INTENTIONALLY LEFT BLANK

ATTACHMENT C
ACTIVE COMPONENT RELIABILITY DATA ANALYSIS

The purpose of component-level reliability data analysis is to provide reliability information for logic model quantification at the appropriate level agreed upon by the systems and data analysts. In this report, the term data is taken to mean reliability data analyzed as part of the preclosure safety analysis (PCSA) from published sources. The fault tree models described in Section 4.3.2 include random failures of active mechanical equipment as basic events. In order to numerically solve these models, estimates of the likelihood of failure of these equipment basic events are needed. This attachment provides a summary of the approach for developing these active component reliability estimates by gathering and reviewing industry-wide data, and applying Bayesian combinatorial methods to develop mean values and uncertainty bounds that best represented the range of the industry-wide information. The discussion also addresses the method used for estimating the probability of common-cause failures (CCF) among multiple components. Finally, a table is given showing the template data values input to the Yucca Mountain Project (YMP) PCSA SAPHIRE models (Section 4.2).

C1 INDUSTRY-WIDE COMPONENT RELIABILITY DATA

While data from the facility being studied is the preferred source of equipment failure rate information, it is common in a safety analysis for information from other facilities in the same industry to be used when facility-specific data is sparse or unavailable. Because the YMP activities are atypical of nuclear power plant activities and no operating history exists, it was necessary to develop the required data from the experience of other industries.

C1.1 COMPONENT 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 SAPHIRE 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.

1. Component Type. Corresponds to the category of equipment at the level 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, cameras, diesel generators, and heat exchangers. For certain complex components, a larger component type such as the canister transfer machine is likely to be broken down by the system analyst in the logic model into constituent component types including motors and brakes, not only to facilitate the data analysis but to evaluate the contribution of various subcomponents to the overall component failure.

2. Component Boundaries. 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.

3. Failure Mode. Failure mode is defined as an undesirable component state (e.g., normally closed motor operated valve doesn't open on demand because of valve mechanical damage that occurred before the demand itself).

4. Selection of Model and Parameters. Stochastic models of failures of different systems component are defined for component failure probability estimation depending on the system operational mode. A set of available models is given in SAPHIRE for Windows and includes the following:

   A. Components of stand-by systems. The main parameter of stand-by system is the unavailability upon demand. Such system unavailability can be modeled by fault tree, where basic events probabilities are equal to system components unavailabilities averaged by time. This model treats the time to failure as a random value with exponential distribution. Such component unavailability is the function of time. In case of periodic test, unavailability is a periodic function of time. For simplifying the calculation, time dependency is usually replaced by the average value over the considered interval. For periodically tested components, the interval average is the average value for the test interval.

      Three types of stand-by system components are identified:

      1) Periodically tested stand-by components. For such components it is necessary to estimate following parameters: failure rate, probability of failure per demand, average restoring time (for repair), and average outage time due to test and maintenance.

      2) Non-tested stand-by component. For such components, the exposure time is set to unit projected operation time for calculation of unavailability. But often the component is tested indirectly or replaced. For example, if the system gets a real actuation signal, the state of the non-tested component can be determined. In this case, the average time to failure for a component is set to the average interval between system actuations. In some instances, the component can be replaced along with the tested components. In this case, test interval for non-tested component is set to average time to failure of tested component.

      3) Monitored components. State of some stand-by components is tested continuously (monitoring). In this case component failure is revealed immediately.

B. Components of systems in operation. For systems in operation, the most important parameter is the probability of failure during the defined mission time. This probability may be estimated based on fault trees or another logic model, where basic event probabilities are set to unavailabilities of components over the interval mission time. Failures of operating components are modeled using an exponentially distribution with a failure rate different from the failure rate in stand-by mode.

   Operating systems contain two main types of components: restorable and non-restorable.

   1) Non-restorable components. Components that cannot be restored in case of failure. Exponential distribution of time between failures for such components is characterized by failure rate, λ.

   2) Restorable components. Components that may be restored in case of failure. In this case restoration means restoration without outage of operation.

C. Stand-by systems following demand. Stand-by systems must fulfill a specific function during the defined time after successful start. During this time such systems are described in the same way as operating systems.

D. Constant probability per demand. The model treats component failure probability as a fixed probability for every demand. For such components, tests are excluded from consideration.

For YMP, the operational mode of failure and standby failures predominate; therefore, constant failure rates and constant probabilities per demand were constructed.

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

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

The YMP PCSA basic event naming convention was therefore developed to incorporate the following information in the 24 character basic event name (consistent with the basic event field in SAPHIRE):

- Area code – physical design or construction area where a component would be installed
- System locator code – operational systems and processes

- Component function identifiers – component function
- Sequence code – numeric sequence and train assignment
- Component type code – three character identifier for general component type, such as battery, actuator, or pump
- Failure mode code – three character identifier for the way in which the component is considered in the fault tree models to have failed, (e.g., FTS for fails to start or FOD for fails on demand).

The area, system locator, and component function codes were obtained from engineering standards from the YMP repository as a whole to be consistent with overall site naming conventions. The sequence codes were taken from the component identification numbers on project drawings, if the design had progressed to that point at the time of the data development and modeling.

Active component type codes were developed to be consistent with the component function identifiers, but since the type codes were limited to three digits and the function identifiers were occasionally four-characters long, in some instances it was necessary to truncate the identifier to construct the type code.

Failure mode codes (FM) were developed using prior database conventions or abbreviations that would be as intuitively obvious as possible.

Both type (TYP) and failure mode were limited to three characters each in order to be consistent with the input constraints and conventions of the SAPHIRE template database feature, which allows the same component failure data to be applied to all items in the model.

A list of the component type and failure mode combinations is provided in Table C1.1-1.

Industry-wide data sources were then collected and reviewed to identify failure rates per hour or failure probabilities per demand that would be relevant to each of the 149 TYP-FM combinations.

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM)

TYP-FM	Component Name & Failure Mode
AHU-FTR	Air Handling Unit Failure to Run
ALM-SPO	Alarm/Annunciator Spurious Operation
AT-FOH	Actuator (Electrical) Failure
ATH-FOH	Actuator (Hydraulic) Failure
ATP-SPO	Actuator (Pneumatic Piston) Spurious Operation
AXL-FOH	Axle Failure
B38-FOH	Bearing Failure
BEA-BRK	Lifting Beam/Boom Breaks
BLD-RUP	Air Bag Ruptures

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
BLK-FOD	Block or Sheaves Failure on Demand
BRH-FOD	Brake (Hydraulic) Failure on Demand
BRK-FOD	Brake Failure on Demand
BRK-FOH	Brake (Electric) Failure
BRP-FOD	Brake (Pneumatic) Failure on Demand
BRP-FOH	Brake (Pneumatic) Failure
BTR-FOD	Battery No Output Given Challenge
BTR-FOH	Battery Failure
BUA-FOH	AC Bus Failure
BUD-FOH	DC Bus Failure
BYC-FOH	Battery Charger Failure
C52-FOD	Circuit Breaker (AC) Fails on Demand
C52-SPO	Circuit Breaker (AC) Spurious Operation
C72-SPO	Circuit Breaker (DC) Spurious Operation
CAM-FOH	Cam Lock Fails
CBP-OPC	Cables (Electrical Power) Open Circuit
CBP-SHC	Cables (Electrical Power) Short Circuit
CKV-FOD	Check Valve Fails on Demand
CKV-FTX	Check Valve Fails to Check
CON-FOH	Electrical Connector (Site Transporter) Failure
CPL-FOH	Coupling (Automatic) Failure
CPO-FOH	Control system Onboard (TEV or Trolley) Failure
CRD-FOH	Badge/Card Reader Failure
CRJ-DRP	Jib Crane Load Drop
CRN-DRP	200-Ton Crane Load Drop
CRN-TBK	200-Ton Crane Two-Blocking Load Drop
CRS-DRP	Crane using Slings Load Drop
CRW-DRP	Waste Package Crane Load Drop
CRW-TBK	Waste Package Crane Two-Blocking Load Drop
CSC-FOH	Cask Cradle Failure
CT-FOD	Controller Mechanical Jamming
CT-FOH	Controller Failure
CT-SPO	Controller Spurious Operation
CTL-FOD	Logic Controller Fails on Demand
DER-FOM	Derailment Failure per Mile
DG-FTR	Diesel Generator Fails to Run
DG-FTS	Diesel Generator Fails to Start
DGS-FTR	Diesel Generator - Seismic - Fails to Run for 29 Days
DM-FOD	Drum Failure on Demand
DM-MSP	Drum Misspooling (Hourly)
DMP-FOH	Damper (Manual) Fails to Operate

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)
DMS-FOH	Demister (Moisture Separator) Failure
DRV-FOH	Drive (Adjustable Speed) Failure
DTC-RUP	Duct Ruptures
DTM-FOD	Damper (Tornado) Failure on Demand
DTM-FOH	Damper (Tornado) Failure
ECP-FOH	Position Encoder Failure
ESC-FOD	Emergency Stop Button Controller Failure to Stop (on Demand)
FAN-FTR	Fan (Motor-Driven) Fails to Run
FAN-FTS	Fan (Motor-Driven) Fails to Start on Demand
FRK-PUN	Forklift Puncture
G65-FOH	Governor Failure
GPL-FOD	Grapple Failure on Demand
GRB-FOH	Gear Box Failure
GRB-SHH	Gear Box Shaft/Coupling Shears
GRB-STH	Gear Box Stripped
HC-FOD	Hand Held Radio Remote Controller Fails to Stop (on Demand)
HC-SPO	Hand Held Radio Remote Controller Spurious Operation
HEP-LEK	Filter (HEPA) Leaks (Bypassed)
HEP-PLG	Filter (HEPA) Plugs
HOS-LEK	Hose Leaking
HOS-RUP	Hose Ruptures
IEL-FOD	Interlock Failure on Demand
IEL-FOH	Interlock Failure
LC-FOD	Level Controller Failure on Demand
LRG-FOH	Lifting Rig or Hook Failure
LVR-FOH	Lever (Two Position; Up-Down) Failure
MCC-FOH	Motor Control Centers (MCCs) Failure
MOE-FOD	Motor (Electric) Fails on Demand
MOE-FSO	Motor (Electric) Fails to Shut Off
MOE-FTR	Motor (Electric) Fails to Run
MOE-FTS	Motor (Electric) Fails to Start (Hourly)
MOE-SPO	Motor (Electric) Spurious Operation
MSC-FOH	Motor Speed Control Module Failure
MST-FOH	Motor Starter Failure
NZL-FOH	Nozzle Failure
PIN-BRK	Pin (Locking or Stabilization) Breaks
PLC-FOD	Programmable Logic Controller Fails on Demand
PLC-FOH	Programmable Logic Controller Fails to Operate
PLC-SPO	Programmable Logic Controller Spurious Operation
PMD-FTR	Pump (Motor Driven) Fails to Run

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand
PPL-RUP	Piping (Lined) Catastrophic
PPM-PLG	Piping (Water) Plugs
PPM-RUP	Piping (Water) Ruptures
PR-FOH	Passive Restraint (Bumper) Failure
PRM-FOH	EPROM (HVAC Speed Control) Failure
PRV-FOD	Pressure Relief Valve Fails on Demand
PV-SPO	Pneumatic Valve Spurious Operation
QDV-FOH	Quick Disconnect Valve Failure
RCV-FOH	Air Receiver Fails to Supply Air
RLY-FTP	Relay (Power) Fails to Close/Open
SC-FOH	Speed Control Failure
SC-SPO	Speed Control Spurious Operation
SEL-FOH	Speed Selector Fails
SEQ-FOD	Sequencer Fails on Demand
SFT-COL	Spent Fuel Transfer Machine Collision/Impact
SFT-DRP	Spent Fuel Transfer Machine Fuel Drop
SFT-RTH	Spent Fuel Transfer Machine Fuel Raised Too High
SJK-FOH	Screw jack (TEV) Failure
SRF-FOH	Flow Sensor Failure
SRP-FOD	Pressure Sensor Fails on Demand
SRP-FOH	Pressure Sensor Fails
SRR-FOH	Radiation Sensor Fails
SRS-FOH	Over Speed Sensor Fails
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand
SRT-FOH	Temperature Sensor/Transmitter Fails
SRT-SPO	Temperature Sensor Spurious Operation
SRU-FOH	Ultrasonic Sensor Fails
SRV-FOH	Vibration Sensor (Accelerometer) Fails
SRX-FOD	Optical Position Sensor Fails on Demand
SRX-FOH	Optical Position Sensor Fails
STR-FOH	Steering (Tractor or Trailer) Failure
STU-FOH	Structure (Truck or Railcar) Failure
SV-FOD	Solenoid Valve Fails on Demand
SV-FOH	Solenoid Valve Fails
SV-SPO	Solenoid Valve Spurious Operation
SWA-FOH	Switch, Auto-Stop Fails (CTT end of Hose Travel)
SWG-FOH	13.8kV Switchgear Fails
SWP-FTX	Electric Power Switch Fails to Transfer
SWP-SPO	Electric Power Switch Spurious Transfer
TD-FOH	Transducer Failure

Table C1.1-1. YMP PCSA Component Types (TYP) and Failure Modes (FM) (Continued)

TYP-FM	Component Name & Failure Mode
TDA-FOH	Transducer (Air Flow) Failure
TDP-FOH	Transducer (Pressure) Fails
TDT-FOH	Transducer (Temperature) Fails
THR-BRK	Third Rail Breaks
TKF-FOH	Fuel Tank Fails
TL-FOH	Torque Limiter Failure
TRD-FOH	Tread (Site Transporter)
UDM-FOH	Damper (Backdraft) Failure
UPS-FOH	Uninterruptible Power Supply (UPS) Failure
WNE-BRK	Wire Rope Breaks
XMR-FOH	Transformer Failure
XV-FOD	Manual Valve Failure on Demand
ZS-FOD	Limit Switch Failure on Demand
ZS-FOH	Limit Switch Fails
ZS-SPO	Limit Switch Spurious Operation

NOTE: AC = alternating current; DC = direct current; CTT = cask transfer trailer; HEPA = high-efficiency particulate air (filter); HVAC = heating, ventilation, and air conditioning; MCC = motor control center; TEV = transport and emplacement vehicle; UPS = uninterruptible power supply.

Source: Original

C1.2 INDUSTRY-WIDE RELIABILITY DATA

Industry-wide data sources are documents containing industrial or military 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. For the YMP PCSA, an industry-wide database was constructed using a library of industry-wide data sources of reliability data from nuclear power plants, equipment used by the military, chemical processing plants, and other facilities. The sources used are listed in Table C1.2-1.

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
Guidelines for Process Equipment Reliability Data with Data Tables. [CCPS] (Ref. C5.1)
Savannah River Site, Generic Data Base Development (U) [SRS Reactors] (Ref. C5.5)
The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve Component. NUREG/CR-3154 (Ref. C5.6)
Waste Form Throughputs for Preclosure Safety Analysis.[BSC 2007](Ref. C5.7)
Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report. [EPRI PRA] (Ref. C5.8)

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database (Continued)

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
Component Failure and Repair Data for Coal-Fired Power Units. EPRI AP-2071 [EPRI Pipe Failure Study] (Ref. C5.10)
Mechanical Reliability: Theory, Models and Applications. [AIAA] (Ref. C5.11)
Military Handbook, Reliability Prediction of Electronic Equipment. MIL-HDBK-217F [MIL-HDBK-217F] (Ref. C5.12)
The In-Plant Reliability Data Base for Nuclear Power Plant Components - Pump Component. NUREG/CR-2886. (Ref. C5.13)
Some Published and Estimated Failure Rates for Use in Fault Tree Analysis [DuPont] (Ref. C5.14)
Analysis of Station Blackout Risk. Volume 2 of Reevaluation of Station Blackout Risk at Nuclear Power Plants. NUREG/CR-6890 (Ref. C5.15)
Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants. NUREG/CR-6928. (Ref. C5.16)
"Train Accidents by Cause from Form FRA F 6180.54." [Federal Railroad Administration] (Ref. C5.17)
Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999. [McKenna] (Ref. C5.20)
Ruggedized Card Reader/Ruggedized Keypad Card Reader. [HID] (Ref. C5.21)
IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems. [IEEE-493] (Ref. C5.22)
IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations. [IEEE-500] (Ref. C5.23)
The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report- Diesel Generators, Batteries, Chargers and Inverters. NUREG/CR-3831 (Ref. C5.24)
Instruments and Software Solutions (for Emergency Response and Health Physics [LAURUS] (Ref. C5.25)
A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002. NUREG-1774. (Ref. C5.26)
Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980. NUREG/CR-1363 (Ref. C5.28)
The Reliability Data Handbook. [Moss] (Ref. C5.32)
Control of Heavy Loads at Nuclear Power Plants. NUREG-0612. (Ref. C5.35)
Handbook of Reliability Prediction Procedures for Mechanical Equipment [NSWC-98-LE1] (Ref. C5.37)
"*Diagnosing the Army's Equipment Readiness: The Equipment Downtime Analyzer* " [Rand] (Ref. C5.38)
Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data. NUREG/CR-4639, (Ref. C5.39)

Table C1.2-1. Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database (Continued)

Industry-wide Data Sources Used in YMP PCSA Active Component Reliability Database
5Nonelectronic Parts Reliability Data 1995. NPRD-95. [NPRD -95] (Ref. C5.40)
Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment. [SAIC Umatilla] (Ref. C5.41)
Offshore Reliability Data Handbook. 2nd Edition [OREDA-92] (Ref. C5.42)
Offshore Reliability Data Handbook. 4th Edition. [OREDA-2002] (Ref. C5.43)
Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants: January 1, 1972-April 30, 1980. NUREG/CR-1205. (Ref. C5.45)
N-Reactor Level 1 Probabilistic Risk Assessment: Final Report. [N-Reactor] (Ref. C5.46)

NOTE: The code in brackets [XXXX] is used to aid the reader in identifying references in Table C4-1.

Source: Original

It was necessary to analyze the industry-wide data to compare the relevancy of the component data selected from the industry-wide data sources with the equipment in the YMP PCSA models.

The data source scope had to be sufficiently broad to cover a reasonable number of the equipment types modeled, yet with enough depth to ensure that the subject matter is appropriately addressed. For example, a separate source might have been used for electronics data versus mechanical data, so long as its use was justified by the detail and the applicability of the information provided. Lastly, the quality of the data source was 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 was made to use the highest quality data source available for each active component type and failure mode.

Data were selected from the industry-wide data sources using the following criteria:

- The component type (TYP) and failure mode (FM) identified in the data source had to match those in the basic events specified in the fault tree. For every component modeled, a comparison was made between the modeled component and the component found in the data source to ensure its suitability for the PCSA. Also, every attempt was made to match the failure modes. Often, the source described the failure mode as "all modes," whereas the fault tree required "fails to operate." In cases such as this, sources with more general failure modes were not used unless they were the only available sources.

- The data source had to be widely available, not proprietary. This ensured traceability and accessibility.

- Mid level or low level quality data sources were used only when high level sources were not available.

- The operating environment is an important factor in the selection of 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 policy and testing policy. If either of these states differed from the modeled facility's state, then the data were reconsidered and usually rejected (unless no alternative existed).

A potential disadvantage of using industry-wide data is that a source may provide failure rates that are not realistic because the source environment, either physical or operational, may not correlate to the facility modeled. Part of the PCSA active component reliability analysis effort, therefore, was to evaluate the similarity between the YMP operating environment and that represented in each data source to ensure data appropriateness.

An example of how data were retrieved from the various data sources is described in the following example for check valves. The failure modes modeled in the PCSA for the check valve are fails per hour (FOH), fails to check (FTX), leaks (LEK), and spurious operation (SPO).

Table C1.2-2 shows a comparison between the failure rates for the check valve and its failure modes from three different industry-wide data sources.

Table C1.2-2. Data Source Comparison for Check Valve

Data Source	Equipment Description	Failure Modes	Data Values Provided	Equipment Boundary Given?	Taxonomy Given?
(Ref. C5.1)	Valve-non-operated, Check	• Fails to Check • Significant Back Leakage	Lower, Mean, Upper	Yes	Yes
(Ref. C5.23)	Driven Equipment Valves, Check	"All Modes"	Low, Recommended, High	No	Yes
(Ref. C5.5)	Check	• Fails to Open • Fails to Close • Plugs • Internal Leakage • Internal Rupture • External Leakage • External Rupture	Mean	No	No

NOTE: IEEE = Institute of Electrical and Electronics Engineers.

Source: Original

Table C1.2-3 shows actual numbers extracted from industry-wide data sources for five failure modes for check valves.

Table C1.2-3. Failure Rates Extracted from Various Data Sources for Check Valve

Failure Mode Description	Failure Mode Code	Data Source	Lower	Median	Upper	EF
Fails to Close (Hourly)	FOH	(Ref. C5.5)	1.27 × 10-7	7.74 × 10-7	4.70 × 10-6	6.1
Leaks	LEK	(Ref. C5.5)	6.98 × 10-7	3.49 × 10-6	1.75 × 10-5	5.0
Fails to Open (Hourly)	FOH	(Ref. C5.5)	1.27 × 10-7	7.74 × 10-7	4.70 × 10-6	6.1
Transfers Closed	SPO	(Ref. C5.23)	8.00 × 10-8	7.81 × 10-7	3.27 × 10-4	5.0
Transfers Open	SPO	(Ref. C5.23)	8.00 × 10-8	7.81 × 10-7	3.27 × 10-4	5.0

NOTE: EF = error factor; FOH = fails per hour; LEK = leaks; SPO = spurious operations.

Source: Original

At this stage of the analysis, it remains to decide which data is appropriate to keep and include in the data pool and which are discarded. The criteria for this process are discussed below.

The guidelines shown in Table C1.2-4 are based on observations of the analysts of their preferences and rationales during the data selection process among the data available at the time.

Table C1.2-4. Guidelines for Industry-wide Data Selection

Data Selection Guidelines	
1.	Preference for greater than zero failures (but not always able to exclude on this basis)
2.	Population of at least five
3.	Denominator greater than 1,000 hours or 100 demands
4.	If mean or median values, some expression of uncertainty surrounding these values (either upper or lower bounds or lognormal error factor)
5.	Data analyst's confidence in the applicability of the data to the YMP based on: • Component design • Driver/operator • Size • Component application • Active versus passive service • Materials/fluids moved (e.g., water versus caustic versus viscous) • Component boundary • What's included and excluded in component definition (e.g., motor, electrical connections) • Failure modes • Operating environment • Physical (e.g., heat, humidity, corrosive) • Functional (e.g., operation, maintenance, and testing frequency)

NOTE: YMP = Yucca Mountain Project.

Source: Original

Given the fact that the YMP will be a relatively unique facility (although portions will be similar to the spent fuel handling and aging areas of commercial nuclear plants), the data development perspective was to collect as much relevant industry-wide failure estimate information as possible to cover the spectrum of equipment operational experience. It is assumed that the YMP equipment would fall within this spectrum (Assumption 3.2.1). The scope of the sources selected for this data set was deliberately broad to increase the probability that YMP operational experience would fall within the bounds. A combined estimate that reflected the uncertainty

ranges defined by the data source values was developed. This process is addressed further in the Bayesian estimation Section C2.

Every attempt was made to find more than one data source for each TYP-FM, although the unique nature of many equipment types made this difficult. Data was extracted from several sources in many cases, then combined using Bayesian estimation (as described further below), and compared by plotting the individual and combined distributions. However, the comparison process often resulted in one source being selected as most representative of the TYP-FM. Ultimately, 53% of the TYP-FMs were quantified with one data source, 7% with two data sources, 8% with three data sources, and 32% with four or more data sources.

C1.3 CRANE AND SPENT FUEL TRANSFER MACHINE DROP ESTIMATES

Industry-wide data was used to quantify the likelihood of experiencing a drop from the 200-ton crane while handling waste forms and their associated containers and for estimating drop probability for jib cranes and cranes used to maneuver waste packages. In addition, drop likelihoods for the spent fuel transfer machine (SFTM) were estimated using industry-wide data.

The rationale for using industry-wide data for these estimates was that a significant amount of crane experience exists within the commercial nuclear power industry and other applications and that this experience could be used to bound the anticipated crane performance at YMP. Further, the repository is expected to have training for crane operators and maintenance programs similar to those of nuclear power plants.

Handling incidents that resulted in a drop were included in the drop probability regardless of cause; they may have been caused by equipment failures (including failures in the yokes and grapples), human error, or some combination of the two.

The industry-wide data for cranes was taken from NUREG-0612 (Ref. C5.35), *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002*. NUREG-1774 (Ref. C5.26), and the *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Ref. C5.8). NUREG-0612 (Ref. C5.35) has several appendices that contain crane data from the Occupational Safety and Health Act Administration, the U.S. Navy, Waste Isolation Pilot Plant, Licensee Event Reports, and from the results of a fault tree analysis. The *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report* (Ref. C5.8) provides estimates from Savannah River Site crane experience in addition to fault tree analysis. Crane failure information was also obtained from quantitative risk study performed for the U.S. Army chemical weapons destruction program (Ref. C5.41).

The information from each of these sources was evaluated in terms of quality, applicability to YMP, and to ensure that the events cited included both equipment failures and human failures. For the industry-wide data provided in terms of the number of events, another major factor was the ability to reasonably and justifiably estimate a meaningful denominator of number of lifts (demands) conducted by the crane population considered in the data source. If this could not be done, the source information could not be used.

A key consideration in evaluating the industry-wide crane data for the 200-ton cranes was the NOG-1 (Ref. C5.3) design requirements that will be placed upon the YMP cranes versus the crane design features reflected in the input data sources. NUREG-1774 (Ref. C5.26, Table 12, pp. 61 – 63) provides a list of the nuclear power plants that had upgraded their cranes to single-failure-proof status consistent with licensee response to U.S. Nuclear Regulatory Commission (NRC) Bulletin 96-02 (Ref. C5.9) which requested specific information relating to their heavy loads programs and plans consistent with the recommendations of NUREG-0554 (Ref. C5.34). This information was used to constrain the denominator of the number of very heavy load lifts from NUREG-1774 (54,000) by using a percentage of percent of nuclear power plants reporting single failure proof cranes out of total plants (43/109). When this information is evaluated, the crane drop frequency calculates to 3.16E-05 which is rounded to 3.2E-05 for these analyses.

Conversely, a separate category of non-single-failure-proof cranes for the waste package manipulating cranes was developed using the remaining percentage (66/109) to adjust the number of lifts. The jib crane load drop likelihood was estimated using U.S. Navy shipyard and on-board crane data from NUREG-0612 (Ref. C5.35, Section 4.2) since there was insufficient information to allow an accurate assessment of jib crane lifts from NUREG-1774 (Ref. C5.26). The Navy load drop data was described in NUREG-0612 (Ref. C5.35, Section 4.2) as reflecting information on "a large number of boom type cranes" described as being "more susceptible to failure" than the gantry or rectilinear cranes primarily found at nuclear power plants. The inclusion of the boom crane data, according to the NUREG, skewed the resulting load drop likelihood a bit higher than would be expected for non-jib type cranes in nuclear facilities. The Navy data was therefore considered the most applicable for the jib crane load drop estimate for the PCSA. The number of crane drop incidents used as the numerator of the 200-ton crane drop estimate from NUREG-1774 (Ref. C5.26) was restricted to those involving very heavy loads (defined in NUREG-1774 as >30 tons) of single-failure-proof cranes. Drops occurring during sling lifts were parsed into a separate category and used to estimate the sling lift-related drop likelihood.

Load drop likelihood due to two-blocking was also estimated using industry-wide data. NUREG-0612 (Ref. C5.35) describes a two-blocking event as: "The act of continued hoisting to the extent that the upper head block and the load block are brought into contact, and unless additional measures are taken to prevent further movement of the load block, excessive loads will be created in the rope reeving system, with the potential for rope failure and dropping of the load." Two-blocking events in the various data sources were evaluated based upon the type of crane involved, as was done for the drop likelihood estimates.

As a result, several categories of crane drop estimates were developed, were coded with TYP-FM designators, and were included in the template database for input to SAPHIRE:

CRN-DRP	200-ton Crane Load Drop	3.2E-05/demand
CRN-TBK	200-ton Crane Two Block Causing Load Drop	4.4E-07/demand
CRS-DRP	200-ton Crane using Slings Load Drop	1.2E-04/demand
CRJ-DRP	Jib Crane Load Drop	6.4E-05/demand
CRW-DRP	Waste Package Crane (Not Single Failure Proof) Load Drop	1.1E-04/demand

CRW-TBK	Waste Package Crane (Not Single Failure Proof) Two Block Causing Load Drop	4.6E-05/demand

In each of these cases, as with the other active component reliability estimates, an effort was made to include a variety of operating experience and combine it together using a parametric empirical Bayes approach. However, for the CRS, CRJ and CRW estimates, since only NUREG-1774 (Ref. C5.26) and NUREG-0612 (Ref. C5.35) data was considered to be applicable, a Jeffreys' non-informative prior approach for the beta distribution was used, since the estimates were per lift (demand).

These crane incident estimates were combined in the SAPHIRE models with the number of estimated YMP crane lifts.

One potential issue regarding the applicability of the industry-wide crane data was the inclusion of hard-wired interlock features on the YMP cranes that might not exist at the nuclear power plants or naval installations from which the industry-wide experience resulted. In other instances, there was concern that interlocks included in the design for use in normal operations, on grapples to verify installation or engagement, could be defeated during maintenance actions where bypasses are permitted to move tools or pallets, since a particular grapple interlock is not standard in industry but is unique to YMP. Further, PCSA is not crediting the grapple interlock function and it was considered that having such interlocks in place would not make the estimated failure probability worse. Therefore the estimates from industry-wide data were considered to be reasonable in that they provided experience-based, and perhaps somewhat pessimistic measures of anticipated crane performance.

Estimates were also developed from industry-wide data source information for the likelihood of SFTM drop, collision, and raising the fuel too high but not dropped (for potential personnel exposure considerations). The primary source for this information was NUREG-1774 (Ref. C5.26, Table 4), which provides brief descriptions of SFTM incidents at U.S. nuclear power plants from 1968 through 2002. A separate study (McKenna/Framatome) (Ref. C5.20) was reviewed, which also included SFTM incidents at U.S. nuclear power plants categorized in terms of Human Error, Equipment Failure, or Misload. Some of these were the same incidents included in NUREG-1774 (Ref. C5.26) so care was taken not to double-count any events. Each of the incidents described was reviewed in detail to evaluate their relevance to the failure modes of interest to the study and their applicability to spent fuel transfers. Incidents related to all types of fuel transfers, such as refueling or new fuel receipt, were used to estimate upper bounds (95th percentiles of a lognormal distribution) and to develop the error factor uncertainty information input to SAPHIRE along with the mean value.

It should be noted that events prior to 1985 were removed from consideration since the number of plants in operation (and therefore the number of lifts per year) would significantly differ from that cited in McKenna/Framatome (Ref. C5.20). Also, McKenna/Framatome stated that reporting practices were inconsistent prior to 1985.

The number of fuel movements used as the denominator of the SFTM estimates was based upon information from McKenna/Framatome (Ref. C5.20), which gave 1,198,723 fuel movements for the 15 year study data window, from 1985 through 1999, or a rough estimate of 79,914.87 per

year. Since the numerator information from NUREG-1774 (Ref. C5.26) was based upon 17 years of data, from 1985 through 2002, the estimated denominator was calculated for consistency as 79,914.87×17 or 1,358,553 SFTM lifts.

As a result, several categories of SFTM event estimates were developed, were coded with TYP-FM designators, and were included in the template database for input to SAPHIRE:

SFT-COL	SFTM Collision/Impact	2.9E-06/demand
SFT-DRP	SFTM Load Drop	5.2E-06/demand
SFT-RTH	SFTM Fuel Raised Too High (but not dropped)	7.4E-07/demand

These SFTM incident estimates were combined in the SAPHIRE models with the number of estimated YMP fuel assembly transfers, specifically: 66,188 based on two transfers each of 33,094 assemblies (Ref. C5.7, Table 4, pg. 27).

The results of the industry-wide data search are documented, organized by component type and failure mode, and can be found in the Excel spreadsheet file "YMP Active Comp Database.xls", located on the CD in Attachment H.

C2 BAYESIAN DATA COMBINATION

The application of industry-wide data sources or expert elicitation introduces uncertainty in the input parameters used in basic events and, ultimately, the quantification of probabilities of event sequences. Uncertainty is a probabilistic concept that is inversely proportional to the amount of knowledge, with less knowledge implying more uncertainty. Bayes' theorem is a common method of mathematically expressing a decrease in uncertainty gained by an increase in knowledge (for example, knowledge about failure frequency gained by in-field experience).

A typical application of Bayes' theorem is illustrated as follows: a failure rate for a given component is needed for fault tree (e.g., a fan motor in the heating, ventilation, and air conditioning (HVAC) system). There is no absolute value but there are several data sources for the same kind of fan and/or similar fans that may exhibit considerable variability for many reasons. Applying any or all of the available data introduces uncertainty in the analysis of the reliability of the HVAC system. Bayes' theorem provides a mechanism for systematically treating the uncertainty and applying λj data sources using the following steps:

1. Initially, estimate the failure rate to be within some range with a probability distribution. This is termed the "prior" probability of having a certain value of the failure rate that expresses the state of knowledge before any new information is applied.

2. Characterize the test information, or evidence, in the form of a likelihood function that expresses the probability of observing the number of failures in the given number of trial if the failure rate is a certain value. The evidence comprises observations or test results on the number of failure events that occur in over a certain exposure, operational, or test duration.

3. Update the probability distribution for the failure rate based on the new body of evidence using the mathematical expression of Bayes' theorem.

The mathematical expression for applying Bayes' theorem to data analysis is briefly described here. Let λ_j be one failure rate of a set of possible failure rates of the fan motor (component j). Initially, the state of knowledge of the "true value" of λ_j is expressed by the probability distribution $P(\lambda)$, the "prior." The choice of the analytic or discrete form of the prior distribution is made by the data analyst. Let E be a new body of evidence, e.g., a new set of test data or field observations. The new evidence improves the data analyst's state of knowledge. The revised, or "updated," probability distribution for the "true value" of λ_j is represented as $P(\lambda_j|E)$. Bayes' theorem gives:

$$P(\lambda_j \mid E) = \frac{P(\lambda_j)L(E \mid \lambda_j)}{\sum_j P(\lambda_j)P(E \mid \lambda_j)} \qquad \text{(Eq. C-1)}$$

In summary, Equation C-1 states that the knowledge of the "updated" probability of λ_j, given the new information E, equals the "prior" probability of λ_j before any new information times the likelihood function, $L(E|\lambda_j)$. The likelihood function expresses the probability of observing the number of failures in the evidence if the failure rate λ_j has a certain value. The likelihood function is defined by the analyst in accordance with the kind of evidence. For time-based failure data, a Poisson model is used for the likelihood function. For demand-based failure data, a binomial model is used. The numerator in Equation C-1 is divided by a normalization factor, which must be such that the sum of the probabilities over the entire set of λ_j equals unity.

There are several approaches for applying Bayes' theorem to data management and combining data sources, as described in NUREG/CR-6823 (Ref. C5.4). For the YMP PCSA, the method known as "parametric empirical Bayes" was used. This permitted a variety of different sources to be statistically combined and compared, whether the inputs were expressed as the number of failures and exposure time or demands, or as a mean and error factor. Examples of the methods used for several combinatorial cases are provided below.

C2.1 PARAMETER ESTIMATION USING DATA FROM DIFFERENT SOURCES

Using multiple reliability databases will typically cause a given active component to have various reliability estimates, each one from a different source. These various estimates can be viewed as independent samples from the same distribution, *g*, representing the source-to-source variability, also called population variability, of the component reliability (Ref. C5.4, Section 8.1). The objective of this section is to outline the methodology for developing the population-variability distribution of active components in the preclosure safety analysis. In a Bayesian approach to reliability estimation, the population-variability distribution of a component constitutes an informative prior distribution for its reliability. This distribution is to be updated, as operating experience becomes available, to produce a reliability distribution specific to the component operated under geologic repository operations area (GROA) conditions. For the time being however, the components anticipated for use at the GROA are yet to be procured and operated. As a consequence, the population-variability distributions developed in this section both aim at and are limited to encompassing the actual component reliability distributions that will be observed at the GROA when operating experience becomes available.

A parametric empirical Bayes method is used to develop the population-variability distributions of active components considered in the preclosure safety analysis. As indicated in "Bayesian Parameter Estimation in Probabilistic Risk Assessment." (Ref. C5.44, Section 5.1.2), this method is a pragmatic approach that has been used in PRA-related applications; it involves specifying the functional form of the prior population-variability distribution, and fitting the prior to available data, using classical techniques, for example, the maximum likelihood method. A discussion of the adequacy of the parametric empirical Bayes method for determining the population-variability distribution is given at the end of this section.

Applying the parametric empirical Bayes method requires first to categorize the reliability data sources into two types: those that provide information on exposure data (i.e., the number of failures that were recorded over an exposure time (in case of a failure rate) or over a number of demands (in case of a failure probability), and those that do not provide such information). In the latter case, reliability estimates for a failure rate or failure probability are provided in the form of a mean or a median value, along with an uncertainty estimate, typically an error factor.

For each data source, the reliability information about a component's failure rate of failure probability is mathematically represented by its likelihood function. If exposure data are provided, the likelihood function takes the form of a Poisson distribution (for failure rates), or a binomial distribution (for failure probabilities) (Ref. C5.44, Section 4.2). When no exposure data are available, the reliability estimates for failure rates or failure probabilities are interpreted as expert opinion, for which an adequate representation of the likelihood function is a lognormal distribution ((Ref. C5.44, Section 4.4) and (Ref. C5.27, pp. 312, 314, and 315)).

The next step is to specify the form of the population-variability distribution. In its simplest form, the parametric empirical Bayes method only considers exposure data and employs distributions that are conjugate to the likelihood function (i.e., a gamma distribution if the likelihood is a Poisson distribution, and a beta distribution if the likelihood is binomial) (Ref. C5.4, Section 8.2.1), which have the advantage of resulting in relatively simpler

calculations. This technique however is not applicable when both exposure data and expert opinion are to be taken into consideration, because no conjugate distribution exists in this situation. Following the approach of "The Combined Use of Data and Expert Estimates in Population Variability Analysis," (Ref. C5.27, Section 3.1), the population-variability distribution in this case is chosen to be lognormal. More generally, for consistency, the parametric empirical Bayes method is applied using the lognormal functional form for the population-variability distributions regardless of the type of reliability data available for the component considered (exposure data, expert opinion, or a combination of the two). In the rest of this section, the population-variability distribution in its lognormal form is noted $g(x,\nu,\tau)$, where x is the reliability parameter for the component (failure rate or failure probability), and ν and τ, the two unknowns to be determined, are respectively the mean and standard deviation of the normal distribution associated with the lognormal. The use of a lognormal distribution is appropriate for modeling the population-variability of failure rates and failure probabilities, provided in the latter case that any tail truncation above $x = 1$ has a negligible effect (Ref. C5.44, p. 99). The validity of this can by confirmed by selecting the failure probability with the highest mean and the most skewed lognormal distribution and calculating what the probability is of exceeding 1. In Table C4-1, PRV-FOD fits this profile, with a mean failure probability of 6.54E-03 and an error factor of 27.2. The probability that the distribution exceeds 1 is 2E-04. Stated equivalently, 99.98% of the values taken by the distribution are less than 1. This confirms that the use of a truncated lognormal distribution to represent the probability distribution is appropriate.

To determine ν and τ, it is first necessary to express the likelihood for each data source as a function of ν and τ only (i.e., unconditionally on *x)*. This is done by integrating, over all possible values of x, the likelihood function evaluated at x, weighted by the probability of observing x, given ν and τ. For example, if the data source i indicates that r failures of a component occurred out of n demands, the associated likelihood function $L_i(\nu,\tau)$, unconditional on the failure probability x, is as follows:

$$L_i(\nu,\tau) = \int_0^1 Binom(x,r,n) \times g(x,\nu,\tau)dx \qquad \text{(Eq. C-2)}$$

where $Binom(x,r,n)$ represents the binomial distribution evaluated for r failures out of n demands, given a failure probability equal to x, and $g(x,\nu,\tau)$ is defined as previously indicated. This equation is similar to that shown in "Bayesian Parameter Estimation in Probabilistic Risk Assessment." (Ref. C5.44, Equation 37). If the component reliability was expressed in terms of a failure rate and the data source provided exposure data, the binomial distribution in Equation C-2 would be replaced by a Poisson distribution. If the data source provided expert opinion only (no exposure data), the binomial distribution in Equation C-2 would be replaced by a lognormal distribution.

The maximum likelihood method is an acceptable method to determine ν and τ (Ref. C5.44, p. 101). The maximum likelihood estimators for ν and τ are obtained by maximizing the likelihood function for the entire set of data sources. Given the fact that the data sources are independent, the likelihood function is the product of the individual likelihood functions for each

data source (Ref. C5.27, Equation 4). To find the maximum likelihood estimators for ν and τ, it is equivalent and computationally convenient to maximize the log-likelihood function, which is the sum of the logarithms of the likelihood function for each data source.

The calculation of ν and τ completely determines the population-variability distribution *g* for the reliability of a given active component. The associated parameters to be plugged into SAPHIRE are the mean and the error factor of the lognormal distribution *g*, which are calculated using the formulas given in NUREG/CR-6823 (Ref. C5.4, Section A.7.3). Specifically, the mean of the lognormal distribution is equal to $\exp(\nu + \tau^2/2)$ and the error factor is equal to $\exp(1.645 \times \tau)$.

The selection of the parametric empirical Bayes method to determine the population-variability distribution is now discussed. This method provides a single "best" solution, while other techniques, such as the hierarchical Bayes method (Ref. C5.4, Section 8.3) differ by using a weighted mix of distributions of the chosen model, which incorporate epistemic (state of knowledge) uncertainty about the model. The parametric empirical Bayes method does not embed epistemic uncertainty but was nevertheless employed because of its satisfactory results for the majority of active components modeled in the preclosure safety analysis. The general adequacy of the method was confirmed by comparing its results to those obtained based on an example using a state-of-knowledge-informed approach (Ref. C5.27). The example involves twelve hypothetical data sources, each documenting the failure rate of motor-driven pumps either in terms of expert judgment or exposure data (Ref. C5.27, Table 1). Table C2.1-1 compares the percentiles predicted by the parametric empirical Bayes method and those found in "The Combined Use of Data and Expert Estimates in Population Variability Analysis." (Ref. C5.27, Table 4). Overall, the percentiles appear to be similar, with a key metric of the distributions, their mean, being nearly identical, and the medians being comparable. Percentiles at the tails of the distributions show more differences, the parametric empirical Bayes method yielding a population-variability distribution more spread out overall than the state-of-knowledge-informed distribution (Ref. C5.27).

Table C2.1-1. Comparison of Results of Parametric Empirical Bayes and Results Reported by Lopez Droguett et al.

Population-Variability Value	Parametric Empirical Bayes Method[a]	Lopez Droguett Results[b]
Mean	6.00×10^{-5}	6.05×10^{-5}
1st percentile	1.32×10^{-7}	3.16×10^{-7}
5th percentile	4.75×10^{-7}	1.38×10^{-6}
10th percentile	9.38×10^{-7}	2.67×10^{-6}
50th percentile (median)	1.04×10^{-5}	1.61×10^{-5}
90th percentile	1.14×10^{-4}	7.79×10^{-5}
95th percentile	2.26×10^{-4}	1.36×10^{-4}
99th percentile	8.10×10^{-4}	4.85×10^{-4}

NOTE: [a] Derivation of the results is given in the following section, Example of Development of Population-Variability Distribution.
[b] "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety, 83* (Ref. C5.27, Table 1)
Source: Ref. C5.27, Table 1

An adjustment to the parametric empirical Bayes method was done in a few instances where the error factor of the calculated lognormal distribution was found to be excessive. In a synthetic examination of the failure rates of various components, "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom," *Reliability Engineering and System Safety, 47* (Ref. C5.19, Figure 3) finds that electromechanical and mechanical components have, overall, a range of variation approximately between 2×10^{-8}/hr (5th percentile) and 6×10^{-5}/hr (95th percentile). Using the definition of the error factor given in NUREG/CR-6823, (Ref. C5.4, Section A.7.3), this corresponds to an error factor of $\sqrt{6 \cdot 10^{-5} / 2 \cdot 10^{-8}} = 55$. Therefore, in the preclosure safety analysis, it is considered that lognormal distributions resulting from the empirical Bayes method that yield error factors with a value greater than 55 are too diffuse to adequately represent the population-variability distribution of a component. In such instances (two such cases in the entire PCSA database, when the error factors from the Bayesian estimation were greater than 200), the lognormal distribution used to represent the population-variability is modified as follows. It has the same median as that predicted by the parametric empirical Bayes method, and its error factor is assigned a value of 55. The median is selected as the unvarying parameter because, contrary to the mean, it is not sensitive to the behavior of the tails of the distribution and therefore is unaffected by the value taken by the error factor. Based on NUREG/CR-6823, (Ref. C5.4, Section A.7.3), the median is calculated as exp(ν), where ν is obtained by the maximum likelihood estimation.

A limitation of the parametric empirical Bayes method that prevented its use for all active components of the preclosure safety analysis is that the calculated lognormal distribution can sometimes have a very small error factor (with a value around 1), corresponding to a distribution overly narrow to represent a population-variability distribution. As indicated in NUREG/CR-6823, (Ref. C5.4, p. 8-4), this situation can arise when the reliability data sources provide similar estimates for a component reliability. The inadequacy of the parametric empirical Bayes method in such situations is made apparent by plotting the probability density function of the lognormal distribution and comparing it with the likelihood functions associated with the reliability estimates of each data source. In the cases where the lognormal distribution does not approximately encompass the likelihood functions yielded by the data sources, it is not used to model the population-variability distribution. Instead, this distribution is modeled using a data source that yields a more diffuse likelihood. In the other cases, the lognormal distribution approximately encompasses the likelihood functions yielded by the data sources, showing that the parametric empirical Bayes method is adequate. An illustration of a graph plotting the population-variability distribution along with the likelihood functions from data, based on the example of the Lopez Droguett et al. paper (Ref. C5.27) is provided below.

Example of Development of Population-Variability Distribution

Mathcad is used to calculate the population-variability distribution of active components. An illustration of such a calculation is given using the example in "The Combined Use of Data and Expert Estimates in Population Variability Analysis." (Ref. C5.27, Table 1). In this example, several data sources supply information about the reliability of motor-driven pumps, as follows:

Four data sources supply point estimates of the failure rates, along with a range (error) factor. This information is given in the following matrix, where the first column contains the estimated hourly failure rate (considered to be a median value) and the second column the associated error factor:

$$A := \begin{pmatrix} 3.0 \cdot 10^{-5} & 5 \\ 2.1 \cdot 10^{-5} & 3 \\ 2.0 \cdot 10^{-5} & 10 \\ 2.53 \cdot 10^{-5} & 10 \end{pmatrix}$$

In addition, eight data sources supply exposure data, which are given in the following matrix, where a recorded number of failures is shown in the first column, and the associated operating time (in hours) is shown in the second.

$$B := \begin{pmatrix} 0 & 76000 \\ 0 & 152000 \\ 0 & 74000 \\ 2 & 74000 \\ 0 & 48000 \\ 3 & 76000 \\ 9 & 10200 \\ 2 & 48000 \end{pmatrix}$$

The population-variability distribution g of the failure rate x is approximated by a lognormal distribution whose unknown parameters, ν and τ, respectively the mean and standard deviation of the associated normal distribution, are to be determined. Calculating ν and τ involves calculating the likelihood function associated with the reliability information in each data source. This is done as follows:

For a data source providing a failure rate point estimate, the likelihood function is a lognormal distribution, function of the failure rate x, and characterized by its median value and associated error factor shown in the matrix A. In Mathcad, the parameters required for defining a lognormal distribution are the mean and standard deviation of the associated normal distribution. Based on the formulas given in NUREG/CR-6823 (Ref. C5.4, Section A.7.3), the mean of the associated normal distribution is the natural logarithm of the median failure rate, and the standard deviation of the associated normal distribution is $\ln(EF)/1.645$, where EF is the error factor.

Because the unknowns to be determined are ν and τ, the likelihood function is expressed as a function unconditional on the value of *x*. This is done by integrating the likelihood function over all possible values of *x* (i.e., theoretically, from 0 to infinity) and weighting by the probability of having a value of *x*, conditional on observing ν and τ. In practice, to facilitate the numerical integration on Mathcad, the integration is performed on a range that encompasses credible values for *x*. In this example, the failure rate range considered varies from 10^{-8}/hr to 10^{-2}/hr. Thus, the likelihood functions, unconditional on *x*, for each of the data source in the matrix *A*, are calculated as follows:

$a := 1..4$

$$fe(a,x) := dlnorm\left(x, ln(A_{a,1}), \frac{ln(A_{a,2})}{1.645}\right) \qquad \text{(Eq. C-3)}$$

$$LA(a, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fe(a,x) \cdot dlnorm(x, \nu, \tau)\, dx \qquad \text{(Eq. C-4)}$$

(In the above formulas, *a* is an index used to particularize a likelihood function to a data source in the matrix *A*.)

For a data source providing exposure data (given in the form of a number *n* of recorded failures over an exposure time *t*), the likelihood function is a Poisson distribution, expressing the probability that *n* failures are observed when the expected number of failures is *x* times *t*. Here also, the likelihood needs to be expressed as a function unconditional on the failure rate *x*, which is done by integrating *x* out, in a similar manner as above:

$b := 1..8$

$$fd(b,x) := dpois(B_{b,1}, B_{b,2} \cdot x) \qquad \text{(Eq. C-5)}$$

$$LB(b, \nu, \tau) := \int_{10^{-8}}^{10^{-2}} fd(b,x) \cdot dlnorm(x, \nu, \tau)\, dx \qquad \text{(Eq. C-6)}$$

(In the above formulas, *b* is an index used to particularize a likelihood function to a data source in the matrix *B*.)

The maximum likelihood method is used to calculate ν and τ. This involves maximizing the likelihood function for the entire set of data sources. This likelihood function is the product of the individual likelihood function for each data source (this is because the data sources are independent from each other). It is equivalent and computationally convenient to find the maximum likelihood estimators for ν and τ by using the sum of the log-likelihood (logarithm of the likelihood) of each data source.

Therefore, the log-likelihood function to be maximized is:

$$L(\nu, \tau) := \sum_{a=1}^{4} ln(LA(a, \nu, \tau)) + \sum_{b=1}^{8} ln(LB(b, \nu, \tau))$$

(Eq. C-7)

To maximize a function, Mathcad requires guess values and a range over which to search for maxima. The quantity ν represents the logarithm of a failure rate, which is expected to be in the 10^{-6}/hr range. Therefore, a guess value for ν is:

$$\nu := ln(10^{-6}) \qquad \nu = -13.8$$

Based on a typical error factor value of 10, a guess value for τ is:

$$\tau := \frac{ln(10)}{1.645} \qquad \tau = 1.4$$

A reasonable range over which to perform the likelihood maximization is as follows:

Given $\nu > -20$ $\nu < -1$

$\tau > 0.01$ $\tau < 5$

The maximum likelihood estimators for ν and τ are:

$L := Maximize(L, \nu, \tau)$ $\nu := L_1$ $\nu = -11.478$

$\tau := L_2$ $\tau = 1.874$

Therefore, the mean and error factors of the population-variability distribution for the failure rate are (based on the formula in NUREG/CR-6823 (Ref. C5.4, Section A.7.3)):

$$m := exp\left(\nu + \frac{\tau^2}{2}\right) \qquad m = 6.00 \times 10^{-5}$$ per hour

$$EF := exp(1.645 \cdot \tau) \qquad EF = 21.8$$

Notable percentiles of the population-variability distribution are as follows (expressed as hourly failure rates) and shown in Figure C2.1-1:

1st percentile: $qlnorm(0.01, \nu, \tau) = 1.32 \times 10^{-7}$

5th percentile: $qlnorm(0.05, \nu, \tau) = 4.75 \times 10^{-7}$

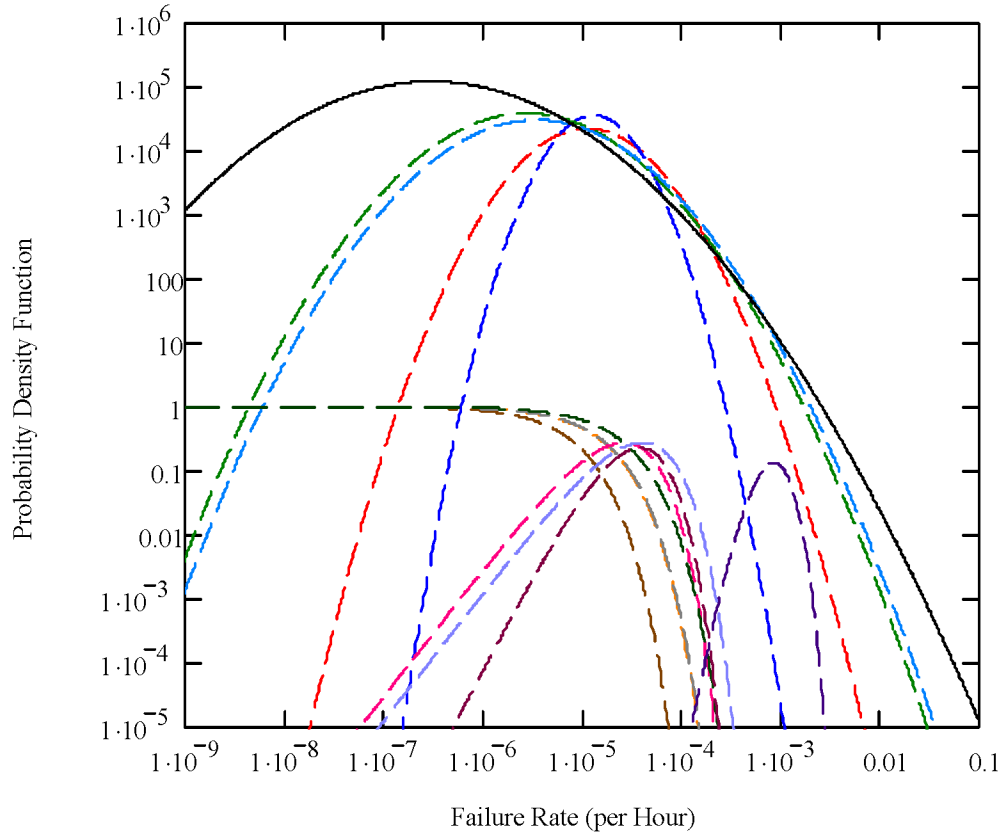
10th percentile: $qlnorm(0.10, \nu, \tau) = 9.38 \times 10^{-7}$

50th percentile: $qlnorm(0.50, \nu, \tau) = 1.04 \times 10^{-5}$

90th percentile: $qlnorm(0.90, \nu, \tau) = 1.14 \times 10^{-4}$

95th percentile: $qlnorm(0.95, \nu, \tau) = 2.26 \times 10^{-4}$

99th percentile: $qlnorm(0.99, \nu, \tau) = 8.10 \times 10^{-4}$



Source: Original

Figure C2.1-1. Likelihood Functions from Data Sources (Dashed Lines) and Population-Variability Probability Density Function (Solid Line)

C2.2 PARAMETER ESTIMATION IN CASE ONLY ONE DATA SOURCE IS AVAILABLE

To be developed, a population-variability distribution requires at least two data sources, and therefore the previous method is not applicable when only one data source is available. In this case, the probability distribution for the reliability parameter of an active component is that yielded by the data source. For example, if the data source provides a mean and an error factor for the component reliability parameter, the probability distribution is modeled in SAPHIRE as a lognormal distribution with that mean and that error factor. If the data source does not readily provide a probability distribution, but instead exposure data (i.e., a number of recorded failures over an exposure time for failure rates, or over a number of demands for failure probabilities) the probability distribution for the reliability parameter is developed through a Bayesian update using Jeffreys' noninformative prior distribution. As indicated in NUREG/CR-6823 (Ref. C5.4,

Section 6.2.2.5.2), this noninformative prior conveys little prior belief or information, thus allowing the data to speak for themselves.

As mentioned in "Bayesian Parameter Estimation in Probabilistic Risk Assessment," (Ref. C5.44, Section 4.2), the likelihood function associated with exposure data is either a Poisson distribution (in the case of failure rates), or a binomial distribution (in the case of failure probabilities).

Applying Bayes' theorem with Jeffreys' noninformative prior in conjunction with a Poisson likelihood function characterized by r recorded failures over an exposure time t results in a closed-form posterior distribution, namely a gamma distribution, characterized by a shape parameter equal to $0.5 + r$, and a scale parameter equal to t; the mean of this distribution is $(0.5 + r)/t$ (Ref. C5.4, Sections 6.2.2.5.2 and A7.6). In SAPHIRE, this distribution is characterized by its mean and by its shape parameter (i.e., $0.5 + r$).

Applying Bayes' theorem with Jeffreys' noninformative prior in conjunction with a binomial likelihood function characterized by r recorded failures out of n demands results in a closed-form posterior distribution, namely a beta distribution, characterized by a parameter "a" equal to $0.5 + r$, and a parameter "b" equal to $n - r + 0.5$; the mean of this distribution is $(0.5 + r)/(n + 1)$ (Ref. C5.4, Sections 6.3.2.3.2 and A7.8). In SAPHIRE, this distribution is characterized by its mean and by the parameter "b" (i.e., $n - r + 0.5$).

C3 COMMON-CAUSE FAILURE DATA

Dependent failures are modeled in event tree and fault tree logic models, with potential dependent failures modeled explicitly via the logic models, whenever possible. For example, failure of the HVAC system is explicitly dependent upon failures in the electrical supply systems that are modeled in the fault trees. Similarly, the effects of erroneous calibration or other human failure events can be explicitly included in the system fault tree models and the basic event probabilities considered during the human reliability analysis. Otherwise, potential dependencies known as common-cause failures are included in fault tree logic, but their probabilities are quantified by an implicit, parametric method. Therefore, another subtask of the active component reliability data analysis is to estimate common-cause failure probabilities.

Surveys of failure events in the nuclear industry have led to several parameter models. Of these, three are most commonly used: the Beta Factor method (Ref. C5.18), the Multiple Greek Letter method (Ref. C5.29) and (Ref. C5.30), and the Alpha Factor method (Ref. C5.31). These methods do not require an explicit knowledge of the dependence failure mode. For the YMP PCSA, CCF rates or probabilities were estimated using the alpha factor method described in NUREG/CR-5485 (Ref. C5.31).

The vast majority of the equipment types for which CCF basic events were modeled in the YMP PCSA are not covered by the detailed component-specific alpha factor sources based on commercial nuclear plant equipment. Therefore, it was necessary to use alpha factors to address the CCF estimates for crane hoist wire ropes, gear boxes, over-torque sensors and the like.

The alpha factor method provides a model to treat common-cause failure probabilities of k-of-m components. In addition, industry-wide alpha factors have been developed for the U.S. Nuclear

Regulatory Commission from experience data collected at nuclear power plants. The data analysis reported in NUREG/CR-5485 (Ref. C5.31) consisted of:

1. Identifying the number of redundant components in each subsystem being reported (e.g., two, three, or four (this is termed the CCF group size, common-cause component group (CCCG) of size *m*)).

2. Partitioning the total number of reported failure events for a given component into the number of components that failed together, i.e., $k = 1$ for one component at a time, $k = 2$ for two components at a time, $k = 3$ for three components at a time, up to m for failure of all components in a given CCF group.

3. Estimating the alpha factor for a given component type based on its definition as the fraction of total failure events that involve k component failures due to common-cause, for a system of m redundant components, using the alpha factor estimator from NUREG/CR-5485 (Ref, C5.31, Table 5-10), as shown below

$$\alpha_k^m = \frac{n_k}{\sum_{j=1}^{m} n_j} \qquad k = 1, \ldots, m \quad ;$$

   where n_i is the number of basic events observed that involve failure of i similar components.

4. Performing statistical analysis and curve fitting to define the mean and uncertainty range for alpha factors for various CCF group sizes up to eight.

The data analysis also produced industry-wide prior distributions for the alpha factors for each CCCG size, based on all CCF events in their database. Events were mapped to a given CCCG size, the maximum likelihood estimator obtained and fit to a constrained noninformative prior distribution. The parameter A_T of a Dirichlet distribution was then calculated for each alpha and the results combined using the geometric mean. The results are the industry-wide mean alpha factors and beta uncertainty distributions reported in NUREG/CR-5485 (Ref. C5.31, Table 5-11) as shown in Table C3-1.

Table C3-1. Industry-Wide Alpha Factors

Table 5-11. Generic prior distributions for various system sizes.

CCCG Size m	α-Factor	Distributions Parameters		Percentiles			Mean
		a	b	P_{05}	P_{50}	P_{95}	
2	α_1	9.5300	0.470	8.20E-01	9.78E-01	1.00E-00	0.95300
	α_2	0.4700	9.530	1.42E-04	2.16E-02	1.81E-01	0.04700
3	α_1	15.2000	0.800	8.42E-01	9.67E-01	9.99E-01	0.95000
	α_2	0.3872	15.613	2.10E-05	8.79E-03	1.01E-01	0.02420
	α_3	0.4128	15.587	3.45E-05	1.01E-02	1.05E-01	0.02580
4	α_1	24.7000	1.300	8.67E-01	9.61E-01	9.95E-01	0.95000
	α_2	0.5538	25.446	1.44E-04	1.08E-02	7.81E-02	0.02130
	α_3	0.2626	25.737	2.98E-07	1.99E-03	4.82E-02	0.01010
	α_4	0.4836	25.516	6.29E-05	8.42E-03	7.17E-02	0.01860
5	α_1	38.042	1.958	8.86E-01	9.58E-01	9.91E-01	0.95106
	α_2	0.7280	39.272	3.72E-04	1.10E-02	6.05E-02	0.01820
	α_3	0.4120	39.588	1.32E-05	3.93E-03	4.22E-02	0.01030
	α_4	0.2336	39.766	4.57E-08	8.97E-04	2.89E-02	0.00584
	α_5	0.5840	39.416	1.24E-04	7.66E-03	5.27E-02	0.01460
6	α_1	50.4724	2.528	8.97E-01	9.58E-01	9.89E-01	0.95231
	α_2	0.7791	52.221	3.76E-04	9.20E-03	4.78E-02	0.01470
	α_3	0.5406	52.459	6.04E-05	5.02E-03	3.79E-02	0.01020
	α_4	0.3127	52.687	9.28E-07	1.56E-03	2.66E-02	0.00590
	α_5	0.2433	52.757	5.77E-08	7.67E-04	2.24E-02	0.00459
	α_6	0.6519	52.348	1.66E-04	6.93E-03	4.27E-02	0.01230
7	α_1	74.5360	3.464	9.12E-01	9.59E-01	9.86E-01	0.95559
	α_2	0.9906	77.009	6.44E-04	8.84E-03	3.79E-02	0.01270
	α_3	0.6817	77.318	1.39E-04	5.05E-03	2.99E-02	0.00874
	α_4	0.4891	77.511	2.21E-05	2.82E-03	2.42E-02	0.00627
	α_5	0.2941	77.706	3.39E-07	8.97E-04	1.74E-02	0.00377
	α_6	0.2051	77.795	3.84E-09	2.94E-04	1.35E-02	0.00263
	α_7	0.8034	77.197	2.89E-04	6.52E-03	3.32E-02	0.01030
8	α_1	97.6507	4.349	9.20E-01	9.60E-01	9.84E-01	0.95736
	α_2	1.1118	100.888	7.25E-04	7.91E-03	3.13E-02	0.01090
	α_3	0.7915	101.209	2.07E-04	4.87E-03	2.52E-02	0.00776
	α_4	0.6253	101.375	6.92E-05	3.34E-03	2.17E-02	0.00613
	α_5	0.4417	101.558	8.51E-06	1.76E-03	1.74E-02	0.00433
	α_6	0.2581	101.742	6.09E-08	4.74E-04	1.21E-02	0.00253
	α_7	0.1969	101.803	1.59E-09	1.93E-04	1.00E-02	0.00193
	α_8	0.9241	101.076	3.82E-04	6.12E-03	2.78E-02	0.00906

Source: NUREG/CR-5485 (Ref. C5.31)

Values from Table C3-1 are applied to the YMP PCSA 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 factor for *k*-of-*m* components for failure-on-demand events (e.g., pump failure to start). For example, for a 2-out-of-2 failure-on-demand event, the mean alpha factors of 0.953 and 0.047 shown in the far right column of Table C3-1 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 is selected from the SAPHIRE code library of potential common-cause models to yield the common-cause failure probability.

For failure-to-operate events (e.g., pump fails to run), the mean alpha factor (M) for events with more than one failure from Table C3-1 is divided by 2 in accordance with NUREG/CR-5485 (Ref. C5.31). (The mean alpha factor for events with one failure is computed as 1 minus the sum of the remaining alpha factors.) To preserve the coefficient of variation, 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 4 results from allowing the standard deviation to be reduced by a factor of 2, like the mean, but because the variance is the square of the standard deviation, the variance is reduced by a factor of 4. The following formulas give the mean and variance of a beta distribution in terms of the parameters a and b (Ref. C5.4, Section A.7.8). To derive an alpha factor for a failure-to-operate event, the mean alpha factor is taken from Table C3-1 (or computed from the following formula) and divided by 2.

$$M = \frac{a}{a+b}.$$

Then, the variance is calculated from the following formula and divided by 4.

$$V = \frac{a \cdot b}{(a+b)^2 \cdot (a+b+1)}.$$

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.

$$b = \frac{\left(M - M^2 - V\right) \cdot (1 - M)}{V}$$

Table C3-2 provides values taken or derived from Table C3-1 in the form required by SAPHIRE, that is, the mean alpha factor and the parameter b, which together completely specify the uncertainty distribution.

Table C3-2. Alpha Factor Inputs for SAPHIRE

SAPHIRE Template Event Identifier[a]	Mean Alpha Factor	Uncertainty Parameter (*b*)
ALPHADEM-1OF2	0.95300	0.470
ALPHADEM-2OF2	0.04700	9.530
ALPHARUN-1OF2	0.97650	0.0506
ALPHARUN-2OF2	0.02350	21.036
ALPHADEM-1OF3	0.95000	0.800
ALPHADEM-2OF3	0.02420	15.613
ALPHADEM-3OF3	0.02580	15.587
ALPHARUN-1OF3	0.97500	0.847
ALPHARUN-2OF3	0.01210	33.018
ALPHARUN-3OF3	0.01290	33.018
ALPHADEM-1OF4	0.95000	1.300
ALPHADEM-2OF4	0.02130	25.446
ALPHADEM-3OF4	0.01010	25.737
ALPHADEM-4OF4	0.01860	25.516
ALPHARUN-1OF4	0.97500	1.361
ALPHARUN-2OF4	0.01065	53.016
ALPHARUN-3OF4	0.00505	53.005
ALPHARUN-4OF4	0.00930	53.012
ALPHADEM-2OF8	0.09812	28.600
ALPHARUN-2OF8	0.04906	64.646
ALPHADEM-8OF8	0.00906	101.076
ALPHARUN-8OF8	0.00453	205.014

NOTE: [a] The identifier follows the pattern ALPHAXXX-kOFn, where XXX = DEM for failures on demand, XXX = RUN for failures during operation, *n* represents the size of the CCF group, and *k* is the number of failed items within the CCF group.

This approach was considered to provide conservative CCF data for all the component types for which common-causes were modeled. This was considered particularly important since the YMP has never operated and therefore the applicability of conventional nuclear plant alpha factors could not be justified.

The conservatism of this approach can be demonstrated by comparing the alpha factors used for the PCSA diesel generator CCF events to those posted on the U.S. Nuclear Regulatory Commission website for use in Probabilistic Risk Assessment studies of commercial nuclear power plants in the U.S.

The alpha factor used for the PCSA for 2 of 2 diesel generators failing to start was the 0.047 value cited earlier, while the mean alpha factor for a CCCG=2 cited by the NRC (Ref. C5.36) is 0.0136.

Diesel generators are the only component types for which such a comparison can be made since the other YMP component types for which CCFs were modeled were not covered by the NRC equipment-specific alpha factors.

C4 ACTIVE COMPONENT RELIABILITY ESTIMATES INPUT TO SAPHIRE

Since the primary active component reliability data task objective is to support the quantification of fault tree models developed in SAPHIRE by the system analysts, the output data had to conform to the format appropriate for input to the SAPHIRE code.

SAPHIRE provides template data to the fault tree models in the form of three input comma delimited files:

- BEA – attributes to assign information to the proper SAPHIRE fields
- BED – descriptions of the component type name and failure mode
- BEI – information on the failure rate or probability estimates and distributions used.

Demonstration files for the .BEA, .BED and .BEI template data files provided with SAPHIRE were originally used to construct the PCSA template data files to ensure the proper formatting of the data for use by the fault tree models. In general, the .BEA file provides attribute designators for the code to implement such that the template data is properly assigned to the appropriate fields in SAPHIRE. The .BED file allows description information to be entered and linked to the template data name or designator (which in the YMP PCSA case was the TYP-FM coding). Examples of descriptions used for the PCSA template data were Clutch Failed to Operate, Relay Spurious Operation, Position Sensor Fails on Demand, and Wire Rope Breaks. The .BEI file contains the actual active component reliability parameters, namely the mean value and uncertainty parameter, either the Lognormal Error Factor, or the shape parameter of the Beta or Gamma distributions.

Geometric means of the input parameters from the industry-wide data sources were initially used as screening values for each TYP-FM and were entered into the .BEI file, along with a default Error Factor of 10. Once the Bayesian combination process was completed for all 275 TYP-FM combinations, mean and uncertainty parameter information was entered into the .BEA files, and tested in SAPHIRE before being distributed to the systems analysts.

Failure probability per demand information was entered as SAPHIRE Calculation Type 1 for a simple probability and failure rate per hour information was entered as SAPHIRE Calculation Type 3 as a mean failure rate in the lambda field. Calc Type 3 uses the formula $P = 1 - \exp(-\lambda T_m)$, where λ is the mean failure rate (or lambda) and T_m is the mission time. Mission time is defined in the SAPHIRE Basics manual as "…the period of time that a component is required to operate in order to characterize the component operation as successful." Since the template data was to be used for all YMP facilities while the mission times would be system-specific, the mission time field in the three template data files was left blank and these times were instead input individually by the systems analysts.

The correlation class field was also used for the YMP template data files "to account for data dependencies among like events in the database" during the uncertainty analysis, as stated in the

SAPHIRE Basics manual. This meant that all components in the same correlation class would be treated the same during the uncertainty analysis. This feature of SAPHIRE is based upon the observations documented (Ref. C5.2) that in the risk models, all components of the same type are quantified with the same failure rate or probability, therefore it is appropriate to group together the experience of all the nominally identified components in the same facility. Therefore, all components of the same type and failure mode are aggregated into a single number, meaning that the dependency between components of the same class must somehow be addressed. For example, if multiple motor-operated valves needed to open for success and all are assigned the same failure probability, then these basic events needed to be correlated via being assigned the same correlation class in the .BEI file. However, if different probabilities were to be used for different motor-operated valves based on the data, then the basic events would not be correlated. In all cases, a correlation class identifier, using the TYP-FM acronyms, was input to the .BEI file to indicate that all equipment with in the same TYP-FM should be correlated by the SAPHIRE model. SAPHIRE then would sample from one distribution and then use this sampled probability for all other basic events with the same correlation class.

The template data was also identified by TYP-FM combination and was utilized by the fault tree models by being imported into SAPHIRE using the MAR-D portion of the code, then by using the Modify Event feature to link the template data to each basic event in the fault tree. This permitted each active component of the same type and failure mode to utilize the same failure estimate and uncertainty information, based on the results of the industry-wide data investigation and Bayesian combination process.

Table C4-1 shows the active component reliability estimates that were input to SAPHIRE as template data for fault tree model quantification.

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
AHU-FTR	Air Handling Unit Failure to Run	G	5.00E-01	—	3.80E-06	1 source; N/D	NUREG/CR-6928 (Ref. C5.16)
ALM-SPO	Alarm/Annunciator Spurious Operation	L	1.30E+01	—	4.74E-07	5 sources N/D; 1 source mean	IEEE-500 (Ref. C5.23), NPRD-95 (Ref. C5.40)
AT-FOH	Actuator (Electrical) Failure	L	1.24E+01	—	7.54E-05	3 sources; N/D	NPRD-95 (Ref. C5.40)
ATH-FOH	Actuator (Hydraulic) Failure	L	3.81E+01	—	8.91E-04	4 sources; N/D	NPRD-95 (Ref. C5.40)
ATP-SPO	Actuator (Pneumatic Piston) Spurious Operation	L	5.00E+00	—	1.34E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
AXL-FOH	Axle Failure	G	5.00E-01	—	1.60E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
B38-FOH	Bearing Failure	L	1.13E+01	—	2.50E-06	8 sources; N/D	NPRD-95 (Ref. C5.40)
BEA-BRK	Lifting Beam/Boom Breaks	G	1.50E+00	—	2.40E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
BLD-RUP	Air Bag Ruptures	B	1.10E+04	1.36E-04	—	1 source; N/D	BSC 2007 (Ref. C5.7)
BLK-FOD	Block or Sheaves Failure on Demand	B	1.30E+06	1.15E-06	—	1 source; N/D	NPRD-95 (Ref. C5.40)
BRH-FOD	Brake (Hydraulic) Failure on Demand	L	5.50E+01	8.96E-06	—	3 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
BRK-FOD	Brake Failure on Demand	L	6.30E+00	1.46E-06	—	3 sources; mean + EF	EPRI PRA (Ref. C5.8)
BRK-FOH	Brake (Electric) Failure	G	2.50E+00	—	4.40E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
BRP-FOD	Brake (Pneumatic) Failure on Demand	L	2.55E+00	5.02E-05	—	4 sources; N/D	NPRD-95 (Ref. C5.40)
BRP-FOH	Brake (Pneumatic) Failure	L	2.55E+00	—	8.38E-06	4 sources; N/D	NPRD-95 (Ref. C5.40)
BTR-FOD	Battery No Output Given Challenge	B	6.05E+01	8.20E-03	—	1 source; N/D	NUREG/CR-4639 (Ref. C5.39)
BTR-FOH	Battery Failure	L	4.30E+00	—	4.29E-06	12 sources N/D; 8 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41)
BUA-FOH	AC Bus Failure	L	3.08E+00	—	6.10E-07	3 sources; N/D	IEEE 493 (Ref. C5. 22), NUREG/CR-6928 (Ref. C5.16)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
BUD-FOH	DC Bus Failure	L	8.70E+01	—	2.40E-07	1 source mean + EF	IEEE-500 (Ref. C5.23)
BYC-FOH	Battery Charger Failure	L	1.00E+01	—	7.60E-06	1 source mean + EF	CCPS (Ref. C5.1)
C52-FOD	Circuit Breaker (AC) Fails on Demand	L	9.80E+00	2.24E-03	—	19 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
C52-SPO	Circuit Breaker (AC) Spurious Operation	L	2.29E+01	—	5.31E-06	12 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NUREG/CR-6928 (Ref. C5.16), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
C72-SPO	Circuit Breaker (DC) Spurious Operation	L	1.20E+00	—	1.07E-06	3 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
CAM-FOH	Cam Lock Fails	L	8.30E+01	—	3.19E-06	4 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
CBP-OPC	Cables (Electrical Power) Open Circuit	G	5.00E-01	—	9.13E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CBP-SHC	Cables (Electrical Power) Short Circuit	G	5.00E-01	—	1.88E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CKV-FOD	Check Valve Fails on Demand	L	1.36E+01	6.62E-04	—	4 sources N/D; 7 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
CKV-FTX	Check Valve Fails to Check	L	1.50E+01	2.20E-03	—	1 source; mean + EF	CCPS (Ref. C5.1)
CON-FOH	Electrical Connector (Site Transporter) Failure	G	5.00E-01	—	7.14E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
CPL-FOH	Coupling (Automatic) Failure	L	5.00E+00	—	1.91E-06	1 source mean + EF	AIAA (Ref. C5.11)
CPO-FOH	Control System Onboard (TEV or Trolley) Failure	G	9.85E+01	—	2.10E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CRD-FOH	Card Reader Failure	L	5.00E+00	—	4.55E-05	1 source mean + EF	HID (Ref. C5.21)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
CRJ-DRP	Jib Crane Drop	B	8.74E+05	6.41E-05	—	1 source; N/D	NUREG-0612 (Ref. C5.35)
CRN-DRP	200 Ton Crane Drop	L	4.32E+01	3.16E-05	—	2 sources N/D; 4 sources mean + EF	NUREG-0612 (Ref. C5.35), NUREG-1774 (Ref. C5.26), EPRI PRA (Ref. C5.8)
CRN-TBK	200 Ton Crane Two Block Drop	L	1.15E+01	4.41E-07	—	1 source N/D; 3 sources mean + EF	NUREG-0612 (Ref. C5.35), NUREG-1774 (Ref. C5.26)
CRS-DRP	200 Ton Crane Sling Drop	B	2.13E+04	1.17E-04	—	1 source; N/D	NUREG-1774 (Ref. C5.26)
CRW-DRP	WP (Non-Single Failure Proof) Crane Drop	B	3.27E+04	1.07E-04	—	1 source; N/D	NUREG-1774 (Ref. C5.26)
CRW-TBK	WP (Non-Single Failure Proof) Crane Two Block Drop	B	3.27E+04	4.59E-05	—	1 source; N/D	NUREG-1774 (Ref. C5.26)
CSC-FOH	Cask Cradle Failure	G	1.50E+00	—	4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
CT-FOD	Controller Mechanical Jamming	L	5.00E+00	4.00E-06	—	1 source; mean + EF	EPRI PRA (Ref. C5.8)
CT-FOH	Controller Failure	L	1.00E+01	—	6.88E-05	1 source mean + EF	CCPS (Ref. C5.1)
CT-SPO	Controller Spurious Operation	L	1.00E+01	—	2.27E-05	1 source mean + EF	CCPS (Ref. C5.1)
CTL-FOD	Logic Controller Fails on Demand	L	1.10E+01	2.03E-03	—	3 sources; N/D	NUREG/CR-6928 (Ref. C5.16)
DER-FOM	Derailment Failure per Mile	G	3.97E+03	—	1.18E-05	1 source; N/D	Federal Railroad Administration (Ref. C5.17)
DG-FTR	Diesel Generator Fails to Run	L	1.51E+01	—	4.08E-03	8 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), IEEE 493 (Ref. C5.22), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-3831 (Ref. C5.24), NUREG/CR-6890 (Ref. C5.15), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
DG-FTS	Diesel Generator Fails to Start	L	3.50E+00	8.38E-03	—	9 sources N/D; 1 source mean + EF	CCPS (Ref. C5.1), IEEE 493 (Ref. C5.22), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-3831 (Ref. C5.24), NUREG/CR-6890 (Ref. C5.15), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
DGS-FTR	Diesel Generator - Seismic - Fails to Run for 29 Days	G	5.05E+01	—	8.27E-04	1 source, N/D	NUREG/CR-6890 (Ref. C5.15)
DM-FOD	Drum Failure on Demand	L	1.00E+01	4.00E-08	—	2 sources mean + EF	EPRI PRA (Ref. C5.8)
DM-MSP	Drum Misspooling (Hourly)	G	5.00E-01	—	6.86E-07	1 source, N/D	NPRD-95 (Ref. C5.40)
DMP-FOH	Damper (Manual) Fails to Operate	L	4.30E+00	—	5.94E-06	3 sources mean + EF	IEEE-500 (Ref. C5.23), N-Reactor (Ref. C5.46), Moss (Ref. C5.32)
DMP-FRO	Damper (Manual) Fails to Remain Open (Transfers Closed)	L	3.20E+00	—	8.38E-08	2 sources N/D; 2 sources mean + EF	NUREG/CR-3154 (Ref. C5.6), NUREG/CR-1363 (Ref. C5.28), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)
DMS-FOH	Demister (Moisture Separator) Failure	L	5.00E+00	—	9.12E-06	1 source mean + EF	EPRI AP-2071 (Ref. C5.10)
DRV-FOH	Drive (Adjustable Speed) Failure	G	5.0E-01	—	2.5E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
DRV-FSO	Drive (Adjustable Speed) Failure to Stop on Demand	B	2.5E+02	—	3.4E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
DTC-RUP	Duct Ruptures	L	2.6E+01	—	3.7E-06	9 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40), SRS Reactors (Ref. C5.5), SAIC Umatilla (Ref. C5.41)
DTM-FOD	Damper (Tornado) Failure on Demand	L	5.0E+00	8.7E-04	—	1 source; mean + EF	IEEE-500 (Ref. C5.23)
DTM-FOH	Damper (Tornado) Failure	L	7.9E+00	—	2.3E-05	2 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), Moss (Ref. C5.32)
ECP-FOH	Position Encoder Failure	G	5.0E-01	—	1.8E-06	2 sources; N/D	NPRD-95 (Ref. C5.40)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
ESC-FOD	Emergency Stop Button Controller Failure to Stop (on Demand)	L	5.0E+00	2.5E-04	—	1 source; mean + EF	EPRI PRA (Ref. C5.8)
FAN-FTR	Fan (Motor-Driven) Fails to Run	L	4.6E+01	—	7.21E-05	11 sources N/D; 6 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
FAN-FTS	Fan (Motor-Driven) Fails to Start on Demand	L	1.0E+01	2.0E-03	—	7 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
FRK-PUN	Forklift Puncture	L	1.06E+01	—	1.20E-05	1 source mean + EF	SAIC Umatilla (Ref. C5.41)
G65-FOH	Governor Failure	G	1.82E+02	—	1.16E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
GPL-FOD	Grapple Failure on Demand	B	1.30E+06	1.15E-06	—	1 source; N/D	NPRD-95 (Ref. C5.40)
GRB-FOH	Gear Box Failure	L	1.40E+01	—	2.21E-04	1 source N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
GRB-SHH	Gear box Shaft/Coupling Shears	L	5.00E+00	—	2.40E-06	1 source; mean + EF	EPRI PRA (Ref. C5.8)
GRB-STH	Gear Box Stripped	L	5.00E+00	—	7.86E-08	1 source; mean + EF	NPRD-95 (Ref. C5.40)
HC-FOD	Hand Held Radio Remote Controller Failure to Stop (on Demand)	L	8.39E+01	1.74E-03	—	1 source N/D; 3 sources mean + EF	EPRI PRA (Ref. C5.8), NPRD-95 (Ref. C5.40)
HC-SPO	Hand Held Radio Remote Controller Spurious Operation	G	5.00E-01	—	5.23E-07	1 source N/D	NPRD-95 (Ref. C5.40)
HEP-LEK	Filter (HEPA) Leaks (Bypassed)	L	1.00E+01	—	3.00E-06	1 source; mean + EF	SRS Reactors (Ref. C5.5)
HEP-PLG	Filter (HEPA) Plugs	L	9.5E+00	—	4.3E-06	3 sources N/D; 2 sources mean + EF	IEEE-500 (Ref. C5.23), NUREG/CR-4639 (Ref. C5.39), SAIC Umatilla (Ref. C5.41)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
HOS-LEK	Hose Leaking	L	2.47E+01	—	1.48E-05	same as HOS-RUP with factor of 10	CCPS (Ref. C5.1), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
HOS-RUP	Hose Ruptures	L	2.47E+01	—	1.48E-06	2 sources N/D; 3 sources mean + EF	CCPS (Ref. C5.1), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
IEL-FOD	Interlock Failure on Demand	L	5.0E+00	2.8E-05	—	1 source; mean + EF	NPRD-95 (Ref. C5.40)
IEL-FOH	Interlock Failure	L	5.50E+01	—	3.43E-05	4 sources; N/D	NPRD-95 (Ref. C5.40)
LC-FOD	Level Controller Failure on Demand	B	6.07E+03	6.25E-04	—	1 source; N/D	NUREG/CR-6928 (Ref. C5.16)
LRG-FOH	Lifting Rig or Hook Failure	G	4.65E+01	—	7.45E-07	1 source; N/D	NPRD-95 (Ref. C5.40)
LVR-FOH	Lever (two position; up-down) Failure	G	9.85E+01	—	2.10E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
MCC-FOH	Motor Control Centers (MCCs) Failure	L	1.00E+01	—	7.49E-06	composite of Relay (RLY-FTP) + Motor Starter (MST FOH) + Limit Switch (ZS-FOH)	
MOE-FOD	Motor (Electric) Fails on Demand	L	5.00E+00	6.00E-05	—	1 source; mean + EF	EPRI PRA (Ref. C5.8)
MOE-FSO	Motor (Electric) Fails to Shut Off	L	1.07E+01	—	1.35E-08	1 source N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12)
MOE-FTR	Motor (Electric) Fails to Run	L	9.50E+00	—	6.50E-06	8 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), OREDA-2002 (Ref. C5.43)
MOE-FTS	Motor (Electric) Fails to Start (Hourly)	L	1.90E+01	—	7.14E-06	5 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40)
MOE-SPO	Motor (Electric) Spurious Operation	L	1.07E+01	—	6.74E-07	1 source N/D; 1 source mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12)
MOH-FOH	Motor (Hydraulic) Failure	G	5.00E-01	—	2.50E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
MSC-FOH	Motor Speed Control Module Failure	G	5.00E-01	—	1.28E-04	1 source; N/D	NPRD-95 (Ref. C5.40)
MST-FOH	Motor Starter Failure	L	1.33E+00	—	1.43E-07	2 sources; N/D	IEEE 493 (Ref. C5.22)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
NZL-FOH	Nozzle Failure	L	7.50E+00	—	2.85E-06	5 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PIN-BRK	Pin (Locking or Stabilization) Breaks	L	1.46E+00	—	2.12E-09	4 sources; N/D	NPRD-95 (Ref. C5.40)
PLC-FOD	Programmable Logic Controller Fails on Demand	B	1.35E+03	3.69E-04	—	1 source; N/D	NPRD-95 (Ref. C5.40)
PLC-FOH	Programmable Logic Controller Fails to Operate	L	1.00E+01	—	3.26E-06	5 sources N/D; 1 source mean + EF	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PLC-SPO	Programmable Logic Controller Spurious Operation	L	1.00E+01	—	3.65E-07	5 sources N/D; 1 source mean + EF	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SAIC Umatilla (Ref. C5.41)
PMD-FTR	Pump (Motor Driven) Fails to Run	L	9.9E+00	—	3.5E-05	6 sources N/D; 87 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-1205 (Ref. C5.45), NUREG/CR-2886 (Ref. C5.13), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
PMD-FTS	Pump (Motor Driven) Fails to Start on Demand	L	3.80E+00	2.50E-03	—	7 sources N/D; 80 sources mean + EF	N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-1205 (Ref. C5.45), NUREG/CR-2886 (Ref. C5.13), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43), SAIC Umatilla (Ref. C5.41), SRS Reactors (Ref. C5.5)
PPL-RUP	Piping (Lined) Catastrophic	L	1.50E+01	—	4.42E-07	1 source; mean + EF	CCPS (Ref. C5.1)
PPM-PLG	Piping (Water) Plugs	L	1.35E+01	—	7.26E-07	1 source N/D; 2 sources mean + EF	DuPont (Ref. C5.14), EPRI Pipe Failure Study (Ref. C5.10), SAIC Umatilla (Ref. C5.41)
PPM-RUP	Piping (Water) Ruptures	L	2.00E+01	—	8.75E-10	1 source; mean + EF	NUREG/CR-6928 (Ref. C5.16)
PR-FOH	Passive restraint (bumper) Failure	G	2.09E+02	—	4.45E-10	1 source; N/D	NPRD-95 (Ref. C5.40)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
PRM-FOH	EPROM (HVAC Speed Control) Failure	G	5.00E-01	—	5.38E-07	1 source; N/D	MIL-HDBK-217F (Ref. C5.12)
PRV-FOD	Pressure Relief Valve Fails on Demand	L	2.72E+01	6.54E-03	—	6 sources N/D; 2 sources mean + EF	CCPS (Ref. C5.1), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
PV-SPO	Pneumatic Valve Spurious Operation	G	5.00E-01	—	2.92E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
QDV-FOH	Quick Disconnect Valve Failure	L	3.56E+00	—	4.26E-06	4 sources N/D	NPRD-95 (Ref. C5.40)
RCV-FOH	Air Receiver Fails to Supply Air	L	1.00E+01	—	6.00E-07	1 source; mean + EF	IEEE-500 (Ref. C5.23)
RLY-FTP	Relay (Power) Fails to Close/Open	G	5.00E-01	—	8.77E-06	1 source N/D	NPRD-95 (Ref. C5.40)
SC-FOH	Speed Control Failure	G	5.00E-01	—	1.28E-04	1 source N/D	NPRD-95 (Ref. C5.40)
SC-SPO	Speed Control Spurious Operation	G	5.00E-01	—	3.20E-05	1 source N/D	NPRD-95 (Ref. C5.40)
SEL-FOH	Speed Selector Fails	L	5.34E+00	—	4.16E-06	3 sources N/D	NPRD-95 (Ref. C5.40)
SEQ-FOD	Sequencer Fails on Demand	B	7.49E+02	3.33E-03	—	1 source N/D	NUREG/CR-6928 (Ref. C5.16)
SFT-COL	Spent Fuel Transfer Machine (SFTM) Collision or Impact	L	4.00E+00	2.94E-06	—	2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SFT-DRP	Spent Fuel Transfer Machine (SFTM) Drop	L	3.00E+00	5.15E-06	—	2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SFT-RTH	Spent Fuel Transfer Machine (SFTM) Raised Fuel Too High	L	7.00E+00	7.36E-07	—	2 sources N/D	NUREG-1774 (Ref. C5.26), McKenna (Ref. C5.20)
SJK-FOH	Screw Jack (TEV) Failure	G	5.00E-01	—	8.14E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
SRF-FOH	Flow Sensor Failure	G	5.00E-01	—	1.07E-06	1 source; N/D	NUREG/CR-4639 (Ref. C5.39)
SRP-FOD	Pressure Sensor Fails on Demand	B	1.25E+02	4.00E-03	—	1 source; N/D	NPRD-95 (Ref. C5.40)
SRP-FOH	Pressure Sensor Fails	L	1.21E+01	—	2.95E-06	8 sources N/D	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16)
SRR-FOH	Radiation Sensor Fails	L	5.00E+00	—	2.00E-05	1 source; mean + EF	Laurus (Ref. C5.25)
SRS-FOH	Over Speed Sensor Fails	G	1.28E+02	—	2.14E-05	1 source; N/D	NPRD-95 (Ref. C5.40)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
SRT-FOD	Temperature Sensor/Transmitter Fails on Demand	L	2.10E+00	7.33E-04	—	2 sources N/D	NUREG/CR-6928 (Ref. C5.16), OREDA-92 (Ref. C5.42)
SRT-FOH	Temperature Sensor/Transmitter Fails	L	1.41E+01	—	7.05E-07	4 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NUREG/CR-6928 (Ref. C5.16), OREDA-2002 (Ref. C5.43)
SRT-SPO	Temperature Sensor Spurious Operation	L	2.80E+01	—	2.23E-06	1 source; mean + EF	OREDA-2002 (Ref. C5.43)
SRU-FOH	Ultrasonic Sensor Fails	G	5.00E-01	—	9.62E-05	1 source; N/D	NPRD-95 (Ref. C5.40)
SRV-FOH	Vibration Sensor (Accelerometer) Fails	L	1.07E+01	—	9.40E-05	4 sources N/D	NPRD-95 (Ref. C5.40)
SRX-FOD	Optical Position Sensor Fails on Demand	B	3.18E+03	1.10E-03	—	1 source; N/D	SAIC Umatilla (Ref. C5.41)
SRX-FOH	Optical Position Sensor Fails	L	5.00E+00	—	4.70E-06	1 source; mean + EF	NPRD-95 (Ref. C5.40)
STR-FOH	Steering (tractor or trailer) Fails	L	4.63E+01	—	1.84E-05	4 sources N/D	NPRD-95 (Ref. C5.40)
STU-FOH	Structure (truck or railcar) Failure	G	1.50E+00	—	4.81E-08	1 source; N/D	NPRD-95 (Ref. C5.40)
SV-FOD	Solenoid Valve Fails on Demand	L	1.17E+01	6.28E-04	—	4 sources N/D; 5 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NSWC-98-LE1 (Ref. C5.37), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)
SV-FOH	Solenoid Valve Fails	L	1.70E+01	—	4.87E-05	1 source; mean + EF	CCPS (Ref. C5.1)
SV-SPO	Solenoid Valve Spurious Operation	L	3.00E+00	—	4.09E-07	1 source; mean + EF	CCPS (Ref. C5.1)
SWA-FOH	Auto-Stop Switch (CTT hose travel) Fails	G	6.50E+00	—	3.12E-06	1 source; N/D	NPRD-95 (Ref. C5.40)
SWG-FOH	13.8kV Switchgear Fails	G	2.85E+01	—	1.31E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
SWP-FTX	Electric Power Switch Fails to Transfer	G	6.50E+00	—	3.59E-07	1 source; N/D	IEEE 493 (Ref. C5.22)
SWP-SPO	Electric Power Switch Spurious Transfer	G	6.50E+00	—	1.55E-07	1 source; N/D	IEEE 493 (Ref. C5.22)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
TD-FOH	Transducer Failure	L	4.70E+00	—	9.84E-05	3 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
TDA-FOH	Transducer (Air Flow) Failure	L	6.21E+00	—	1.65E-04	2 sources N/D	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37)
TDP-FOH	Transducer (Pressure) Fails	L	5.35E+01	—	2.20E-04	23 sources N/D; 2 sources mean + EF	NPRD-95 (Ref. C5.40), NSWC-98-LE1 (Ref. C5.37)
TDT-FOH	Transducer (Temperature) Fails	L	2.95E+01	—	1.04E-04	12 sources N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40)
THR-BRK	Third Rail Breaks	L	1.00E+01	—	1.01E-08	1 source; mean + EF	NPRD-95 TRK-BRK adjusted with failure information from Federal Railroad Administration Safety Data website (Ref. C5.17)
TKF-FOH	Fuel Tank Fails	L	1.11E+01	—	4.40E-07	15 sources; N/D	NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
TL-FOH	Torque Limiter Failure	G	8.05E+01	—	8.05E-05	1 source N/D	NPRD-95 (Ref. C5.40)
TRD-FOH	Tread (Site Transporter)	L	3.40E+00	—	5.89E-07	1 source N/D; 1 source mean + EF	NPRD-95 (Ref. C5.40), Rand (Ref. C5.38)
UDM-FOH	Damper (Backdraft) Failure	L	7.90E+00	—	2.26E-05	2 sources N/D; 1 source mean + EF	IEEE-500 (Ref. C5.23), Moss (Ref. C5.32)
UPS-FOH	Uninterruptible Power Supply (UPS) Failure	L	5.08E+00	—	2.02E-06	10 sources; N/D	NPRD-95 (Ref. C5.40)
WNE-BRK	Wire Rope Breaks	L	5.00E+00	2.00E-06	—	1 source; mean + EF	EPRI PRA (Ref. C5.8)
XMR-FOH	Transformer Failure	L	1.53E+01	—	2.91E-07	13 sources N/D; 2 sources mean + EF	CCPS (Ref. C5.1), MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16)
XV-FOD	Manual Valve Failure on Demand	L	1.00E+01	6.48E-04	—	3 sources N/D; 12 sources mean + EF	CCPS (Ref. C5.1), N-Reactor (Ref. C5.46), NUREG/CR-4639 (Ref. C5.39), NUREG/CR-6928 (Ref. C5.16), SRS Reactors (Ref. C5.5)

Table C4-1. Active Component Reliability Estimates Entered into SAPHIRE Models (Continued)

TYP-FM	Component Name & Failure Mode	Dist. Type	Uncert. Value	Demand Proba-bility	Hourly Failure Rate	Number of Inputs	Input Data Sources[a]
ZS-FOD	Limit Switch Failure on Demand	L	5.7E+00	2.9E-04	—	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), SRS Reactors (Ref. C5.5)
ZS-FOH	Limit Switch Fails	L	6.03E+00	—	7.23E-06	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39)
ZS-SPO	Limit Switch Spurious Operation	L	5.56E+00	—	1.28E-06	3 sources N/D	MIL-HDBK-217F (Ref. C5.12), NPRD-95 (Ref. C5.40), NUREG/CR-4639 (Ref. C5.39)

NOTE: [a] Refer to Section C1.2 for specific citation to data sources.

B = beta distribution; Dist. = Distribution; EF = Lognormal Error Factor; G = gamma distribution; L = lognormal distribution; N/D = Numerator/Denominator; TYP-FM = component type and failure mode.

Source: Original

C5 REFERENCES; DESIGN INPUTS

The PCSA is based on a snapshot of the design. The reference design documents are appropriately documented as design inputs in this section. Since the safety analysis is based on a snapshot of the design, referencing subsequent revisions to the design documents (as described in EG-PRO-3DP-G04B-00037, *Calculations and Analyses* (Ref. 2.1.1, Section 3.2.2.F)) that implement PCSA requirements flowing from the safety analysis would not be appropriate for the purpose of the PCSA.

The inputs in this Section noted with an (*) indicate that they fall into one of the designated categories described in Section 4.1, relative to suitability for intended use.

C5.1 *AIChE (American Institute of Chemical Engineers) 1989. *Guidelines for Process Equipment Reliability Data with Data Tables.* G-07. New York, New York: American Institute of Chemical Engineers, Center for Chemical Process Safety. TIC: 259872. ISBN: 978-0-8169-0422-8.

C5.2 *Apostolakis, G. and Kaplan, S. 1981. "Pitfalls in Risk Calculations." *Reliability Engineering, 2,* 135-145. Barking, England: Applied Science Publishers. TIC: 253648.

C5.3 ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).* New York, New York: American Society of Mechanical Engineers. TIC: 257672. ISBN: 0-7918-2939-1.

C5.4 *Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment.* NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121.

C5.5 *Blanton, C.H. and Eide, S.A. 1993. *Savannah River Site, Generic Data Base Development (U).* WSRC-TR-93-262. Aiken, South Carolina: Westinghouse Savannah River Company. TIC: 246444.

C5.6 *Borkowski, R.J.; Kahl, W.K.; Hebble, T.L.; Fragola, J.R.; Johnson, J.W. 1983. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report-The Valve-Component.* NUREG/CR-3154. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071129.0315.

C5.7 BSC 2007 (Bechtel SAIC Company). *Waste Form Throughputs for Preclosure Safety Analysis.* 000-PSA-MGR0-01800-000-00A. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071106.0001.

C5.8 *Canavan, K.; Gregg, B.; Karimi, R.; Mirsky, S.; and Stokley, J. 2004. *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks, Updated Quantification and Analysis Report.* 1009691. Palo Alto, California: Electric Power Research Institute. TIC: 257542.

C5.9 *Crutchfield, D.M. 1996. "Movement of Heavy Loads Over Spent Fuel, Over Fuel in the Reactor Core, or Over Safety-Related Equipment." NRC Bulletin 96-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. Accessed February 12, 2008. ACC: MOL.20080213.0021. URL: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/bulletins/1996/bl96002.html

C5.10 *Derdiger, J.A.;Bhatt, K.M.;Siegfriedt, W.E. 1981. *Component Failure and Repair Data for Coal-Fired Power Units*. AP-2071. Palo Alto, California: Electric Power Research Institute. TIC: 260070.

C5.11 *Dhillon, B.S. 1988. *Mechanical Reliability: Theory, Models and Applications.* AIAA Education Series. Washington, D.C.: American Institute of Aeronautics & Astronautics. TIC: 259878.

C5.12 *DOD (U.S. Department of Defense) 1991. *Military Handbook, Reliability Prediction of Electronic Equipment.* MIL-HDBK-217F. Washington, D.C.: U.S. Department of Defense. TIC: 232828.

C5.13 *Drago, J.P.; Borkowski, R.J.; Fragola, J.R.; and Johnson, J.W. 1982. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report — The Pump Component.* NUREG/CR-2886. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0222.

C5.14 *E.I. du Pont de Nemours & Company 1981. *Some Published and Estimated Failure Rates for Use in Fault Tree Analysis*. Wilmington, Delaware: E.I. du Pont de Nemours & Company. TIC: 260092

C5.15 *Eide, S.A.; Gentillon, C.D.; Wierman, T.E.; and Rasmuson, D.M. 2005. *Analysis of Station Blackout Risk.* Volume 2 of *Reevaluation of Station Blackout Risk at Nuclear Power Plants.* NUREG/CR-6890. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071114.0165.

C5.16 *Eide, S.A.; Wierman, T.E.; Gentillon, C.D.; Rasmuson, D.M.; and Atwood, C.T. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.* NUREG/CR-6928. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071211.0229.

C5.17 *Federal Railroad Administration 2004. "Train Accidents by Cause from Form FRA F 6180.54." Washington, D.C.: U.S. Department of Transportation, Federal Railroad Administration. Accessed 03/12/2004. ACC: MOL.20040311.0211. URL: http://safetydata.fra.dot.gov/OfficeofSafety/Query/Default.asp

C5.18 *Fleming, K.N. 1975. *A Reliability Model for Common Mode Failures in Redundant Safety Systems.* GA-A13284. San Diego, California: General Atomic Company. ACC: MOL.20071219.0221.

C5.19 *Fragola, J.R. and McFadden, R.H. 1995. "External Maintenance Rate Prediction and Design Concepts for High Reliability and Availability on Space Station Freedom."

Reliability Engineering and System Safety, 47, 255-273. New York, New York: Elsevier. TIC: 259675.

C5.20 *Framatome ANP (Advanced Nuclear Power) 2001. *Summary, Commercial Nuclear Fuel Assembly Damage/Misload Study – 1985-1999.* Lynchburg, Virginia: Framatome Advanced Nuclear Power. ACC: MOL.20011018.0158.

C5.21 *HID Corporation [n.d.]. Ruggedized Card Reader/Ruggedized Keypad Card Reader. Dorado 740 and 780. Irvine, California: HID Corporation. TIC: 260007.

C5.22 *IEEE Std 493-1997. 1998. *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 243205. ISBN: 1-55937-969-3.

C5.23 *IEEE Std 500-1984 (Reaffirmed 1991). 1991. *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations.* New York, New York: Institute of Electrical and Electronics Engineers. TIC: 256281.

C5.24 *Kahl, W.K. and Borkowski, R.J. 1985. *The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report - Diesel Generators, Batteries, Chargers, and Inverters.* NUREG/CR-3831. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071212.0181.

C5.25 *Laurus Systems [n.d.]. Instruments and Software Solutions for Emergency Response and Health Physics. Ellicott City, Maryland: Laurus Systems. TIC: 259965.

C5.26 Lloyd, R.L. 2003. *A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002.* NUREG-1774. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20050802.0185.

C5.27 *Lopez Droguett, E.; Groen, F.; and Mosleh, A. 2004. "The Combined Use of Data and Expert Estimates in Population Variability Analysis." *Reliability Engineering and System Safety, 83,* 311-321. New York, New York: Elsevier. TIC: 259380.

C5.28 *Miller, C.F.; Hubble, W.H.; Trojovsky, M.; and Brown, S.R. 1982. *Data Summaries of Licensee Event Reports of Valves at U.S. Commercial Nuclear Power Plants from January 1, 1976 to December 31, 1980.* NUREG/CR-1363, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071219.0223.

C5.29 *Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Analytical Background and Techniques.* Volume 2 of *Procedures for Treating Common Cause Failures in Safety and Reliability Studies.* NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

C5.30 *Mosleh, A.; Fleming, K.N.; Parry, G.W.; Paula, H.M.; Worledge, D.H.; and Rasmuson, D.M. 1988. *Procedural Framework and Examples.* Volume 1 of *Procedures for*

Treating Common Cause Failures in Safety and Reliability Studies. NUREG/CR-4780. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 221775.

C5.31 *Mosleh, A.; Rasmuson, D.M.; and Marshall, F.M. 1998. *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment.* NUREG/CR-5485. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20040220.0106.

C5.32 *Moss, T.R. 2005. *The Reliability Data Handbook.* New York, New York: American Society of Mechanical Engineers Press. TIC: 259912. ISBN: 0-7918-0233-7.

C5.33 Not Used.

C5.34 NRC (U.S. Nuclear Regulatory Commission) 1979. *Single-Failure-Proof Cranes for Nuclear Power Plants.* NUREG-0554. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 232978.

C5.35 NRC 1980. *Control of Heavy Loads at Nuclear Power Plants.* NUREG-0612. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 209017.

C5.36 NRC 2005. *CCF Parameter Estimation 2005.* Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20080213.0022.

C5.37 *NSWC (Naval Surface Warfare Center) 1998. *Handbook of Reliability Prediction Procedures for Mechanical Equipment.* NSWC-98/LE1. West Bethesda, Maryland: Naval Surface Warfare Center, Carderock Division. TIC: 245703.

C5.38 *Peltz, E.; Robbins, M.; Boren, P.; Wolff, M. 2002. *Diagnosing the Army's Equipment Readiness: The Equipment Downtime Analyzer.* Santa Monica, California: RAND. TIC: 259917. ISBN: 0-8330-3115-5.

C5.39 *Reece, W.J.; Gilbert, B.G.; and Richards, R.E. 1994. *Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR), Volume 5: Data Manual, Part 3: Hardware Component Failure Data.* NUREG/CR-4639, Vol. 5, Rev. 4. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071220.0209.

C5.40 *Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. *Nonelectronic Parts Reliability Data 1995.* NPRD-95. Rome, New York: Reliability Analysis Center. TIC: 259757.

C5.41 *SAIC (Science Applications International Corporation) 2002. *Umatilla Chemical Agent Disposal Facility Quantitative Risk Assessment.* Report No. SAIC-00/2641. Volume I. Abingdon, Maryland: Science Applications International Corporation. ACC: MOL.20071220.0210.

C5.42 *SINTEF Industrial Management 1992. *OREDA, Offshore Reliability Data Handbook.* 2nd Edition. Trondheim, Norway: OREDA. ISBN: 825150188.1

C5.43 *SINTEF Industrial Management 2002. *OREDA, Offshore Reliability Data Handbook.* 4th Edition. Trondheim, Norway: OREDA. ISBN: 8214027055. TIC: 257402.

C5.44 *Siu, N.O. and Kelly, D.L. 1998. "Bayesian Parameter Estimation in Probabilistic Risk Assessment." *Reliability Engineering and System Safety, 62,* 89-116. New York, New York: Elsevier. TIC: 258633.

C5.45 *Trojovsky, M. 1982. *Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to September 30, 1980.* NUREG/CR-1205, Rev. 1. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20080207.0024.

C5.46 *Zentner, M.D.; Atkinson, J.K.; Carlson, P.A.; Coles, G.A.; Leitz, E.E.; Lindberg, S.E.; Powers, T.B.; and Kelly, J.E. 1988. *N Reactor Level 1 Probabilistic Risk Assessment: Final Report.* WHC-SP-0087. Richland, Washington: Westinghouse Hanford Company. ACC: MOL.20080207.0021.