about the root causes of those multiple failures and the need to postulate their occurrence to be thorough in the PRA.

The main source of CCF data is generic information that was collected from a spectrum of plants and was used to develop factors that are then applied toward calculating CCF rates for various standard equipment types. This chapter discusses the steps that are followed, the different models that are used, and how they are implemented to develop the data needed for CCF basic events in the PRA model.

7.2 Methodology

Common Cause Failure Analysis (CCFA) is typically addressed in a PRA as follows:

- The PRA **System Analysis task** identifies where common cause failure modeling is needed in the fault tree models and specifies the CCF Basic Events in the System Notebooks.
  - Note, however, that since there are usually multiple system analysts on a PRA, the Data Analysis task needs to coordinate all the analysts/notebooks.
- The **Data Analysis task** performs the following:
  - Reviews plant-specific failure history to ensure that any significant CCF events that have occurred are considered in the quantification. The rationale for screening out plant-specific failures must be documented in the Data Analysis Notebook.
  - Reviews the CCF basic events in the System Notebooks to:
    - Ensure that the component boundaries and failure modes are clear and consistent.
    - Identify the common cause group size (CCCG) based on the number of components in the group and the number presumed failed in each basic event.
    - Determine whether the component undergoes staggered or non-staggered testing.
  - Selects generic distributions from one of the CCF model approaches discussed in this chapter.
  - Provides CCF data input for the CCF basic events identified by the PRA systems analysts based on the format required by the PRA model software used (for example, CAFTA, SAPHIRE).

7.3 CCF Event Definition

The identification of systems and components to model common cause is based on the methodology presented in NUREG/CR-5485 [70].

7.3.1 CCF Event Screening and Plant-Specific Data Review

Screening criteria are used to identify the most-likely common cause failures while excluding components that are relatively insensitive to common cause failure. Screening is done on the basis of system-specific configuration, the potential failure mode for the component, and factors such as multiple component spatial location and environmental conditions. Examples of screening criteria, drawing from PRA experience and Appendix A of NUREG/CR-4780 [71], are shown in Table 7-1.

Table 7-1
Common cause failure event screening criteria

Screening Criteria	Rationale
CCFs to Include	
Major component types and failure modes	CCFs of pump failure to start and run, and motor operated valve failure modes have the greatest system impact.
Identical redundant components within a system	Components within a system that are identical and represent redundancy would have significant CCF impact in the PRA logic model.
Components located near each other	Plant-specific data suggest that CCFs are an issue for like component types located in close proximity to each other.
CCFs to Exclude	
Passive failures	Passive component failures are excluded since 1) their occurrence is anticipated to be extremely low compared to active component CCFs, and 2) the failures are usually due to individual failures based on plant-specific data reviews. EXCEPTION: Strainer plugging CCF would be included because strainer failures tend to affect more than one component, whereas a manual valve transferring closed, for example, does not.
Less frequent failure modes	If pump failure to start and run, and motor operated valve failure modes exist, then other less frequent events may be neglected.
Redundant devices that provide an insignificant contribution	For example, common cause failures of redundant actuation devices in a single train system that requires a pump to start and motor operated valves to open based on initiation signals from redundant sources would be neglected. This is because failure would be dominated by the failure of the pump or MOV, each in single element cutsets.
Cross-system CCFs if no strong link is identified	Systems that have a different function, are not physically connected and/or are at different locations separated by barriers may be excluded since the CCF potential is low.

Some component dependencies are explicitly treated in other phases of the fault tree or PRA analyses and, to avoid double counting, should not be included in this CCFA. Examples of these are:

- Functional Dependencies – There are many examples of dependent failures that arise from the functional dependence of a component or set of components on the same functional inputs such as an actuation signal, electric power supply or component cooling input. Multiple failures associated with loss of common support functions or inputs are explicitly modeled in the event tree and fault tree logic and hence should not be included in the CCFA.
- External Events – Dependencies among component failures due to the effects of "external" events (earthquake, fire, flood) are treated explicitly in the PRA by selecting these events as common cause initiating events and explicitly modeling the probability that damage from these events extends to various combinations of components and structures in the plant. Therefore, these events are not included in the CCFA.
- Human Errors – Human errors such as 1) incorrect calibration of sensors or instruments, and 2) failure to restore components to service after their isolation for test or maintenance are included as separate basic events in the fault trees known as pre-initiator Human Failure Events (HFEs). These multiple coincident component disablements due to test and maintenance-related human actions should not be included in the CCFA.
- Maintenance and Testing Unavailability – Unavailability of multiple components due to maintenance, repair (unscheduled corrective maintenance), and testing are included as separate events in the system fault trees and are quantified as discussed in Section 5.

While it is primarily the job of the system analyst to identify CCFs for inclusion in the PRA model, a review of the events included in the CCFA against these other categories should be conducted to ensure that double-counting does not occur.

In addition, plant-specific failures contained in the EPIX database should also be reviewed by the data analyst against the Table 7-1 screening criteria. This is done to ensure that any significant plant-specific events that have occurred are considered in the quantification. It is recommended to discuss any suspected CCF events with plant maintenance personnel to clarify whether or not the events are “real,” since database descriptions can be cryptic.

Most often, the plant-specific data either substantiates the generic CCF data categories or is screened from further consideration based on the criteria in Table 7-1.

Some examples of plant-specific data screening are:

- The plugging of an instrument line header was not included as a common cause failure because the plugging was considered minor and no instances of plugging had been documented in corrective action reports either prior to or since that event.
- Thermal binding that caused a single motor operated valve failure to open was not considered a common cause failure as it was unique to that valve and was not observed in any other MOVs.

NOTE: CCFs for components that could fail due to a common operator error because they are all affected by the same emergency or normal operating procedures are addressed in the Human Reliability Analysis (HRA) task.

7.3.2 CCF Component Boundary and Failure Mode Definition

Boundaries for the CCF event are based on consideration of the fault tree modeling and data collection boundary for the corresponding independent failure event as discussed in Section 5.2.1. Sub-components that would be considered along with the major component include:

- Couplings between the motor and a pump
- Actuator, valve, and power supply circuit breaker in a motor operated valve
- Turbine and pump for a turbine-driven pump component
- Engine, generator, starting/control air, and output breaker for an emergency diesel generator

NOTE: It has been observed that the boundaries provided in NUREG/CR-6928 are not defined in the same manner or to the same level of detail as they are in the NRC CCF database. There may be overlap in the boundaries and these are believed to result in conservative estimates of the CCF failure rates.

The failure modes of interest to the PRA for the CCFs come from the independent component failure basic events. For example, the CCF events for the diesel generator would use the same failure to start or failure to run failure modes as for the individual component failure data (developed as discussed in Section 5).

7.3.3 Common Cause Groupings

Common cause groupings are established for redundant components with similar design, function and operating/maintenance considerations and are assigned unique identifiers (common cause failure basic events). Although this step may be done initially by the system analyst, it is important for the data analyst to understand the basis for the groupings for proper generic data application.

A set of components should be defined as a common cause component group (CCCG) when they are of the same component type (pumps, valves, and so on), and when they meet the following conditions:

- Same initial conditions (for example, normally open, normally closed, energized, deenergized) and operating characteristics (for example, normally running, standby). One valve that is normally open and another valve which is normally closed should not be included the same CCCG.
- Same use or function such as system isolation, flow modulation, parameter sensing, motive force, and so on. For example, a check valve in the injection lines of the safety injection system (which prevents flow of primary coolant into the system) and a check valve in the discharge line from a pump (which provides backflow through an idle pump) should not be included in the same CCCG as they are subject to different system conditions (for example, pressure, flow) both in standby and during system operation.
- Same failure mode (failure to open on demand, failure to start on demand, and so on). Two similar pumps that both fail to start and run should be included in the same group.

- Same service condition (clean water or raw water).
- Same safety classification.
- Same maintenance practices.
- Same unit (or across multiple units if the operating conditions are consistent).

The above conditions are used to account for factors affecting component interdependence and to identify the presence of identical redundant components.

Table 7-2 shows an example of component groupings for typical NPP PRA systems and components, where a unique CCF group name is allocated based on system, component type, number of components, and failure mode.

Table 7-2
Example CCF component grouping (CCCGs)

System	CCF Group	PRA Component	Population	Failure Mode
DC Power (DC.CAF)	QDCBATTERY	Battery	2	Fails on demand
	QDCBATCHG	Battery Charger	4	Fails during operation
Fire Water (FP.CAF)	QFPFPCKVS	Check Valves	2	Fail to Open
Service Water (SW.CAF)	QSW3PMPR	Pumps	2	Fail to Run
	QSWSPMPSTR	Pumps	2	Fail to Start
	QSWSPMPRUN	Pumps	2	Fail to Run 1st Hour
	QSWSBRMPRUN2	Pumps	2	Fail to Run After 1st Hour
	QSWSCVOPEN	Check Valves	2	Fail to Open
Instrument Air (AS.CAF)	QASCMPRPFTS	Compressors	4	Fail to Start
	QASCMPRFTR	Compressors	4	Fail to Run
	QASDRYISOL	AOV	4	Fail to Close
	QASDRYBYPSS	AOV	2	Fail to Open

It should be noted that while it is possible to model CCFs of CCCGs greater than 4, this practice is not recommended for the following reasons based on EPRI experience with the application of the CAFTA PRA software [56]:

1. There is no solid data basis for quantifying groups greater than 4, substantiated by the MGL method truncation at groups of 4 [70, 71] and the CAFTA PRA software CCF module input limits of alpha factor and MGL parameters to a maximum of those used for groups of four components.
2. Adding complexity to the PRA model through large CCF groups slows down the calculation time with no real analytical benefit.
3. The PRA cutsets become more difficult to review and resolve with reasonable recovery rules.

7.3.4 Staggered vs. Non-Staggered Testing

This step establishes whether the CCCG being considered is tested in a staggered or non-staggered fashion. The component testing interval has a significant bearing on the calculation of CCF factors because it is assumed that CCFs are most often discovered as a result of scheduled testing.

Staggered testing schemes test one component at a time in a multiple component system, at different test intervals (for example, in a two pump system, pump A is tested in the first and third quarter and pump B is tested in the second and fourth quarter). If a failure occurs in the first tested component, an evaluation would immediately be performed on the other components in the system to assess the likelihood of a common mode failure and to determine if additional unscheduled tests are required. This approach provides an additional layer of protection against CCF, as the likelihood of an undetected CCF event would be reduced.

Non-staggered testing is when testing of all like components in a system is performed at the same time.

Staggered testing is more desirable for equipment reliability, as it provides an additional layer of protection against CCF. This is because the potential exposure time for undetected failures is much shorter for a staggered testing scheme with associated verification compared to the exposure time for a corresponding non-staggered testing scenario. It is also assumed that when one component is found in a failed condition as the result of a staggered testing scheme, an evaluation is performed on the corresponding identical components to assess their functionality and determine if unscheduled tests are required.

If the testing scheme cannot be established as either staggered or non-staggered, assuming that non-staggered testing is done results in a slightly higher CCF factor for most terms.

7.4 Calculation of Common Cause Basic Event Failure Probabilities

There are a number of accepted methods for calculation of common cause event failure probabilities that are supportable with the currently available data on common cause events. These methods each include a parametric model and a set of procedures for estimating the numerical values of the common cause parameters defined for that model from generic industry and plant-specific data. The models include the Basic Parameter model [70], beta-factor method [71], MGL method [70, 71], and alpha factor method [72, 73]. A comparison of these methods is provided in Table7-3, including the PRA standard capability category addressed by their use.

Table 7-3
CCF method summary

CCF Method	Pros	Cons	Capability Category [7]
Basic Parameter	Assumes that probability of each independent and common cause event is symmetric. Useful in explaining similarities and differences of alternative common cause models.	Difficult to estimate parameters from experience data.	CCII when used for significant basic events; CCIII when used for all CCF basic events
Beta factor	Simple model. Used to model dependencies between redundant and identical components of a system.	For systems with more than two components or trains (m>2), the pure application of the beta factor method does not provide a distinction between different numbers of multiple failures. This simplification can lead to conservative predictions that are only adequate for screening values or for final quantification of low-risk significance basic events.	CCI
MGL	Based on Beta but can distinguish among common cause events affecting larger numbers of components in a higher order redundant system.	Normally applied to common cause groups of up to four components. With more than four components, it is normally assumed that any common cause event that would fail four components would fail all components in the group. MGL parameters are mutually interdependent, but not addressed during uncertainty quantification and tend to result in a slight understatement of the variance of the resulting uncertainty distributions.	CCII when used for significant basic events; CCIII when used for all CCF basic events
Alpha factor	Industry-wide alpha factors are available from the NRC operational experience website [21], are regularly updated and have been developed from experience data collected at nuclear power plants. Uncertainty is more tractable for the Alpha factor method than for MGL (per NUREG/CR-6823 [13]).	Very similar to MGL method, except provides a model to treat CCF probabilities of *k*-of-*m* components (beyond groups of four) – this may encourage excessive model complexity.	CCII when used for significant basic events; CCIII when used for all CCF basic events

The key assumption in all these CCF models is that the probability of each independent and common cause event is symmetric. This means that the probability of a common cause event, which is dependent on the total number of components failed by the event, is independent of the specific combination of components affected.

The basic concepts of these methods are discussed below, while the practical issues involved in estimating the model parameters are discussed in Section 7.5.

7.4.1 Basic Parameter Model

As explained in NUREG/CR-4780 [70], all parametric CCF models can be derived from a simple "Basic Parameter Model," which states that each common cause basic event in the expanded fault tree can be defined as a basic parameter: $Q_k^{(m)}$, which is defined as the probability of failure of the event that fails exactly k components in a CCCG of m identical components.

When k = 1, the event corresponds with the independent failure of the component, whereas when $k \geq 2$, the events are the common cause events. In the extreme case of k = m, the event is the global common cause event (also referred to as a lethal shock event) that fails all m components in the CCCG.

An example of how the Basic Parameter Model works for CCCGs from 1 to four components is shown below:

$$Q(A) = Q(B) = Q(C) = Q(D) = Q_1^{(4)} \quad \textbf{Eq. 7-1}$$

$$Q(AB) = Q(AC) = Q(AD) = Q(BC) = Q(BD) = Q(CD) = Q_2^{(4)} \quad \textbf{Eq. 7-2}$$

$$Q(ABC) = Q(ABD) = Q(ACD) = Q(BCD) = Q_3^{(4)} \quad \textbf{Eq. 7-3}$$

$$Q(ABCD) = Q_4^{(4)} \quad \textbf{Eq. 7-4}$$

The use of superscripts in the above equations adds emphasis to the fact that the basic event parameters are in general a function of the size of the group. The probability of a CCF of two specific components in a group of three components is therefore not equal to the probability of a CCF of two specific components in a group of four components, everything else being equal. This complication makes it difficult to estimate parameters from service data for this method. However, the Basic Parameter method has played a useful role in explaining the similarities and differences of alternative common cause models.

7.4.2 Beta-Factor Method

The beta factor method is most often applied to model dependencies between redundant and identical components of a system. The underlying assumption behind this simple model is that there are two extreme types of failures, those that occur independently for each component, and CCFs that result in complete failure of all components in a CCCG.

The beta factor method assumes that Q, the total (constant) failure probability for each component, can be expanded into independent and common cause failure contributions:

$$Q = Q_i + Q_{cc} \quad \textbf{Eq. 7-5}$$

where Q_i is the unit failure probability for independent failures and Q_{cc} is the unit failure probability for CCFs.

For convenience, a parameter β is defined as the fraction of the total failure probability of the component that is attributable to common cause failures:

$$\beta = \frac{Q_{cc}}{Q_i + Q_{cc}} = \frac{Q_{cc}}{Q} \quad \textbf{Eq. 7-6}$$

so that

$$Q_{cc} = \beta Q. \quad \textbf{Eq. 7-7}$$

The above definitions can be used to derive expressions for the overall unreliability or failure probability of a multiple-unit system combining dependent and independent failures where appropriate.

When this model is applied to a CCCG of m components, the underlying assumption is that all CCFs will impact all m components. Under this assumption, its relationship to the basic parameter method can be defined as:

$$Q_i = Q_1^{(m)} = (1-\beta^{(m)})*Q \quad \textbf{Eq. 7-8}$$

and

$$Q_{cc} = Q_m^{(m)} = \beta^{(m)}*Q \quad \textbf{Eq. 7-9}$$

where

$\beta^{(m)}$ = "beta", the 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 for a common cause group of size *m*.

Again, since the basic parameter terms are dependent on the size of the common cause group, so is $\beta^{(m)}$, and, therefore, the beta factor for a group of two components, everything else being equal, will not be the same as the beta factor for a group of three or four components, and so on. For this reason, the superscript is used to show this dependence.

For systems with more than two components or trains (m>2), the pure application of the beta factor method does not provide a distinction between different numbers of multiple failures. This simplification can lead to conservative predictions that are normally adequate for screening values or for final quantification of low-risk significance basic events. For this reason, the beta factor method only satisfies Capability Category I of the ASME/ANS PRA Standard.

For common cause basic events in CCCG sizes of three or greater and that have a high level of safety significance (that is, with Fussell-Vesely (FV) basic event importance values of more than 0.001) or for events in these larger groups whose realistic quantification may be needed for specific applications, the MGL or alpha factor method should be used.

7.4.3 Multiple Greek Letter Method

The MGL model [71] is an extension of the beta factor method. In this method, other parameters in addition to the beta factor method are introduced to distinguish among common cause events affecting larger numbers of components in a higher order redundant system.

The MGL parameters consist of a set of failure fractions used to quantify the conditional probabilities of all the possible ways a CCF of a component can be shared with other components in the same group, given component failure has occurred. For a system of "m" redundant components and for each given failure mode, "m" different parameters are defined.

All parameters are applicable to a specific failure mode associated with a failure probability, Q.

Q = total single-component failure probability, accounts for both independent and CCF modes affecting that component [74].

$\beta^{(m)}$ = "beta," the 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 for a common cause group of size *m* [74].

$\gamma^{(m)}$ = "gamma," the 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 for a common cause group of size *m* [74].

$\delta^{(m)}$ = "delta," the conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more additional components, given that three specific components have failed for a common cause group of size *m* [74].

The MGL method is normally applied to common cause groups of up to four components. With more than four components, it is normally assumed that any common cause event that would fail four components would fail all components in the group.

The general equation that expresses the probability of multiple-component failures due to common cause, $Q_k^{(m)}$ as defined in the Basic Parameter model in terms of the MGL model parameters is given by:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^{k} \rho_i \right) (1 - \rho_{k+1}) Q_t \qquad \text{Eq. 7-10}$$

$\rho_1 = 1, \rho_2 = \beta, \rho_3 = \gamma, \rho_4 = \delta \ldots \rho_{m+1} = 0$

where "m" is the number of components in the common cause group, and "k" is the number of specific components that fail such that $1 < k < m$. The binomial coefficient

$$\binom{m-1}{k-1} = \frac{(\text{m-1})!}{(\text{m-k})!(\text{k-1})!} \quad \text{Eq. 7-11}$$

represents the number of different ways that a specific component can fail with (k-1) other components in a group of (m-1) similar components.

Note that for two components, the MGL and beta factor methods are equivalent. The following equations express the probability of multiple component failures due to common cause in terms of the MGL parameters for a three-component common cause group:

$$\boldsymbol{Q_1^{(3)} = (1 - \beta)Q_t} \quad \text{Eq. 7-12}$$

$$\boldsymbol{Q_2^{(3)} = \frac{1}{2}\beta\,(1 - \gamma)Q_t} \quad \text{Eq. 7-13}$$

$$\boldsymbol{Q_3^{(3)} = \gamma\beta Q_t} \quad \text{Eq. 7-14}$$

where

$Q_t = Q_1^{(m)} + Q_m^{(m)}$ = the total failure frequency of each component due to all independent and common cause events; per Appendix A of NUREG/CR-5485 [70].

The equations for a four-component common cause group are the following:

$$\boldsymbol{Q_1^{(4)} = (1 - \beta)Q_t} \quad \text{Eq. 7-15}$$

$$\boldsymbol{Q_2^{(4)} = \frac{1}{3}\beta\,(1 - \gamma)Q_t} \quad \text{Eq. 7-16}$$

$$\boldsymbol{Q_3^{(4)} = \frac{1}{3}\beta\gamma\,(1 - \delta)Q_t} \quad \text{Eq. 7-17}$$

$$\boldsymbol{Q_4^{(4)} = \beta\gamma\delta Q_t} \quad \text{Eq. 7-18}$$

The parameters that are input to the MGL formulas are extracted from the CCF Parameter Estimations document downloaded from the NRC operational experience website [21] and the values are selected for the component type and failure mode that corresponds to the individual component failure rate and mode.

7.4.4 Alpha Factor Method

The alpha factor method was developed in Reference [72] to address a limitation of the MGL method that arises when performing quantitative uncertainty analysis. This limitation is created by the mutual interdependence of the MGL parameter definitions, which is normally ignored during uncertainty quantification and this tends to result in a slight understatement of the variance of the resulting uncertainty distributions [75]. However the MGL and alpha factor methods produce the same mean point estimates of the CCF probabilities and the uncertainty impact is very small, not enough to justify changing existing MGL models to alpha factor models. The alpha factor method is very similar to the MGL method, except that instead of expressing fractions of failures in a

component that are of a common cause character, it uses fractions of failure that occur in a system. While the alpha factor method provides the same point estimates as the MGL for a given interpretation of the data, the alpha factor method provides a more complete and robust quantification of the uncertainties than MGL. Details on the development and application of the alpha factor method are found in References [70] through [73].

The alpha factor method provides a model to treat CCF probabilities of *k*-of-*m* components. In addition, industry-wide alpha factors have been developed by the NRC from experience data collected at nuclear power plants and are available on their website [21].

The alpha factor method differentiates between staggered and non-staggered testing schemes (as defined previously in Section 7.3.4) for the determination of the correct CCF formula.

General formulas for the alpha factor method from NUREG/CR-5485 [70] are provided below:

Staggered testing scheme:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \qquad \text{Eq. 7-19}$$

Non-staggered testing scheme:

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad \text{Eq. 7-20}$$

where:

$$\binom{m-1}{k-1} = \frac{(\text{m-1})!}{(\text{m-k})!(\text{k-1})!} \qquad \textbf{Eq. 7-21}$$

$Q_k^{(m)}$= probability of a common cause basic event involving *m* components in a CCCG of *k* size

α_k= fraction of total frequency of failure events that occur in the system and involve the failure of k components due to a common cause

m = CCCG size

k = number of failures of components in CCCG needed for failure of system

$\alpha_t = \sum_{k=1}^{m} k\, \alpha_k\, Q_t$ = total failure frequency of each component due to all independent and common cause events; per the footnote to Table 5-4 in NUREG/CR-5485 [70],

$$Q_t = Q_1/\alpha_1 \qquad \textbf{Eq. 7-22}$$

where Q_1 is the independent failure rate for the individual component type and failure mode of interest, calculated as discussed in Section 5, and α_1 is the alpha factor parameter for the first term.

Table 7-4 provides the equations for the alpha factor method for basic event level CCF estimation.

Table 7-4
Alpha factor basic event CCF equations

CCCG Size (m)	No. of Failed Components (k)	Alpha Factor CCF Basic Event Probability Equation	
		Staggered Testing	Non-Staggered Testing
2	1	$\alpha_1 * Q_t$	$1 * \alpha_1/\alpha_t * Q_t$
	2		$2 * \alpha_2/\alpha_t * Q_t$
3	1	$\alpha_1 * Q_t$	$1 * \alpha_1/\alpha_t * Q_t$
	2	$1/2\ (\alpha_2 * Q_t)$	$1 * \alpha_2/\alpha_t * Q_t$
	3	$\alpha_3 * Q_t$	$3 * \alpha_3/\alpha_t * Q_t$
4	1	$\alpha_1 * Q_t$	$1 * \alpha_1/\alpha_t * Q_t$
	2	$1/3\ (\alpha_2 * Q_t)$	$2/3 * \alpha_2/\alpha_t * Q_t$
	3	$1/3\ (\alpha_3 * Q_t)$	$1 * \alpha_3/\alpha_t * Q_t$
	4	$\alpha_4 * Q_t$	$4 * \alpha_4/\alpha_t * Q_t$
5	1	$\alpha_1 * Q_t$	$1 * \alpha_1/\alpha_t * Q_t$
	2	$1/4\ (\alpha_2 * Q_t)$	$1/2 * \alpha_2/\alpha_t * Q_t$
	3	$1/6\ (\alpha_3 * Q_t)$	$1/2 * \alpha_3/\alpha_t * Q_t$
	4	$1/4\ (\alpha_4 * Q_t)$	$1 * \alpha_4/\alpha_t * Q_t$
	5	$\alpha_5 * Q_t$	$5 * \alpha_5/\alpha_t * Q_t$
6	1	$\alpha_1 * Q_t$	$1 * \alpha_1/\alpha_t * Q_t$
	2	$1/5\ (\alpha_2 * Q_t)$	$2/5 * \alpha_2/\alpha_t * Q_t$
	3	$1/10\ (\alpha_3 * Q_t)$	$3/10 * \alpha_3/\alpha_t * Q_t$
	4	$1/10\ (\alpha_4 * Q_t)$	$2/5 * \alpha_4/\alpha_t * Q_t$
	5	$1/5\ (\alpha_5 * Q_t)$	$1 * \alpha_5/\alpha_t * Q_t$
	6	$\alpha_6 * Q_t$	$6 * \alpha_6/\alpha_t * Q_t$

Note:
The alpha values are specific to a given CCCG group. For example, the α_1 for CCCG =2 is different than the α_1 for CCCG = 3. These values are obtained from the common cause database on the NRC operational experience website [21]. The α_t changes for each CCCG group as well.

A walk-through will now be presented for an example using motor-driven pump data.

For the CCCG size $m = 3$ for a staggered testing scheme, the following equations from Table 7-5 apply:

Table 7-5
CCF equations for example CCCG size m = 3

No. of Failed Components (*k*)	Alpha Factor CCF Basic Event Probability Equations for Staggered Testing
1	$\alpha_1 * Q_t$
2	$1/2\ (\alpha_2 * Q_t)$
3	$\alpha_3 * Q_t$

For $k = 1$, the formula is $\alpha_1 * Q_{t,}$, where $Q_t = Q_1/\alpha_1$.

The variable Q_1 is the individual failure rate for the component type and failure mode being considered for the CCF group. In this case, MDP data from NUREG/CR-6928 [4] for "MOTOR DRIVEN PUMP FAIL TO START ALL SYSTEMS SPAR: MDP-FS" was used, from Table A.2.27-7, Running/Alternating, FTS. The mean value is 0.002.

The value α_1 comes from the CCF Parameter Estimations document downloaded from the common-cause database on the NRC operational experience website [21] and the values are selected for the component type and failure mode that corresponds to the individual component failure rate and mode. Since MDP data for "MOTOR DRIVEN PUMP FAIL TO START ALL SYSTEMS SPAR: MDP-FS" was used, the alpha factor parameters used are from section 1.1.1, page 11 of the 2010 parameter estimations. For CCCG = 3, the mean value for α_1 is 0.9762240. A screenshot of the parameter estimate from the database is given in Figure 7-1.

MOTOR DRIVEN PUMP FAIL TO START ALL SYSTEMS SPAR: MDP-FS

Component :	Motor Driven Pump
Failure Mode :	Fail to start
Start Date :	1997/01/01
Data Version :	2010/12/31

Total Number of Independent Failure Events: 557.40
Total Number of Common-Cause Failure Events: 23

ALPHA FACTOR DISTRIBUTIONS

CCCG = 2

Alpha Factor	5th%	Mean	Median	95th%	MLE	a	b
α_1	0.9608200	0.9750580	0.9758710	0.9865300	0.9755030	3.7868E+02	9.6868E+00
α_2	1.35E-02	2.49E-02	2.41E-02	3.92E-02	2.45E-02	9.6868E+00	3.7868E+02

CCCG = 3

Alpha Factor	5th%	Mean	Median	95th%	MLE	a	b
α_1	0.9650900	0.9762240	0.9767570	0.9855350	0.9768880	5.7666E+02	1.4045E+01
α_2	7.22E-03	1.42E-02	1.36E-02	2.30E-02	1.35E-02	8.3706E+00	5.8233E+02
α_3	4.08E-03	9.61E-03	9.06E-03	1.70E-02	9.65E-03	5.6739E+00	5.8503E+02

Figure 7-1

Screenshot of motor driven pump FTS common cause parameters from NRC database [21]

So **for *k* = 1**, the CCF value for 1 component out of a group of 3 failing is

$$\alpha_1 * (Q_1/\alpha_1) = Q_1$$

This means that the probability of 1 out of 3 failing is equivalent to the individual failure rate of the component of 0.002.

For *k* = 2, the formula is $1/2\ (\alpha_2 * Q_t)$.

$$Q_t = Q_1/\alpha_1 = 0.002/\ 0.976224 = 2.05E\text{-}03.$$

For CCCG = 3, the mean value for α_2 is 1.42E-02 (see Figure 7-1).

So the value that is input for the CCF basic event of 2 components out of a group of 3 failing is

$$1/2\ (\alpha_2 * (Q_1/\alpha_1)) = ½\ (0.0142 * 2.05E\text{-}03) = 1.45E\text{-}05.$$

For *k* = 3, the formula is $\alpha_3 * Q_t$.

For CCCG = 3, the mean value for α_3 is 9.61E-03 (see Figure 7-1).

Q_t is the same as calculated above for $k = 2$.

So the value that is input for the CCF basic event of 3 components out of a group of 3 failing is

$$\alpha_3 * Q_t = 9.61E\text{-}03 * 2.05E\text{-}03 = 1.97E\text{-}05.$$

These CCF basic event values are then manually input to the PRA model *k* of *m* CCF basic events.

CAFTA also allows the user to build CCF groups and input the parameters so that the software can do the necessary calculations, as discussed in the following section.

7.5 CCF Data Application to PRA Models

This section discusses how the CCF data is applied in the two main PRA model software types, CAFTA and SAPHIRE.

7.5.1 CAFTA

CAFTA allows the data analyst to either input CCF data to CCF component basic events they have defined themselves (or that have been previously defined by the PRA) or to use the CAFTA CCF module [56] to define a CCF group. Reference [44] provides detailed instructions on applying the CAFTA CCF module.

The CAFTA CCF module allows the user to define a group of basic events of the same component type and failure mode as a CCF group. The CCF group is represented in the risk model as a newly named basic event in the fault tree with the combination basic events (such as 2 of 3, 3 of 3) in an OR gate underneath it. All members of the CCF group will use the same individual component failure probability[5] and CAFTA will check to ensure that all the BEs in the group are using it.

The CAFTA CCF group size can theoretically be anything, but CAFTA only evaluates up to CCCG groups of 4. So for example, for a group of four components, CAFTA will evaluate the individual component failure probability, the pairs failure combinations, the triples combinations failures, and then the probability of all components failing. This same method would be used for groups larger than 4. This is evidenced by the CCF module only accepting the β, γ, and δ parameters for MGL and $\alpha 2$, $\alpha 3$ and "$\alpha 4$ or more" parameters in the Alpha factor module.

To quantify the CCFs using CAFTA, the analyst would therefore define a CCF BE and determine whether Alpha factor or MGL will be used to quantify it (other CCF methods are not supported by CAFTA). The analyst must choose between staggered and non-staggered testing for using the Alpha factor. The analyst would then input either MGL parameters or Alpha factor parameters from the NRC operational experience website [21] into the CCF group window.

If the user is not developing CCF groups using the CCF module of CAFTA and is instead quantifying the CCF basic events manually, then the basic event level CCF calculations based on the CCCG and the combination (for example, pair, triple) would have to be performed separately and input by hand to each CCF basic event. The calculations are CCF method dependent and would be performed using the equations shown in Section 7.4.

Regarding Uncertainties: Based on information from the EPRI CAFTA support team, the analyst needs to be sure to use UNCERT 3.0 with the option "Make a copy of the Database" checked. It will then sample all the parameters (Numbers everywhere including type codes and variables) and calculate the probabilities. In order to apply uncertainties to the CCF Parameters (Alpha factor), the analyst must enter a Type Code for the Factor then double click it and this will allow the analyst to set a distribution there. CAFTA rewrites the CCF Basic Events value (normally a straight number) with an equation (the CCF Formula for each event) and then samples the type codes and calculates the value of the CCF event using that equation.

7.5.2 SAPHIRE

Alpha factor values calculated using the data from the NRC operational experience website [21] and the formulas in Table 7-4 can be applied using the CCF algorithms contained in the SAPHIRE code compound event library to combine the random failure probabilities of the events in the CCF group with the appropriate alpha factors for *k*-of-*m* components for failure-on demand events (for example, pump failure to start).

---

[5]When using the CAFTA BE group tool, the individual failure probability is actually the total failure probability Q_t [defined in section 7.4.4] rather than the independent failure probability, due to vestiges of how CAFTA has been u used over the years by 3rd party applications. This introduces a slight conservatism to the model that is rarely detectible, except for small CCF groups where the combined failure probability is very high.

For example, for a 2-out-of-2 failure-on-demand event, the alpha factors associated with α_1 and α_2 are input into a compound event with the two component demand failures and the 2-of-2 failure criteria. The CCF algorithm for the alpha-factor common-cause model with staggered testing can then be used to yield the CCF probability.

For failure-to-operate events (for example, pump fails to run), the mean alpha factor (M) for events with more than one failure is divided by two in accordance with NUREG/CR-5485 [70]. (The mean alpha factor for events with one failure is computed as 1 minus the sum of the remaining alpha factors.) The variance (V) of each failure-to-operate alpha factor is set at one fourth that of the corresponding failure-on-demand alpha factor. The factor of four results from allowing the standard deviation to be reduced by a factor of two, like the mean, but because the variance is the square of the standard deviation, the variance is reduced by a factor of four. A reduction factor of two is applied to the standard deviation because it preserves the coefficient of variation of the underlying distribution.

The following formulas give the mean and variance of a beta distribution in terms of the parameters a and b (α and β in Section 2.3.4.4). To derive an alpha factor for a failure-to-operate event, the mean alpha factor is taken from the NRC operational experience website [21] (or computed from the following formula) and divided by two.

$$M = \frac{a}{a+b}. \qquad \textbf{Eq. 7-23}$$

Then, the variance is calculated from the following formula and divided by four.

$$V = \frac{a \cdot b}{(a+b)^2 \cdot (a+b+1)} \qquad \textbf{Eq. 7-24}$$

Inserting the modified values of M and V into the following formula (which can be derived from the two formulas above) yields the parameter b.

The mean alpha factor and the parameter b, together completely specify the CCF uncertainty distribution in the form required by the SAPHIRE code.

$$b = \frac{(M - M^2 - V) \cdot (1 - M)}{V} \qquad \textbf{Eq. 7-25}$$

7.6 Standard and Regulatory Requirements

ASME/ANS RA-Sa–2009 [7] contains the following Supporting Requirements (SRs) in the area of component data analysis (DA) relevant to CCF analysis:

DA-D5, Capability Category II says to use one of the following models or justify use of an alternative:

1. Alpha Factor Model
2. Basic Parameter Model
3. Multiple Greek Letter Model
4. Binomial Failure Rate Model

DA-D6, Capability Category II: Consistency between generic CCF data, plant experience data and component boundaries.

DA-D7, Consistency of generic CCF event data screening and independent failure event screening.

In addition, the following Supporting Requirements from other areas of the standard apply to and interface with the CCF analysis task:

- SY-B3 – Systematic process to define CCCGs and justify the basis for them
- SY-B4 – Consistency between CCF modeling and CCF data analysis (see DA-D6)

7.7 Guidance per Findings and Experience

Peer Reviews have been and continue to be conducted to evaluate the adequacy of Internal Events PRAs against the ASME/ANS PRA Standard guidance in the area of Data Analysis (DA). The following issues reflect findings that have been made in recent PRAs in the chapter topic area and recommended guidance based upon finding recommendations and PRA data practitioner experience:

1. Plant experience use per ASME/ANS PRA Standard SR DA-D6

   Finding: No evidence that a review was performed of generic common cause failure probabilities to be consistent with available plant experience. There is no discussion of available plant experience with respect to common cause failures.

   Recommended Resolution: Plant experience with respect to common cause failures should be reviewed to ensure it is consistent with generic data; see guidance in Section 7.3.

2. Support System Initiating Events: Identification and Quantification Guideline

   From Westinghouse: Would it be defendable to adjust the alpha factors for a SSIE CCF group by the allowed outage time for the initial failed component? The SSIE guideline only provides this option for the average repair time and most plants do not have enough data to support an average repair time calculation. Using the 8760 hour IE failure rate in an SSIE tree is too high and the results of just the CCF failure can be higher than industry average for loss of that system.

   Response: This issue will be addressed in what will ultimately be a new EPRI report addressing SSIE.

7.8 Research Areas Under Development

The NRC has funded insights studies by the Idaho National Laboratory on the set of common-cause failures of emergency diesel generators, motor-operated valves, motor-driven pumps, and circuit breakers. The data were derived from the NRC CCF database, which is based on U.S. commercial nuclear reactor power plant data. The insight studies are documented in NUREG/CR-6819, "Common-Cause Failure Event Insights" [76] and are the result of in-depth reviews of the CCF data for these components. The objective of these reports is to look beyond the CCF parameter estimates to gain further understanding of why CCF events occur and what measures may be taken to prevent, or at least mitigate, the effect of these CCF events.

Also listed on the NRC Reactor Operational Experience website [21] is a discussion about the International Common-Cause Data Exchange (ICDE) Project to allow multiple countries to exchange CCF data to enhance the quality of risk analyses that include CCF modeling. As the website states, "Because CCF events are typically rare events, most countries do not experience enough CCF events to perform meaningful analyses. Data combined from several countries, however, yields sufficient data for more rigorous analyses."

The objectives of the ICDE Project are the following:

- To collect and analyze CCF events in the long term so as to better understand such events, their causes, and their prevention
- To generate qualitative insights into the root causes of CCF events, which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences
- To establish a mechanism for the efficient feedback of experience gained on CCF phenomena, including the development of defenses against their occurrence, such as indicators for risk based inspections

A draft NUREG based on joint NRC-INL studies on common cause analysis was published in November 2011 [77] including the way data is collected and used in SPAR-H, as well as the way CCFs are handled during event assessment. Event assessment is an application of probabilistic risk assessment in which observed equipment failures and outages are mapped into the risk model to obtain a numerical estimate of the event's risk significance. The research evaluates causal modeling and conditional probabilities and how these impact CCF data results.

8
DOCUMENTATION

8.1 Introduction

The data analysis process, interim steps and results must be substantiated and fully documented, which can require a substantive effort to produce. The integral nature of analysis documentation to the concept of PRA quality was expressed early on in the PRA Procedures Guide [1]:

> "… a PRA is said to have quality when the insights or risk profiles it produces reflect the appropriate use of risk-assessment methods as well as information about the plant and the site – and when the resulting documentation clearly and accurately conveys the resulting insights and risk profiles as well as their bases."

Peer reviews of PRAs have placed additional emphasis on the need for clear and thorough documentation of the PRA data analysis. Reviewers are looking for examples and evidence of the work performed so that they can verify that the standard requirements have been met. In addition, the PRA needs to provide traceability from initial inputs to final results to provide a strong technical basis for the work that has been done, as well as guidelines for the next round of updates that are performed.

8.2 Methodology

Documentation should include:

- Component boundary definitions
- Component failure modes (for example, failure to start, failure to run)
- Numerator and denominator data values and their sources
- Test and maintenance unavailabilities
- Supporting equipment repair and recovery data
- Common cause failure values
- Uncertainty

Data notebooks, correspondence files, or similar records should be updated whenever the data is updated to provide traceability of information sources, assumption bases, and calculation results. *Documentation should be sufficiently complete to allow the results to be reproduced, all information sources to be identified, and the bases for judgments and assumptions to be clearly understood.*

Supplementary spreadsheet and database files should officially included as part of the PRA documentation to provide the necessary background information for a peer review and so that the entire database is captured for future reference.

All major assumptions made in the analysis should be identified and documented. Supporting analyses based upon other literature should be clearly referenced. The report should describe all tasks of the analysis in sufficient detail to permit the reader to understand which parameters were developed, what data sources were used, what analytical methods were employed, and how the data pathway flows from initial data source to the table of results input to the PRA models. For example, for component failure data, this would mean that any MWOs that were used as input to failure rates are cited by MWO number and associated with the component type and failure mode to which they were attributed.

Interim or draft reports should be reviewed by those responsible for ensuring technical quality as part of the overall PRA Quality Assurance program, focusing on the interpretation of the results and on verifying that the document is understandable and usable. To achieve the latter, it is necessary to ensure that all assumptions are clearly stated, data sources are given, and the results presented are reproducible.

The production of reports is a substantial task. Each analyst can expect to spend one to twp man-months documenting his or her work. An additional month may be spent incorporating peer review comments for the final report.

The documentation and supporting calculations should be retained for future use and as a resource when questions arise.

8.3 Standard and Regulatory Requirements

RG 1.200 [8] Section 1.2.6 on Documentation states that:

> Traceability and defensibility provide the necessary information such that the results can easily be reproduced and justified. The sources of information used in the PRA are both referenced and retrievable. The methodology used to perform each aspect of the work is described either through documenting the actual process or through reference to existing methodology documents. Key sources of uncertainty are identified and their impact on the results assessed.

For *initiating events*, the ASME/ANS PRA Standard [7] SRs for documentation are the following:

- IE-D1 – Document initiating event analysis in a reviewable manner.
- IE-D2 – Document the processes used to select, group, screen, model and quantify initiating events. This SR provides a list of specific requirement for documentation that should be followed.
- IE-D3 – Document modeling assumptions and sources of uncertainty (as identified in QU-E1 and QU-E2).

NOTE: the ASME/ANS PRA Standard also specifically requires that plant personnel be interviewed to determine if plant-specific initiating events have been overlooked. Documentation of these interviews is important to the ability to verify having met this SR IE-A8.

For *data analysis*, ASME/ANS PRA Standard SRs for documentation are:

- DA-E1 – Document data analysis in a reviewable manner.
- DA-E2 – Document the processes used for data parameter definition, grouping, and collection including parameter selection and estimation, including the inputs, methods, and results. This SR provides a list of specific requirement for documentation that should be followed.
- DA-E3 – Document the sources of model uncertainty and related assumptions (as identified in QU-E1 and QU-E2).

8.4 Guidance per Findings and Experience

Peer reviews have been and continue to be conducted to evaluate the technical adequacy of Internal Events PRAs against the ASME/ANS PRA Standard guidance in the technical element of data analysis. The following issues reflect findings that have been made in recent PRAs in the chapter topic area and recommended guidance based upon finding recommendations and PRA data practitioner experience.

1. Inclusion of Calculation Details per ASME/ANS PRA Standard SR DA-E1

   Finding: This SR is not met. Documentation of the data analysis is not complete due to the lack of any reference to the basis for the data results. It was noted during the review that the data analysis is actually calculated using spreadsheets, however, those spreadsheets are not part of the data analysis package.

   Recommended Resolution: Ensure that supporting calculational material is officially included as part of the PRA documentation to provide the necessary background information.

2. Generic Data Information per ASME/ANS PRA Standard SR DA-C1

   Finding: Some generic data collected from a recognized source, NUREG-CR/6928. Other generic data collected from a source called “Generic Data Aggregation.” Unable to find documentation of process and methodology used for data collection and analysis for Generic Data Aggregation.

   Recommended Resolution: In-house data aggregation tools should be described as part of the PRA documentation in terms of the methodology and equations for aggregating the data and the input information used.

3. Surveillance Test Details per ASME/ANS PRA Standard SR DA-C10

   Finding: Capability Category I met. Documentation in Appendix D1 was not sufficient to determine if it was necessary to decompose surveillance test data into sub-elements and whether this was done.

   Recommended Resolution: Ensure model validation, as described in Section 3.6 is adequately performed and documented.

4. Basic Event Probability Documentation per ASME/ANS PRA Standard SR DA-E2

   Finding: The PRA documentation does not show the probabilities or basis for the probabilities for certain basic events. No evidence was found that these basic event values are not appropriate.

   Recommended Resolution: Internal review of the PRA database documentation should be conducted to allow disconnects to be identified. All basic event probabilities in the model should be able to be traced back to the supporting data and assumptions.

5. Operator Interviews per ASME/ANS PRA Standard SR IE-A8

   Finding: The Initiating Event section of PRA peer review states "Other plant-specific initiators and event precursors were also investigated using an FMEA of plant systems as discussed below and this was reviewed with plant personnel to verify expected plant response." But it is not clear that interviews were conducted.

   Recommendation: The SR for Capability Category II requires plant personnel interviews to ensure no initiating events were overlooked, so this step should be conducted and documented.

6. Calculation of initiating event frequencies per ASME/ANS PRA Standard SRs IE-C4 and IE-C5

   Finding: The calculation of initiating event frequencies is summarized, but there must be a table that shows the actual calculations using generic, plant-specific, and Bayesian updating.

   Recommendation: Analysts should include this table to document the calculations to meet these SRs.

9
REFERENCES

1. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, NUREG/CR-2300, Vol. 1, Prepared under the auspices of the American Nuclear Society (ANS) and the Institute of Electrical and Electronics Engineers (IEEE) for the U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.
2. 10CFR50.65, Requirements for monitoring the effectiveness of maintenance at nuclear power plants, 56 Federal Register 31324, 10 July 1991.
3. NUREG/CR-5750 and INEEL/EXT-98-00401, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995," Idaho National Engineering and Environmental Laboratory for the U.S. Nuclear Regulatory Commission, Washington, DC, 1999.
4. NUREG/CR-6928 and INL/EXT-06-11119, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," Idaho National Laboratory for the U.S. Nuclear Regulatory Commission, Washington, DC, February 2007.
5. S. A. Eide et al., "Reevaluation of Station Blackout Risk at Nuclear Power Plants," U.S. Nuclear Regulatory Commission, NUREG/CR-6890 (INEEL/EXT-05-00501), December 2005.
6. *Regulatory Assessment Performance Indicator Guideline*, NEI 99-02, Revision 5, Nuclear Energy Institute, Washington, DC, July 2007.
7. ASME/ANS RA-Sa–2009, Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, American Society of Mechanical Engineers, New York, NY, February 2009.

   [Note: Addenda B was released in 2013. While a detailed review of the relevant support requirements was not performed against these guidelines, however, a high level review found no discrepancies between the guidance provided here and the new Addenda.]
8. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," U.S. Nuclear Regulatory Commission, Revision 2, March 2009.
9. *Education of Risk Professionals Module 3, PRA 103-104 Initiating Events/Accident Sequences and Criteria*. EPRI, Palo Alto, CA: 2013. 1022996.
10. M. Drouin, G. Parry, J. Lehner, G. Martinez-Guridi, J. LaChance, and T. Wheeler, *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making*, NUREG-1855, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC, March 2009.
11. *Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments*. EPRI, Palo Alto, CA: 2008. 1016737.
12. *Practical Guidance on the Use of Probabilistic Risk Assessment in Risk-Informed Applications with a Focus on the Treatment of Uncertainty*. EPRI, Palo Alto, CA: 2012. 1026511.

13. C. L. Atwood, J. L. LaChance, H. F. Martz, D. L. Anderson, M. Englehardt, D. Whitehead, and T. Wheeler, "Handbook of Parameter Estimation for Probabilistic Risk Assessment," NUREG/CR-6823, U.S. Nuclear Regulatory Commission, Washington, DC, September 2003.

14. J. Forester, A. Kolaczkowski, S. Cooper, D. Bley, and E. Lois, NUREG-1880, "ATHEANA User's Guide," U.S. Nuclear Regulatory Commission, Washington, DC, June 2007.

15. R. J. Budnitz, G. Apostolakis, D. M. Boore, L. S. Cluff, K. J. Coppersmith, C. A. Cornell, and P. A. Morris, "Recommendations for Probabilistic Hazard Analysis: Guidance on Uncertainty and Use of Experts," NUREG/CR-6372, U.S. Nuclear Regulatory Commission, Washington, DC, April 1997.

16. H. A. Linstone and M. Turoff, *The Delphi Method: Techniques and Applications*, Addison-Wesley, Reading, MA, 1975.

17. A. Ang and W. Tang, *Probability Concepts in Engineering Planning and Design*, Vol. I, Wiley and Sons, Inc., New York, NY, 1975.

18. WASH-1400 (NUREG-75/014), "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.

19. Living Probabilistic Safety Assessment (LPSA), IAEA-TECDOC-1106, International Atomic Energy Agency (IAEA), Vienna, Austria, August 1999.

20. NEA/CSNI/R(2004)20, "Risk Monitors – The State of the Art in their Development and Use at Nuclear Power Plants," Organisation for Economic Co-Operation and Development (OECD), Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI), Paris, France, 2004.

21. U.S. Nuclear Regulatory Commission, "Reactor Operational Experience Results and Databases, Parameter Estimates," http://nrcoe.inel.gov/results

    a. Initiating Event Database http://nrcoe.inel.gov/resultsdb/InitEvent/

    b. Loss of Offsite Power data – http://nrcoe.inel.gov/resultsdb/LOSP/

    c. Component Reliability Database – http://nrcoe.inel.gov/resultsdb/AvgPerf/

    d. Performance Indicator Program – http://nrcoe.inel.gov/resultsdb/IndustryPerf/

    e. International Common Cause Failure Exchange – http://nrcoe.inel.gov/resultsdb/ICDE/

    f. Common Cause Failure Parameters – http://nrcoe.inl.gov/results/CCF/ParamEst2010/ccfparamest.htm

22. *Pipe Rupture Frequencies for Internal Flooding Probabilistic Risk Assessments: Revision 3*. EPRI, Palo Alto, CA: 2013. 3002000079.

23. *Losses of Offsite Power at U.S. Nuclear Power Plants: Summary of Experience Through 2012*. EPRI, Palo Alto, CA: 2013. 3002000697.

24. *Losses of Offsite Power at U.S. Nuclear Power Plants – 2011*. EPRI, Palo Alto, CA: 2012. 1025749.

25. *Losses of Offsite Power at U.S. Nuclear Power Plants – 2010*. EPRI, Palo Alto, CA: 2011. 1023147.

26. *Losses of Offsite Power at U.S. Nuclear Power Plants – 2000–2009*. EPRI, Palo Alto, CA: 2010. 1021508.

27. *Loss of Offsite Power – 2005*. EPRI, Palo Alto, CA: 2006. 1013239.

28. *Loss of Offsite Power at U.S. Nuclear Power Plants – 2004 Update*. EPRI, Palo Alto, CA: 2005. 1011764.

29. *Losses of Off-Site Power at U.S. Nuclear Power Plants – Through 2003*. EPRI, Palo Alto, CA: 2004. 1009889.

30. *Losses of Off-Site Power at U.S. Nuclear Power Plants – Through 1999*. EPRI, Palo Alto, CA: 2000. 1000158.

31. *Losses of Off-Site Power at U.S. Nuclear Power Plants – Through 1997*. EPRI, Palo Alto, CA: 1998. TR-110398.

32. *Losses of Off-Site Power at U.S. Nuclear Power Plants – Through 1995*. EPRI, Palo Alto, CA: 1996. TR-106306.

33. *Losses of Off-Site Power at U.S. Nuclear Power Plants – Through 1992*. EPRI, Palo Alto, CA, 1993. NSAC-194.

34. *Quantitative Assessment of Human-Induced Loss of Offsite Power (HI-LOOP) Event Frequencies at U.S. Commercial Nuclear Power Plants (NPP)*. EPRI, Palo Alto, CA: 2013. 3002000414.

35. NUREG/CR-4639**,** Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Vols. 1–5, U.S. Nuclear Regulatory Commission, Washington, DC, 1994.

36. IEEE Std. 493-2007, *Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, Institute of Electrical and Electronics Engineers (IEEE), 2007.

37. T. R. Moss, *The Reliability Data Handbook*, 1st Edition. ASME Press (American Society of Mechanical Engineers). New York, NY, 2005

38. W. Denson, G. Chandler, W. Crowell, A. Clark, and P. Jaworski, *Nonelectronic Parts Reliability Data*, NPRD-95. Rome, NY, 1994.

39. Mil HDBK 217F, *Reliability Prediction of Electronic Equipment*, US Department of Defense, Washington, DC, 1991.

40. SINTEF Industrial Management, *OREDA - Offshore Reliability Data Handbook*, 4th Edition. Trondheim, Norway, 2002.

41. N. Siu and D. Kelly, "Bayesian Parameter Estimation in Probabilistic Risk Assessment," Reliability Engineering and System Safety 62 (1998) 89-116.

42. C. P. Robert and G. Casella, *Monte Carlo Statistical Methods*, 2nd Ed., Springer-Verlag, New York, NY, 2004.

43. Kelly, D., "When the Details Matter – Sensitivities in PRA Calculations that Could Affect Risk-Informed Decision-Making," INL/CON-10-18285 Preprint, Idaho National Laboratory, Idaho Falls, Idaho, 2010.

44. EPRI Risk and Reliability Workstation User Group Knowledge Base Articles, http://teams.epri.com/RR/RRUG/Knowledge%20Base/Forms/KBView.aspx, Electric Power Research Institute, Palo Alto, CA.

    a. KB66: Bayesian Calculation in CAFTA

    b. KB67: Common Cause Formulas and Application in CAFTA

45. M. D. Muhlheim, et al, "The Use of Probabilistic Safety Techniques for Evaluating the Advanced CANDU Reactor," Proceedings of the Eighth International Conference on Probabilistic Safety Assessment & Management (PSAM 8), New Orleans, LA, May 2006.

46. R. Tregoning and P. Scott, "Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process," NUREG-1829, U.S. Nuclear Regulatory Commission, Washington, DC, April 2008.

47. IAEA-TECDOC-719, "Defining initiating events for purposes of probabilistic safety assessment," International Atomic Energy Agency, Vienna, Austria, September 1993.

48. Licensee Event Report Search (LERSearch), https://lersearch.inl.gov/LERSearchCriteria.aspx, US Nuclear Regulatory Commission, Washington, DC.

49. Generating Availability Data System (GADS) Data Reporting Instructions – Effective January 2012, North American Electric Reliability Corporation (NERC), Atlanta, GA, 2012.

50. INPO website, (http://www.inpo.org), Operating Experience>>Advanced Search of Specific Databases.

51. *Support System Initiating Events*. EPRI, Palo Alto, CA: 2008. 1016741.

52. IEEE Std 500-1984 (Reaffirmed 1991), *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York, NY, 1991.

53. *Guidelines for Process Equipment Reliability Data with Data Tables*, American Institute of Chemical Engineers (AIChE), Center for Chemical Process Safety (CCPS), New York, NY, 1989.

54. C. H. Blanton and S. A. Eide, *Savannah River Site - Generic Data Base Development (U)*. WSRC-TR-93-262, Westinghouse Savannah River Company, Aiken, SC, 1993.

55. R. J. Borkowski, W. K. Kahl, T. L. Hebble, J. R. Fragola, and J. W. Johnson, "The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve-Component," NUREG/CR-3154. U.S. Nuclear Regulatory Commission. Washington, DC, 1983.

56. *CAFTA Fault Tree Analysis System, Version 5.3, Software Manual*. EPRI, Palo Alto, CA: 2007. 1015515.

57. C. L. Smith and S. T. Wood, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE), Version 8: Overview and Summary*, NUREG/CR-7039, Vol. 1, Idaho National Laboratory for the U.S. Nuclear Regulatory Commission (NRC), June 2011. Further information available at https://saphire.inl.gov/.

58. *Nuclear Plant Reliability: Data Collection and Usage Guide*. EPRI, Palo Alto, CA, 1992. TR-100381.

59. NEI 99-02, Revision 5, Regulatory Assessment Performance Indicator Guideline, Nuclear Energy Institute, Washington, D.C., July 2007.

60. K. Heffner, "Mitigating Systems Performance Index - Reporting Demands and Failures in MSPI," Attachment 3 to Public Meeting Summary on the Reactor Oversight Process, ML061390208, US NRC, Washington DC, 17 May 2006.

61. S. Eide and D. Zeek, Mitigating Systems Performance Index Baselines, INEEL, Idaho Falls, ID, presented at PSAM 7/ESREL '04, December 2003.

62. D. M. Rasmuson, T. E. Wierman, and K. J. Kvarfordt, "An Overview of the Reliability and Availability Data System (RADS)," International Topical Meeting on Probabilistic Safety Analysis, PSA '05, September 2005.

63. B. Brady, Memorandum to N. Chokshi and M. Cheok, "Summary of Equipment Performance and Information Exchange (EPIX) Ad Hoc Working Group Meeting," U.S. NRC, Washington, DC, 29 June 2005.

64. Welker, E. and M. Lipow, "Estimating the Exponential Failure Rate from Data with No Failure Events," *Proceedings of the 1974 Annual Reliability and Maintainability Symposium*, Los Angeles, California, IEEE Catalog Number 74CHO820-1RQC, Volume 7, Number 2, Institute of Electrical and Electronics Engineers, New York, New York, 1974.

65. R. Bailey, "Estimation from Zero-Failure Data," *Risk Analysis*, Vol. 17, No. 3, Society for Risk Analysis, 1997.

66. *Risk-Informed Technical Specifications Initiative 5b - Risk-Informed Method for Control of Surveillance Frequencies*, Industry Guidance Document, NEI 04-10, Revision 1, Nuclear Energy Institute (NEI), Washington, DC , April 2007.

67. *An Approach For Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications*, Regulatory Guide 1.177, Rev. 1, U.S. Nuclear Regulatory Commission, Washington, DC., May 2011.

68. S. Eide, "Evaluating Component Failure Probability As a Function of Demand Interval Using EPIX/RADS," PSA 2013, Columbia, SC, 22-26 September 2013.

69. NUMARC 93-01, *Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants*, Nuclear Energy Institute (NEI), Washington, DC, May 2001.

70. A. Mosleh, D. M. Rasmuson, and F. M. Marshall, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," NUREG/CR-5485, U.S. Nuclear Regulatory Commission, Washington, DC, 1998.

71. A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge, and D. M. Rasmuson, *Analytical Background and Techniques*, Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, U.S. Nuclear Regulatory Commission, Washington, D.C., 1988.

72. T. E. Wierman, D. M. Rasmuson, and A. Mosleh, *Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding*, NUREG/CR-6268, Idaho National Laboratory for U.S. Nuclear Regulatory Commission, Washington, D.C., September 2007.

73. F. M. Marshall, D. M. Rasmuson, and A. Mosleh, *Common-Cause Failure Parameter Estimations*, NUREG/CR-5497, U.S. Nuclear Regulatory Commission, Washington, DC., 1998.

74. A. K. Verma, A. Srividya, and D. T. Karanki, *Reliability and Safety Engineering*, Springer-Verlag London Limited, 2010.

75. *Education of Risk Professionals Module 4*. EPRI, Palo Alto, CA, 2012. 1025289.

76. T. E. Wierman, D. M. Rasmuson, and N. B. Stockton, *Common-Cause Failure Event Insights*, Vols. 1-4, NUREG/CR-6819, Idaho National Engineering and Environmental Laboratory for the U.S. Nuclear Regulatory Commission, Washington, DC, May 2003.

77. S-H. Shen, D. Marksberry, G. DeMoss, K. Coyne, D. M. Rasmuson, D. L. Kelly, J. A. Schroeder, and C. L. Smith, *Common-Cause Failure Analysis in Event and Condition Assessment: Guidance and Research*, Draft NUREG-XXXX, U.S. Nuclear Regulatory Commission, Washington, DC, November 2011, ML111890290.

A
DEFINITION OF TERMS[6]

accident sequence: a representation in terms of an initiating event followed by a sequence of failures or successes of events (such as system, function, or operator performance) that can lead to undesired consequences, with a specified end state (for example, core damage or large early release).

aleatory uncertainty: the uncertainty inherent in a nondeterministic (stochastic, random) phenomenon. Aleatory uncertainty is reflected by modeling the phenomenon in terms of a probabilistic model. In principle, aleatory uncertainty cannot be reduced by the accumulation of more data or additional information. (Aleatory uncertainty is sometimes called "randomness.")

availability: the complement of unavailability.

catastrophic failure: a failure that is both sudden and causes termination of one or more fundamental functions [2].

common cause failure (CCF): a failure of two or more components during a short period of time as a result of a single shared cause.

component: an item in a nuclear power plant, such as a vessel, pump, valve, or circuit breaker.

component boundary: demarcation of the equipment included in defining a component and interfaces with excluded piping, electrical and instrumentation systems [2].

core damage: uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage involving a large fraction of the core are anticipated and involving enough of the core, if released, to result in offsite public health effects [7].

core damage frequency (CDF): Expected number of core damage events per unit of time.

data source: descriptive text in a given subject area whose primary purpose is to discuss a reliability or risk topic, but that also contains some useful reliability data [2].

data window: a timeframe established for a given data study [2].

degraded failure: a failure that is gradual or partial; it does not cease all function but compromises that function. It may lower output below a designated point, raise output above a designated point, or result in erratic output. If left unattended, the degraded mode may result in a catastrophic failure [2].

demand: a signal or action that should change the state of a device, or an opportunity to act and thus, to fail [2].

---

[6] Adopted from ASME/ANS RA-Sa–2009 [1] unless noted as from the AIChE Guidelines for Process Equipment Reliability Data [2].

epistemic uncertainty: the uncertainty attributable to incomplete knowledge about a phenomenon that affects our ability to model it. Epistemic uncertainty is reflected in ranges of values for parameters, a range of viable models, the level of model detail, multiple expert interpretations, and statistical confidence. In principle, epistemic uncertainty can be reduced by the accumulation of additional information. (Epistemic uncertainty is sometimes also called "modeling uncertainty.")

equipment: a term used to broadly cover the various components in a nuclear power plant. Equipment includes electrical and mechanical components (for example, pumps, control and power switches, integrated circuit components, valves, motors, and fans), and instrumentation and indication components (for example, status indicator lights, meters, strip chart recorders, and sensors). Equipment, as used in the ASME/ANS PRA standard, excludes electrical cables.

error factor: the ratio of the 95^{th} percentile to the median value of a lognormal distribution [2]. Alternatively, the square root of the ratio of the 95^{th} percentile to the 5^{th} percentile.

event tree: a logic diagram that begins with an initiating event or condition and progresses through a series of branches that represent expected system or operator performance that either succeeds or fails and arrives at either a successful or failed end state.

expert elicitation: a formal, highly structured, and documented process whereby expert judgments, usually of multiple experts, are obtained.

expert judgment: information provided by a technical expert, in the expert's area of expertise, based on opinion, or on an interpretation based on reasoning that includes evaluations of theories, models, or experiments.

exposure: an equipment's operating time in hours or the historical number of demands experienced by the equipment population [2].

external event: an event originating outside a nuclear power plant that directly or indirectly causes an initiating event and may cause safety system failures or operator errors that may lead to core damage or large early release. Events such as earthquakes, tornadoes, and floods from sources outside the plant and fires from sources inside or outside the plant are considered external events. (See also internal event.) By historical convention, LOOP not caused by another external event is considered to be an internal event.

failure mechanism: any of the processes that result in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error.

failure mode: A specific functional manifestation of a failure (that is, the means by which an observer can determine that a failure has occurred) by precluding the successful operation of a piece of equipment, a cable, or a system (for example, fails to start, fails to run, leaks).

failure modes and effects analysis (FMEA): a process for identifying failure modes of specific components and evaluating their effects on other components, subsystems, and systems.

failure probability: the likelihood that an SSC will fail to operate upon demand or fail to operate for a specific mission time.

failure rate: expected number of failures per unit time, evaluated, for example, by the ratio of the number of failures in a population of components to the total time observed for that population.

fault tree: a deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events.

Fussell-Vesely (FV) importance measure: for a specified basic event, FV importance is the fractional contribution to the total of a selected figure of merit for all accident sequences containing that basic event. For PRA quantification methods that include non-minimal cutsets and success probabilities, the FV importance measure is calculated by determining the fractional reduction in the total figure of merit brought about by setting the probability of the basic event to zero.

generic data: data that are typical for a system. Such data will not have been collected for the particular system but will have been collected, estimated, or aggregated from many generally similar systems [2].

human failure event: a basic event in the fire PRA plant response model that represents a failure or unavailability of a piece of equipment, system, or function that is caused by human inaction or inappropriate action.

initiating event: any event either internal or external to the plant that perturbs the steady- state operation of the plant, if operating, thereby initiating an abnormal event such as transient or LOCA within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to core damage or large early release.

initiator: see initiating event.

internal event: a perturbation to steady-state operations that challenges plant control and safety systems whose failure could potentially lead to core damage. The perturbation can be caused by operator error, equipment failure from internal or external causes or a combination thereof. By definition an initiating event requires a reactor trip (manual or automatic). [7] By historical convention, loss of offsite power is considered to be an internal event, and internal fire is considered to be an external event except when the loss is caused by an external hazard that is treated separately (for example, seismic-induced LOOP). Internal floods have sometimes been included with internal events and sometimes considered as external events.

key safety functions: the minimum set of safety functions that must be maintained to prevent core damage and large early release. These include reactivity control, reactor pressure control, reactor coolant inventory control, decay heat removal, and containment integrity in appropriate combinations to prevent core damage and large early release.

large early release: the rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of off-site emergency response and protective actions such that there is a potential for early health effects.

large early release frequency (LERF): expected number of large early releases per unit of time.

LERF analysis: Evaluation of containment response to severe accident challenges and quantification of the mechanisms, amounts, and probabilities of subsequent radioactive material releases from the containment .

Level 1 analysis: identification and quantification of the sequences of events leading to the onset of core damage.

may: used to state an option to be implemented at the user's discretion.

mean: the measure of the central tendency of a distribution, often referred to as its arithmetic average [2].

median: midpoint of the failure data distribution [2].

mission time: the time period that a system or component is required to operate in order to successfully perform its function.

operating time: total time during which components or systems are performing their designed function.

plant: a general term used to refer to a nuclear power facility (for example, "plant" could be used to refer to a single unit or multiunit site).

plant-specific data: data consisting of observed sample data from the plant being analyzed.

point estimate: estimate of a parameter in the form of a single number.

prior distribution (priors): in Bayesian analysis, the expression of an analyst's prior belief about the value of a parameter prior to obtaining sample data.

probabilistic risk assessment (PRA): a qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release, and its effects on the health of the public [also referred to as a probabilistic safety assessment (PSA)].

PRA configuration control program: a process to monitor changes in the design, operation, maintenance, and industry-wide operational history that could affect the PRA. These changes include inputs that impact operating procedures, design configuration, initiating event frequencies, system or subsystem unavailability, and component failure rates. The program should include monitoring of changes to the PRA technology and industry experience that could change the results of the PRA model. (Ref. [1], Section 1-5)

reactor-year: a calendar year in the operating life of one reactor, regardless of power level.

reliability: the complement of unreliability.

repair: restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modeled functionality. Generally modeled by using actuarial data.

repair time: the period from identification of a component failure until it is returned to service.

risk: Probability and consequences of an event, as expressed by the "risk triplet," that is the answer to the following three questions: 1) What can go wrong? 2) How likely is it? and 3) What are the consequences if it occurs?

risk achievement worth (RAW) importance measure: for a specified basic event, RAW importance reflects the increase in a selected figure of merit when an SSC is assumed to be unable to perform its function due to testing, maintenance, or failure. It is the ratio or interval of the figure of merit, evaluated with the SSC's basic event probability set to one, to the base case figure of merit.

risk-significant equipment: equipment associated with a significant basic event. (See also significant basic event.)

safety function: function that must be performed to control the sources of energy in the plant and radiation hazards.

screening: a process that eliminates items from further consideration based on their negligible contribution to the probability of an accident or its consequences .

screening criteria: the values and conditions used to determine whether an item is a negligible contributor to the probability of an accident sequence or its consequences.

shall: used to state a mandatory requirement.

should: used to state a recommendation.

significant basic event: a basic event that contributes significantly to the computed risks for a specific hazard group. For internal events, this includes any basic event that has an FV importance value greater than 0.005 or a RAW importance greater than 2. For hazard groups that are analyzed using methods and assumptions that can be demonstrated to be conservative or bounding, alternative numerical criteria may be more appropriate, and, if used, should be justified.

significant contributor: in the context of a) an internal events accident sequence/cutset, a significant basic event or an initiating event that contributes to a significant sequence b) accident sequences/cutsets for hazard groups other than internal events, the following are also included: the hazard source, hazard intensity, and hazard damage scenario; for example, for Fire PRA, fire ignition source, physical analysis unit, or fire scenario that contributes to a significant accident sequence would also be included, and c) an accident progression sequence, a contributor that is an essential characteristic (for example, containment failure mode, physical phenomena) of a significant accident progression sequence, and if not modeled would lead to the omission of the sequence [7].

state-of-knowledge correlation: the correlation that arises between sample values when performing uncertainty analysis for cutsets consisting of basic events using a sampling approach (such as the Monte Carlo method); when taken into account this correlation results, for each sample, in the same value being used for all basic event probabilities to which the same data apply.

statistical model: a model in which a modeling parameter or behavior is treated as a random variable with specified statistical characteristics.

support system: a system that provides a support function (for example, electric power, control power, or cooling) for one or more other systems.

unavailability: the probability that a system or component is not capable of supporting its function including, but not limited to, the time it is disabled for test or maintenance.

uncertainty: a representation of the confidence in the state of knowledge about the parameter values and models used in constructing the PRA.

uncertainty analysis: the process of identifying and characterizing the sources of uncertainty in the analysis, and evaluating their impact on the PRA results and developing a quantitative measure to the extent practical.

unreliability: the probability that a system or component will not perform its specified function under given conditions upon demand or for a prescribed time.

A.1 References

1. ASME/ANS RA-Sa–2009, Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, American Society of Mechanical Engineers, New York, NY, February 2009.
2. American Institute of Chemical Engineers (AIChE), *Guidelines for Process Equipment Reliability Data with Data Tables*, American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, NY, 1989.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002000774

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com