3. COMPONENT FAILURE AND BOUNDARY DEFINITIONS

3.1 Failure Definitions

While the terms "faults" and "failures" are casually used interchangeably, in the context of fault tree analysis these terms have more distinct meanings. Thus, for data analysis, it is necessary for one to understand the distinctions. Generally speaking, all failures are faults, but not all faults are failures. To put it another way, failures comprise a subset of the larger set of faults. For probabilistic risk assessment (PRA) purposes, **failures** are regarded as basic (and undesired) events which:

- render a component, subsystem, or system incapable of performing its intended function,
- represents a basic fault tree input that is not analyzed further, and
- require numerical estimates if quantification is to be performed.

Faults, on the other hand, are higher order events (representing the occurrence or existence of an undesired state of a component or set of components) which are analyzed further, and ultimately resolved into their constituent failures (Breeding, Leahy, and Young 1985; ANS and IEEE 1983; and Vesely et al. 1981).

The failures modeled in PRA can have many causes or mechanisms. For example, failure of a motor-operated valve (MOV) to open on demand can occur due to physical problems with the valve (stem failure, disc separation, etc.), problems with the motor operator (motor failure, control circuit failure, breaker failure, etc.), or due to loss of motive or control power. In addition, the MOV may be unavailable due to test or maintenance on its constituent parts. As such, each failure (i.e., basic event) is the sum of the contributions from each piece-part included in the component boundary. Thus, it is critical to define what the component boundary is in order to get the right data.

3.2 Component Boundary Definitions

In order to collect failure data for components, it is necessary to define **component boundaries** by specifying the scope of each item to be considered as a single entity. The PRA model and the data collection should be coordinated so that the boundaries of the components are defined identically. For example, all pieces of an MOV are typically considered to be part of a single "component" when collecting reliability data even though the valve consists of various piece parts (e.g., electric motor, gearbox, limit switches, torque switches, reversing contacts and coils, stem, disc, valve body, etc.) that may be separately identified in the plant maintenance records. PRAs typically do not model failures of every switch, relay, or contact in a control circuit of a pump because that type of detail is difficult to obtain from the plant data. Instead, failures of these components are typically included with actual failures of the pump to establish a pump failure rate.

If generic data sources are used, it becomes the responsibility of the analyst to ensure that the component boundary definitions used in the generic data source are compatible with the boundary definitions used by the PRA being performed.

Some typical examples of component boundaries are shown in Table 3.1. The boundaries of a component should include all components specific to the component. However, the component boundary should not include piece-parts that are shared with other components modeled in the PRA. For example, the component boundary for emergency-actuated valves commonly includes the valve control circuit. However, the components needed to generate an actuation signal that initiates multiple components modeled in the PRA should not be included as part of that specific valve boundary. Similarly, a diesel generator boundary will typically include the fuel day tank but the fuel oil transfer pumps are not included since they are required for operation of all the plant's diesel generators.

3.3 Failure Severity

The raw data for a specific component will contain some events not relevant to the component failure modes being analyzed. These events can be screened from further analysis. Some of the events will be component failures that should be included in the data assessment. The type of component failures will determine how they are classified and subsequently used to generate the required component failure data.

Component malfunction events are commonly classified into one of the following three **failure severity** categories:

Table 3.1 Examples of component boundaries.

Component	Component Boundary
Diesel Generators	The diesel generator boundary includes the generator body, generator actuator, lubrication system (local), fuel system (local), cooling components (local), startup air system, exhaust and combustion air system, individual diesel generator control system, circuit breaker for supply to safeguard buses and their associated local control circuit (coil, auxiliary contacts, wiring, and control circuit contacts) with the exception of all the contacts and relays which interact with other electrical or control systems.
Motor Pumps	The pump boundary includes the pump body, motor/actuator, lubrication system cooling components of the pump seals, the voltage supply breaker, and its associated local control circuit (coil, auxiliary contacts, wiring, and control circuit contacts).
Turbine-Driven Pumps	The turbine-driven pump boundary includes the pump body, turbine/actuator, lubrication system (including pump), extractions, turbopump seal, cooling components, and local turbine control system (speed).
Motor-Operated Valves	The valve boundary includes the valve body, motor/actuator, the voltage supply breaker and its associated local open/close circuit (open/close switches, auxiliary and switch contacts, and wiring and switch energization contacts).
Air-Operated Valves	The valve boundary includes the valve body, the air operator, associated solenoid-operated valve, the power supply breaker or fuse for the solenoid valve, and its associated control circuit (open/close switches and local auxiliary and switch contacts).
Fans	The fan boundary includes the fan, the voltage supply breaker, and its associated control circuit (open/close switches and local auxiliary and switch contacts).
Batteries	The battery component boundary typically includes just the battery. Battery chargers are modeled as separate components.
Bus Circuit Breakers	A bus circuit breaker boundary includes the breaker and its associated control circuit (open/close switches and local auxiliary and switch contacts).

- catastrophic failures,
- degraded failures, and
- incipient failures.

A **catastrophic (complete) failure** is one that prevents the component from performing its mission as defined in the PRA (Whitehead 1993). Catastrophic failures require some kind of repair or replacement action on the component in order to restore the component to operability. For example, a valve that fails to open due to a valve operator mechanical failure is a catastrophic failure.

A **degraded failure** is such that a component can perform its mission, but at less than the optimum performance level (Whitehead et al. 1993). An **incipient failure** is such that there is no significant degradation in performance but there are indications of a developing fault (Whitehead et al. 1993). The difference between the two is generally a matter of severity. For example, an event involving pump shaft vibration indicates possible damage to the pump bearings. Severe vibration may be considered as degraded failure if the pump produces less than maximum flow. Shaft seizure or other failures could occur within a few hours if the pump remains running and thus would likely be removed from operation for corrective maintenance. In contrast, minor vibration may not result in degraded flow. This would thus be an incipient failure. The significance of this event is that it also could result in removal of the pump from operation for inspection, lubrication, or some other corrective action. Information about the types of repairs made, the parts replaced, and the urgency of the repairs often provides important insight about the severity of these two types of component failures.

Although both degraded and incipient failures will typically lead to a corrective action, the corrective action may or may not make the component unavailable to perform its function. For example, maintenance on the operator of a valve that is normally open will not lead to the unavailability of the valve if it is required to be open for system operation. This illustrates the importance of ascertaining from event records the modes of a component operation that a corrective action would prevent.

Sometimes the event information is so unclear and incomplete that a definite classification of the severity of a component malfunction event is not possible. For example, Mosleh and Apostolakis (1985) cites one maintenance work request issued at a nuclear power plant that described the problem as follows: "Check valve RHR-V-1A is leaking badly." The maintenance foreman's description of the corrective action read: "Fixed it, not leaking anymore!" No further information was available. From the description given, one cannot say for sure whether the leak was internal or external, or whether it was large enough to result in functional failure of the check valve.

Unfortunately, the above example is not uncommon. Descriptions of the malfunctions and repairs are often very brief. The data analyst, then, is faced with the difficult task of deciding whether to call a malfunction a failure or not. The inability to distinguish between severity levels of failures is particularly important as the difference between the frequencies of catastrophic and degraded modes of failures can be significant. Therefore, in the absence of sufficient information, the conservative assumption could be made that all such events be recorded as catastrophic failures. Unfortunately, conservative categorization of uncertain events can lead to significantly higher failure rates.

Ultimately, the definition of failure from the system analysis decides the classification of the data. Thus, the failure of a component must match the definition of the failure as described in the PRA model. A component must fail to perform its function as defined in the model. For example, a relief valve that opens at 1,115 psig instead of the required 1,110 psig is not failed, although it may be described as failed by the governing technical specifications, and a pump that delivers 645 gpm instead of the required 700 gpm is not failed if 645 gpm is sufficient for the function that it is required to perform.

4. DATA SOURCES

Two types of data sources can be utilized to produce the various parameter estimates that are needed in a probabilistic risk assessment (PRA). This chapter identifies and discusses these two data sources. Section 4.1 identifies and discusses plant-specific data sources. Section 4.2 does the same for generic data sources.

4.1 Plant-Specific Data Sources

Use of plant-specific data in a PRA produces risk estimates that reflect the actual plant experience.

The scope of a plant-specific data analysis is determined by the events that are included in the PRA models. In general, plant-specific data are generally reviewed for the following types of events:

1. The accident initiating events analyzed in the PRA.

2. The components included in system models (generally fault trees). For components the definition includes the component boundary and failure mode. For unavailabilities due to maintenance or testing it is necessary to know whether the unavailabilities are to be specified at the component, segment, train, or system level.

3. Some recovery events included in the PRA models. Although most recovery events are analyzed using human reliability analysis, the probabilities of some events can be based upon a review of operating experience.

Once the data needs are identified, the sources of raw data at the plant are identified. In most cases, the information needed may have to come from multiple sources. For example, identification of maintenance events and their duration may come from a control room log, but other sources such as maintenance work requests may be required to determine other information such as whether a component had experienced a catastrophic or degraded failure.

There are many sources of raw data at a nuclear power plant. Different plants have different means of recording information on initiating events and component failure and maintenance events. Since no one source exists at a nuclear power plant that contains all the necessary data, different sources must be reviewed. The ease in which the plant-specific data can be interpreted and the subsequent quality of the resulting parameter estimates are a function of how well the plant personnel recorded the necessary information.

Basic requirements associated with raw data sources and some typical sources of raw data available at nuclear power plants are identified in the following sections.

4.1.1 Requirements on Data Sources

There are a variety of data sources that exist at a plant and can be used in a data analysis. However, there are some basic requirements that these raw data sources should meet in order to be useful. Some typical requirements, some of which were suggested in EPRI TR-100381 (EPRI 1992), are delineated below.

4.1.1.1 Initiating Events

For reports on initiating events it is essential to include the status of those systems that would be impacted as a result of the event. This is typically not a problem since the Licensee Event Report (LER) that is required to be filed with the Nuclear Regulatory Commission (NRC) following a plant trip usually contains this type of information. It is also common for utilities to generate additional detailed trip reports that delineate the cause and effects of the event. Such reports need to specify critical information needed for data analysis such as the power level at the time of the plant trip and the sequence of events, including the timing of individual events.

4.1.1.2 Component Failures

For each event at a plant resulting in the unavailability of a component, it is necessary that the raw data sources identify the particular component or set of components associated with the event. In order to determine if a specific event contributes to a particular component failure mode or to an unavailability due to the component being in maintenance (either preventive or corrective), it is necessary to be able to distinguish between different degrees of degradation or failure. The event reports should therefore specify whether maintenance was required and if the maintenance was corrective or preventive. If the component maintenance is preventive there is generally no failure that initiates the maintenance.

If an event involves corrective maintenance, information is required to allow determination of the severity of the failure (see Section 3.3 for definitions of event severity). The ability to distinguish between severity levels of failures is particularly important since the difference between the frequencies of catastrophic and degraded modes of failures can be significant. In addition, information is required to determine the component in which the failure actually occurred and the mode of failure. Finally, it should be possible to determine the time the component is unavailable during each maintenance event.

The data analysis may use plant data on component unavailability that is being collected for other than PRA purposes. The requirements for recording the data for these other purposes may use definitions of severity and failure modes that are different from the PRA definitions. The definitions used for the data collection programs should be determined and an appropriate translation to the PRA basic events made.

4.1.1.3 Recovery Events

The information needed to estimate the probabilities associated with recovering specific components or systems from a failed state is similar to that needed for component failures. Specific information pertaining to the type of failure experienced by the component or system (e.g., fail to operate, fail to start, fail to run), the number of repair occurrences, and the time required to perform the repair is needed to produce component repair probabilities.

4.1.2 Data Sources

Data sources that can provide information for determining the number of initiating events include:

- internal plant failure records (e.g., scram reports or unusual event reports),
- operator logs,
- LERs, and
- monthly operating reports/Gray Book.

Some data sources that typically provide information on the occurrence of component failures include:

- LERs,
- internal plant failure records (e.g., failure reports, trouble reports, or unusual event reports),
- maintenance records (e.g., maintenance work orders, work request records),
- plant logs (e.g., control room log, component history logs), and
- data bases (e.g., Equipment Performance and Information Exchange System/Nuclear Plant Reliability Data System).

The evaluation of component failure rates also requires the number of demands and operating time for the components. Sources of data for these parameters include:

- monthly operating reports/Gray Book,
- component history logs,
- plant population lists,
- test procedures,
- plant operating procedures, and
- component demand or operating time counters

Repair information can be obtained from sources such as:

- plant logs and
- maintenance work orders.

The type of information available in these sources and their limitations are discussed in the following sections.

4.1.2.1 Regulatory Reports

All plants are required to submit LERs to the NRC for all events meeting the 10 CFR 50.73 reporting criteria presented in NUREG-1022 (NRC 2000a). LERs deal with significant events related to the plant, including plant shutdowns required by the technical specifications, multiple train failures, engineered safety feature actuations, and conditions outside the design basis or not covered by plant procedures. An LER includes an abstract that describes the major occurrences during the event; the components, systems, or human failures that contributed to the event; the failure mode, mechanism, and effect of each failed component; and an estimate of the elapsed time from the discovery of the failure until the safety system train was returned to service. A computerized search of LER information is possible using the Sequence Coding and Search System (SCSS) (Gallaher et al. 1984).

LERs generally provide a good description of the causes of a reactor trip and subsequent events. However, their value for obtaining component failure data is very limited. The reporting criteria are limited to safety-related trains or system failures, and therefore LERs are not generally submitted for all failures. Furthermore, LERs may not be submitted for every

safety-related component failure since individual component failures do not have to be reported if redundant equipment in the same system was operable and available to perform the safety function. The reporting criteria for LERs are also subject to interpretation by the persons generating the reports and thus can lead to inconsistencies in the LER data base. Furthermore, there are other perceived deficiencies in the LERs (Whitehead et al. 1993) that limit the usefulness of the LER system for use in obtaining estimates of component failure rates. The NRC staff prepared NUREG-1022, Revision 1 (NRC 1998), to address general issues in reporting that have not been consistently applied. It covers some of the issues identified above.

The LER rule published in 1983 has recently been amended and the reporting guidance in NUREG-1022, Revision 2 (NRC 2000a) has been revised to eliminate the burden of reporting events of little or no safety significance, to better align the rules with the NRC's current needs and to clarify the reporting guidance where needed. However, the rule still only requires the reporting of failures leading to the unavailability of safety-related system trains. Thus, LERs will not provide failure data for all risk significant components.

In summary, LERs are a good source for identifying and grouping initiating events. However, they have very limited value for obtaining component failure data.

A plant's Technical Specifications requires that a monthly operating report be provided by the plant licensee to the NRC. The scope of the information requested of the licensees was originally identified in Draft Regulatory Guide 1.16 (NRC 1975a) and includes operating statistics and shutdown experience information. The information requested to be included in the monthly operating report contents was revised by Generic Letter 97-02 (NRC 1997) and eliminated some reporting requirements. Information that still must be reported includes identification of all plant shutdowns, whether they were forced or scheduled shutdowns, their duration, the reason for the shutdown, the method of shutting down the reactor, and corrective actions that were taken. In addition, the monthly operating reports include the number of hours the reactor was critical, the number of hours the generator was on line, and the net electrical output of the plant.

The NRC initially compiled the information from the monthly operating reports on a monthly basis and published it in a hard copy form as NUREG-0020, "Licensed Operating Reactors - Status Summary Report" (NRC 1995b). This document is referred to as the "Gray Book." NUREG-0020 was discontinued after the December 1995 report. However, the data requested in Generic Letter 97-02 is being collected and computerized as part of the NRC Performance Indicator Project.

In summary, the monthly operating reports provide information on the number of scrams, the time spent at full power, and the time spent in shutdown. This information can be used in identifying and grouping initiating events and in calculating the exposure time in which they occurred. It is important to note that this same information is generally available from the control room logs and other sources. Thus, in general, the monthly operating reports can be used to supplement or verify other data sources.

4.1.2.2 Internal Plant Failure Reports

Different plants have different means of recording initiating events and component failures. For each automatic and manual scram, most plants generate an internal scram report. Scram reports generally cover the same information provided in LERs and monthly operating reports. Thus, they can be used as the primary or supplementary source for evaluating plant scrams.

Most plants have a means of recording component failures, records that are for the licensee's own use rather than for a regulatory use. Reports are generally created when significant component failures or degraded states occur during plant operation or are identified during plant surveillance tests. These reports may be called Unusual Occurrence Reports, Action Reports, Failure Reports, Discrepancy Reports, or Trouble Reports. Some of the events documented in these reports may lead to an LER. However, these reports may not identify all component failures and generally are not exhaustive. Thus, these reports are useful for supplemental information but are not a good source of component reliability data.

4.1.2.3 Maintenance Records

At all plants, some form of written authorization form is required to initiate corrective or preventative maintenance work, or design changes. These authorization forms are known under different names at various plants including work request/completion records, maintenance work orders, clearance requests, work requests, or tag-out orders. Maintenance records are a primary source of component failure data since

they usually identify the component being maintained, whether the component has failed or is degraded, the corrective action taken, and the duration of the maintenance action. The time of the failure is also available but maintenance records generally contain limited information on the impact, cause, and method of discovery of the component failure.

4.1.2.4 Plant Logs

At each plant, a control room log is typically completed for each shift and contains a record of all important events at a plant. Control room logs identify power level and plant mode changes, essential equipment status changes, major system and equipment tests, and entry and exit of Technical Specification Limiting Conditions of Operation (LCOs). When properly maintained, a control room log is a good source of information on major equipment and unit availability. However, the amount of information entered can vary from shift to shift. Furthermore, the entries tend to be brief.

The control room logs are difficult to use as a source of maintenance data since the tag-out and tag-in for a maintenance event may span days or even months and may not be dutifully recorded. The control room logs are also limited in value as a source of component failure data since not all failures may be recorded by the operators. Component maintenance and failure information is generally found more easily in maintenance work orders. All plant trips are likely to be recorded on control room logs, but likely will not include a description of the cause of the trip or the subsequent transient behavior. LERs or plant scram reports must be reviewed to obtain this additional information.

In summary, control room logs are good supplementary sources of information but there are usually more convenient and complete sources of information available such as maintenance records. However, the control room logs are probably the best source of data for indicating when redundant system trains are switched from operating to standby status.

There may be other logs at a plant that contain essential data. One example is a component history log. These logs typically contain data on every failure and maintenance and test action for a given component. As such, component history logs are good sources for identifying not only the number of component failures, but also the number of demands a component experiences.

4.1.2.5 Component Exposure Data Sources

Calculation of plant-specific failure rates requires determination of the number of failures and the corresponding number of demands or operating time. As indicated in the previous subsections, some of the data sources used to establish the number of failures also contain information on the number of demands and operating time. However, these sources do not contain all component demands or the operating time for all components. Additional documents that must be reviewed for information about component demands and operating hours include test procedures.

In addition to demands presented by automatic initiations and maintenance activities (obtained from sources such as control room logs and maintenance records), periodic testing is an important source of demands especially for safety-related equipment. To establish the number of demands due to testing, testing procedures pertinent to a component must be reviewed. In addition to the actual test demands, additional test demands may be imposed by technical specifications following failure of a component. A typical example where this is imposed is when a diesel generator is unavailable for operation. Test logs or similar records can be examined to obtain an estimate of the number of tests carried out during the time period of interest.

It should also be noted that at some plants, some major components may be monitored to count the number of actuations experienced by the breakers (breaker cycle counters). In addition, the operating hours for large motor-driven components at some plants may be automatically registered on running time meters at the electrical switchgear. Such counters and logs can be used to supplement the demand and operating time information obtained from other sources.

4.1.3 Plant-Specific Data Bases

The Institute of Nuclear Power Operations (INPO) has maintained several databases of component failure data provided by each nuclear power plant since 1984. The first, Nuclear Plant Reliability Data System (NPRDS), was a proprietary computer-based collection of engineering, operational, and failure data on systems and components in U.S. nuclear power plants through 1996. The second, the Equipment Performance and Information Exchange (EPIX) System, replaced NPRDS and includes data reported since 1987. Both data bases are discussed in the following sections.

4.1.3.1 Nuclear Plant Reliability Data System (NPRDS)

In the early 1970s, industry committees of the American National Standards Institute (ANSI) and the Edison Electric Institute (EEI) recognized the need for failure data on nuclear plant components. As a result, a data collection system was developed whose objective was to make available reliability statistics (e.g., failure rates, mean-time-between-failures, mean-time-to-restore) for safety related systems and components.

This system, the Nuclear Plant Reliability Data System (Tashjian 1982), was developed by Southwest Research Institute (SwRI). Plants began reporting data on a voluntary basis in 1974, and continued reporting to SwRI until 1982. In January 1982, the INPO assumed management responsibility for the system until reporting was terminated at the end of 1996.

Originally the scope of the NPRDS covered the systems and components classified by ANSI standards as Safety Class 1, 2, or 1E, with a few exceptions such as reactor vessel internals and spent fuel storage. However, later the scope was expanded to cover any system important to safety and any system for which a loss of function can initiate significant plant transients (Simard 1983). By the end of 1984, 86 nuclear power plant units were supplying detailed design data and failure reports on some 4,000 to 5,000 plant components from 30 systems (Simard 1985).

Data reported to NPRDS consisted of two kinds: engineering reports and failure reports. The engineering reports provided detailed design and operating characteristics for each reportable component. The failure reports provided information on each reportable component whenever the component was unable to perform its intended function. The same operational data contained in NUREG-0200 was also included in the system. The NPRDS failure reports provided to INPO were generally generated by plant licensees utilizing maintenance records such as maintenance work orders. These reports utilized a standard set of component boundaries and failure mode definitions.

4.1.3.1.1 Limitations in the Data Available from the NPRDS

Several issues regarding the quality and utility of the NPRDS data have been observed, including:

1. Input to NPRDS was discontinued on December 31, 1996.
2. The number of component demands is provided by estimation.
3. The exposure time is estimated.
4. The amount of time needed to repair components out for corrective maintenance is not provided.
5. Maintenance rates are not provided.
6. The voluntary nature of the reporting system introduces uncertainty into measuring the frequency at which a particular type of problem occurs.
7. The final results of a problem investigation or the ultimate corrective action taken are not always included.
8. Report entries tend to be brief and often do not provide enough information to identify the exact failure mechanism.

4.1.3.2 Equipment Performance and Information Exchange (EPIX) System

The need for high-quality, plant-specific reliability and availability information to support risk-informed applications was one impetus for a proposed reliability data rule by the NRC to require utilities to provide such information. Instead of a regulatory rule, the nuclear industry committed to voluntarily report reliability information for risk-significant systems and equipment to the EPIX system. EPIX is a web-based database of component engineering and failure data developed by INPO to replace NPRDS. The utilities began reporting to EPIX on January 1, 1997.

EPIX enables sharing of engineering and failure information on selected components within the scope of the NRC's Maintenance Rule (10 CFR 50.65) and on equipment failures that cause power reductions. It also provides failure rate and reliability information for a limited number of risk-significant plant components. This includes components in the systems included in the scope of the Safety System Performance Indicator (SSPI) program. EPIX consists of:

- a site-specific database controlled by each INPO member site with web-based data entry and retrieval,
- an industry database on the INPO web site where selected parts of the site-specific database are shared among plants, and
- a retrieval tool that provides access to the vast historical equipment performance information available in the NPRDS.

Events reported to EPIX include both complete failures of components and degraded component operation. The number of demands and operating hours (i.e., reliability data) and the unavailability are required to be collected for key components in the SSPI safety systems for each plant. In addition, contributors to EPIX are also to include one-time estimates of the number of demands and run hours for other risk-significant components not included in SSPI systems.

4.1.3.3 Reliability and Availability Data System (RADS)

The NRC has developed the Reliability and Availability Data System (RADS) to provide the reliability and availability data needed by the NRC to perform generic and plant-specific assessments and to support PRA and risk-informed regulatory applications. The NRC is incorporating data from EPIX and INPO's SSPI system along with information from other data sources (e.g., LERs and monthly operating reports) into RADS. Data are available for the major components in the most risk-important systems in both boiling water reactors (BWRs) and pressurized water reactors (PWRs).

The reliability parameters that can be estimated using RADS are:

- probability of failure on demand,
- failure rate during operation (used to calculate probability of failure to continue operation),
- maintenance out-of-service unavailability (planned and unplanned), and
- time trends in reliability parameters.

The statistical methods available in RADS include classical statistical methods (maximum likelihood estimates and confidence intervals), Bayesian methods, tests for homogeneity of the data for deciding whether to pool the data or not, Empirical Bayes methods, and methods for trending the reliability parameters over time.

4.2 Generic Data Sources

Several generic data sources currently available and used throughout the nuclear power PRA industry are identified in this section. Several of these data bases are discussed with regard to their attributes, strengths, and weaknesses. Data bases for both initiating events and component failure rates are included. Some data sources represent compilations of raw data which have been collected directly from various facilities and processed and statistically analyzed. Other data sources utilize the results of the statistical analyzes of other data bases to derive estimates for component probabilities.

Section 4.2.1 contains discussions and summaries of generic data bases sponsored by the NRC for use in both government and industry PRAs. Section 4.2.2 contains discussions and summaries of generic data bases sponsored by the Department of Energy (DOE) for use in PRAs. Section 4.2.3 contains discussions and summaries of generic data bases developed by nuclear power industry related organizations. Section 4.2.4 contains a summary of a foreign data base, the Swedish T-book. Section 4.2.5 contains a discussion of several non-nuclear data bases which could be useful for some data issues in nuclear power PRA. Section 4.2.6 describes a process for selecting a generic data value from these sources.

4.2.1 NRC-Sponsored Generic Data Bases

The discussion of NRC-sponsored generic data bases is presented in two sections. The first discusses current data bases. These data sources are deemed appropriate for current and future use. The second section briefly summarizes some historical data bases that have been used or referenced in past analyses. **While useful at the time, these data bases are no longer considered appropriate sources of information.**

4.2.1.1 Current Data Bases

Current NRC-sponsored data bases are discussed in the following subsections. Major attributes for each data base are identified, and limitations associated with each data base are provided.

As a reminder, these data bases are considered to be appropriate sources of information for use in PRAs or other risk assessments. However, it is the user's responsibility to ensure that any information from these data bases used in their analysis is appropriate for their analysis.

4.2.1.1.1 Severe Accident Risks Study Generic Data Base (NUREG-1150)

The generic data base developed for the NRC's Severe Accident Risks study (NUREG-1150) (NRC 1990) is documented in NUREG/CR-4550 as supporting documentation (Drouin et al. 1990). This data base was developed from a broad base of information, including:

- WASH 1400 (NRC 1975b),
- the IREP data base (Carlson et al. 1983),
- Zion (ComEd 1981), Limerick (PECO 1982), Big Rock Point (CPC 1981), and the Reactor Safety Study Methodology Application Program (RSSMAP) PRAs (Hatch et al. 1981),
- NRC LER summaries (Hubble and Miller 1980, Appendices O through Y), and
- the NRC's Station Blackout Accident Analysis (Kolaczkowski and Payne 1983).

Component failure probabilities, failure rates, and initiating event frequencies typically modeled in the NUREG-1150 plant analyses are included in the data base. A mean value and an error factor on a log normal distribution are provided for each entry into the data base.

Limitations in the Data Available from NUREG-1150

The basis of the NUREG-1150 data base is from a broad group of prior PRA analyses and generic data bases. Thus, it does not directly represent the results of the analysis of actual operational data. Furthermore, the data upon which those previous analyses are based suffer from limitations similar to those for older NRC data sources and the NPRDS data base (Sections 4.2.1.2 and 4.2.3.1).

4.2.1.1.2 Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 - 1996

The report *Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980 - 1996*, NUREG/CR-5496 (Atwood et al. 1998), presents an analysis of loss of offsite power (LOSP) initiating event frequency and recovery times for power and shutdown operations at commercial nuclear power plants. The evaluation is based on LERs for events that occurred during 1980 through 1996. The primary objective of the study was to provide mean and uncertainty information for LOSP initiating event frequencies and recovery times. A secondary objective was to re-examine engineering insights from NUREG-1032 (a LOSP study covering the years 1968 through 1985) using the more recent data.

The major findings of the report are:

- Not all LOSP events that occur at power result in a plant trip.
- Plant-centered events clearly dominate the LOSP frequency during both power and non-power operational modes.
- Plant-centered LOSP frequency is significantly higher during shutdown modes than during power operation.
- No statistically significant variation among units was found for plant-centered sustained initiating events.
- During shutdown, statistically significant variation among plants was found for plant-centered sustained initiating events.
- Equipment faults were the main contributor (58%) to plant-centered LOSP initiating events that occurred during power operations. Human error accounted for a smaller contribution (23%).
- During shutdown conditions, human error was the dominant contributor (58%).
- A clear downward trend can be seen for the plant-centered initiating event frequency.
- Grid-related LOSP frequency is small.
- For severe weather, statistically significant site-to-site variability exists for sustained shutdown LOSP frequencies.
- Severe weather events had significantly longer sustained recovery times.
- For sustained recovery times, no pattern was found correlating unit design class with longer recovery times.
- Longer recovery times were observed for sustained plant-centered LOSP events that did not result in a plant trip or that occurred during shutdown.

Nominal frequencies and upper and lower bounds are given in the report.

Limitations in the Data Available from NUREG/CR-5496

The generic data base developed in this NRC-sponsored data study is based on raw data from LERs. LERs constitute data involving only reportable events at nuclear power plants, and the degree of detail provided in the LERs varies. Some information needed in the data analysis had to be estimated (e.g., allocation of 1980 time into critical and shutdown time), and the analysis ended with events that occurred in 1996. Thus, the data base does not contain events that occurred after 1996, and may not be representative of actual current operational experience.

4.2.1.1.3 Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995

The report *Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995*, NUREG/CR-5750 (Poloski et al. 1999a), presents an analysis of initiating event frequencies at domestic nuclear power plants. The evaluation is based primarily on the operational experience from 1987 through 1995 as reported in LERs. The objectives of the study were to:

- provide revised frequencies for initiation events in domestic nuclear plants,
- compare these estimates to estimates used in PRAs and Individual Plant Evaluations (IPEs), and
- determine trends and patterns of plant performance.

Major findings of the report are:

- Combined initiating event frequencies for all initiators from 1987 through 1995 are lower than the frequencies used in NUREG-1150 (NRC 1990) and industry IPEs by a factor of five and four, respectively.
- General transients constitute 77% of all initiating events, while events that pose a more severe challenge to mitigation systems constitute 23%.
- Over the time period of the study, either a decreasing or constant time trend was observed for all categories of events.
- Loss of coolant accident (LOCA) frequencies are lower than those used in NUREG-1150 and industry IPEs.

Nominal frequencies and upper and lower bounds are given in the report.

Limitations in the Data Available from NUREG/CR-5750

The generic data base developed in this NRC-sponsored data study is primarily based on raw LER data from 1987 through 1995. For some events (e.g., LOCAs) information from additional operating experience, both domestic and foreign, was used with other sources of information (e.g., engineering analyses) to estimate the initiating event frequencies. Since the analysis ended with events that occurred in 1995 and made use of other sources of information, the data base may not be representative of actual current operational experience.

4.2.1.1.4 System Reliability Studies

A series of system reliability studies, documented in the multi-volume NUREG/CR-5500 report,[1] presents an analysis of system unreliability for various systems.[2] The following volumes comprise the systems that will be studied::

- Volume 1: auxiliary/emergency feedwater system (Poloski et al. 1998),
- Volume 2: Westinghouse reactor protection system (Eide et al. 1999a),
- Volume 3: General Electric reactor protection system (Eide et al. 1999b),
- Volume 4: high-pressure coolant injection system (Grant et al. 1999a),
- Volume 5: emergency diesel generator power system (Grant et al. 1999b),
- Volume 6: isolation condenser system (Grant et al. 1999c),
- Volume 7: reactor core isolation cooling system (Poloski et al. 1999b),
- Volume 8: high-pressure core spray system (Poloski et al. 1999c),
- Volume 9: high pressure safety injection system (Poloski et al. 2000),
- Volume 10: CE reactor protection system (Wierman et al. 2002a), and
- Volume 11: B&W reactor protection system (Wierman et al. 2002b).

With the exception of the reactor protection system volumes, the analyses of the other systems are based on information obtained from LERs. For the reactor protection system volumes, the analyses are based on information obtained from NPRDS and LERs.

The analyses: (1) estimate the system unreliability based on operating experience, (2) compare the estimates with estimates using data from PRAs and IPEs, (3) determine trends and patterns in the data, and (4) provide insights into the failures and failure mechanisms associated with the system.

[1] Currently, it is expected that some of these reports will be updated with new information.

[2] Train, subsystem or system data can be combined with basic event failure data to obtain improved estimates of component failure rates. A Bayesian method for doing this is described in Martz and Almond 1997.

Unreliability estimates (means and distributions) are provided for the entire system for each plant. In addition, unreliability estimates for major train segments failure modes (e.g., failure to start – pump, driver, valves, and associated piping) are provided. Common cause failure estimates are also provided.

Limitations in the Data Available from NUREG/CR-5500

The information available from this NRC-sponsored data study is based on that available from LERs and NPRDS. LERs constitute data only involving reportable events at nuclear power plants, and the degree of detail provided in the LERs varies. The limitations associated with NPRDS are provided in Section 4.2.3.1. The information used in the studies spans various time frames, with the most up-to-date information coming from 1997. Thus, the results of the studies may not be representative of actual current operational experience.

4.2.1.1.5 Component Performance Studies

A series of component performance studies, documented in the multi-volume NUREG-1715 report, presents an analysis of component performance for various components. The following volumes comprise the components that have been studied:

- Volume 1: turbine-driven pumps (Houghton and Hamzehee 2000a),
- Volume 2: motor-driven pumps (Houghton and Hamzehee 2000b),
- Volume 3: air-operated valves (Houghton 2001a), and
- Volume 4: motor-operated valves (Houghton 2001b).

The analyses are based on information obtained from NPRDS and LERs. The data included in the studies cover the period 1987 through 1995.

The analyses: (1) estimate the system-dependent unreliability of selected components, (2) compare the estimates with estimates from PRAs and IPEs, (3) determine trends and patterns in the data, and (4) provide insights into component performance, including component failure mechanisms.

System-dependent unreliability estimates (means and distributions) for various failure mechanisms are provided for each component. Trends in component failure rates were also evaluated in these studies.

Limitations in the Data Available from NUREG-1715

The information available from this NRC-sponsored data study is based on that available from LERs and NPRDS. LERs constitute data only involving reportable events at nuclear power plants, and the degree of detail provided in the LERs varies. The limitations associated with NPRDS are provided in Section 4.2.3.1. The information used in the studies spans various time frames, with the most up-to-date information coming from 1998. Thus, the results of the studies may not be representative of actual current operational experience.

4.2.1.2 Historical Data Bases

In the past, NRC sponsored several programs to develop data bases on nuclear power plant component reliability and initiating event frequencies. These programs included:

- In-Plant Reliability Data Base for Nuclear Power Plant Components (IPRDS) (Drago et al. 1982) – established at Oak Ridge National Laboratory to establish methods for data collection and analysis.
- Nuclear Reliability Evaluation Program (NREP) – generic data base developed to support the Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815 (Papazoglou et al. 1984).
- Interim Reliability Evaluation Program (IREP) Generic Data Base – developed to support the performance of five PRAs in the 1980s and documented in the IREP procedures guide (Carlson et al. 1983).
- Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) – developed as a repository of human error and hardware failure information that could be used to support a variety of analytical techniques for assessing risk. NUCLARR was documented in five volumes as NUREG/CR-4639 (Gertman et al. 1990).

Major attributes for each program and the resulting data bases are documented in the cited references.

4.2.2 DOE-Sponsored Generic Data Bases

Several data bases have been developed to support DOE-sponsored projects. Two of these data bases are discussed in the following sections.

4.2.2.1 Component External Leakage and Rupture Frequency Estimates

Estimates of external leakage and rupture frequencies for components such as piping, valves, pumps, and flanges are necessary for detailed risk analysis of internal flooding. These estimates have been developed and documented in EGG-SSRE-9639 (Eide et al. 1991). The estimates are based on an analysis of data gathered from a comprehensive search of LERs contained in Nuclear Power Experience (NPE) (Hagler-Bailly 1972).

The NPE data base was searched for data covering the period September 1960 through June 1990. The external leakage and rupture events collected from the data were converted to component leakage and rupture frequencies in a three-step process:

1. The ratios of external rupture events to external leakage and rupture events were examined for various components by size and system to decide how to group the data.
2. The final probabilities of an external rupture, given an external leakage or rupture event, were determined.
3. Lastly, the external leakage and rupture frequencies were obtained by estimating component populations and exposure times.

Limitations in the Data Available from EGG-SSRE-9639

The generic data base developed in this DOE-sponsored data study is based on raw LER data from 1960 through 1990. LERs constitute data only involving reportable events at nuclear power plants, and the degree of detail provided in the LERs varies. Since the analysis ended with events that occurred in 1990, the data base may not be representative of actual current operational experience.

4.2.2.2 Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs

A generic component failure data base was developed by the Idaho National Engineering Laboratory (INEL) for light water and liquid sodium reactor PRAs. This data base is documented in EGG-SSRE-8875 (Eide et al. 1990). The intent of this project was to base the component failure rates on available plant data as much as possible rather than on estimates or data from other types of facilities. The NUCLARR data base and the Centralized Reliability Data Organization (CREDO) (Manning et al. 1986) were used as the primary sources of component failure data. If specific components and failure modes were not covered in those two sources, then other standard sources such as IEEE STD-500 (IEEE 1983) (for electrical components) and WASH-1400 (NRC 1975b) were used. The data base is organized into four categories according to the working fluid of the component:

- mechanical components (water or steam),
- mechanical components (liquid sodium),
- mechanical components (air or gas), and
- electrical components.

Limitations in the Data Available from EGG-SSRE-8875

The generic data base developed in this DOE-sponsored data study is based on information from multiple sources. Since the analysis ended with events that occurred in 1990, the data base may not be representative of actual current operational experience.

4.2.3 Industry Data Bases

Several data bases developed within the nuclear power industry for both risk assessment and for plant operations are summarized here. Data bases discussed in this section were developed by the Electric Power Research Institute (EPRI) and the consulting firms of EQE, International and Science Applications International Corporation (SAIC).

Although the NPRDS and EPIX data bases (described in Section 4.1.3) contain plant-specific data, they can be used to generate generic failure rates for components. Methods for aggregating individual plant data to estimate failure rates are described in Section 8.2 of this handbook. Aggregation of data from EPIX can be performed using the RADS software developed under the NRC auspice.

4.2.3.1 EQE, International

The EQE, International generic data base (formerly known as the Pickard, Lowe, and Garrick or PLG data base) for light water reactors is set up to support PRA and reliability analysis for which both point estimates

and uncertainty distributions are developed.[3] The data base contains information on:

- Component failure rates,
- Common cause failures,
- Component maintenance frequencies and mean durations,
- Initiating events,
- Fire and flood events at nuclear sites, and
- Shutdown events involving loss of residual heat removal (RHR) cooling and loss of inventory.

The fire, flood, and shutdown events are a compendium of experience event summaries from all U.S. nuclear sites. The common cause data are presented as event description and have been classified according to the methodology of NUREG/CR-4780 (Mosleh et al. 1989). The fire, flood, shutdown and common cause events have, in addition to the description, information in various fields making them convenient for sorting and for use in plant-specific screening analysis.

All other data are in the form of distributions and are compatible with the PLG risk assessment software, RISKMAN® . These distributions are generated using the data analysis module of RISKMAN® which can be used as a stand-alone software. The distributions developed are available to the other modules of RISKMAN® used for fault-tree quantification and core damage sequence quantification.

The actuarial data are from over 20 nuclear sites in the U.S. and in Europe. Other sources of generic information also used are:

- EPRI reports on components, shutdown accident events, initiating events, loss of offsite power;
- Special NUREG reports on components such as pumps, valves, diesel/generators;
- Compiled data bases such as Nuclear Power Experience, NUCLARR, IEEE-500 (IEEE 1983), NPRDS, etc.; and
- Insurance company databases for loss events.

The database includes statistics for components that cover population, demands, operating times, failures, and maintenance outages and durations at specific plants. It also includes event-by-event analyses for initiating events, common cause failures, and fires and floods over the whole U.S. plant population. In addition to this factual information, parameter estimates from published sources of generic reliability data are also provided.

The actuarial data and the other generic data are combined using a two-stage Bayesian updating technique. The generic distributions maintain what is referred to as plant-to-plant variability. Since the data are developed specifically to be used for Monte Carlo sampling, they are defined with a minimum of 20 discrete bins with special attention given to the tails of the distributions.

The database is available in a format compatible with RISKMAN® and also as ASCII files.

Limitations in the Data Available from EQE, International

The EQE data base is proprietary, so the adequacy and comprehensiveness of the underlying data have not been evaluated for this document. As noted above, several of the sources of generic information incorporated into the data base are discussed previously in this chapter (e.g., NUCLARR, NPRDS); thus, it is possible that some of the data from the EQE data base may have limitations similar to other data bases discussed in this chapter. However, it should be noted that the proprietary nature of the EQE data base precludes any definitive judgment as to how data bases such as NUCLARR and NPRDS were utilized in the development of the EQE database.

4.2.3.2 Science Applications International Corporation

Science Applications International Corporation (SAIC) has developed a generic, proprietary data base for application to PRAs on commercial nuclear power plants.[4]

The scope of the data base for components and their failure modes was established by a review and tabulation of all basic events and component failures in SAIC-conducted PRAs. Components were grouped

[3] The information on the EQE/PLG data base is based on personal correspondence from Shabha Rao, PLG, Newport Beach, California, to Timothy Wheeler, Sandia National Laboratories, September 16, 1999, and to Donnie Whitehead, Sandia National Laboratories, April 4, 2001.

[4] The information on the SAIC data base is based on a personal correspondence from Alan Kolaczkowski, Vice President, SAIC, to Donnie Whitehead, Sandia National Laboratories, April 18, 2001.

into generic categories rather than specifically by system or application. Thus, all basic events for motor-driven pumps were categorized into a single "motor-driven-pump" category rather than delineated size or by system. Some component failure modes were merged to reflect the available data (e.g., air-operated valves fail-to-open and fail-to-close were combined into a single failure mode – fail-to-operate. Component boundary definitions are given for all components in the SAIC generic data base.

The data base was developed by collecting all sources of available parameter estimates relevant to the component failures defined by the scoping process. Each data source was evaluated against a set of acceptance criteria, including availability (no proprietary sources were included), compatibility of data to being fit to a lognormal distribution, and Bayesian updating. Any source which used Bayesian parameter estimation methods to develop estimates for component failure modes was rejected. Such data sources were considered to be too plant-specific for inclusion into a generic data base.

Each individual data source selected against the acceptance criteria was fitted to a lognormal distribution. Then, all data sources for each particular component failure were aggregated through a weighted sum approach (each source was weighted equally). Each aggregated distribution was fitted to a lognormal distribution.

Limitations in the Data Available from the SAIC Data Base

The SAIC data base is proprietary, so the adequacy and comprehensiveness of the underlying data have not been evaluated for this document.

4.2.3.3 Advanced Light Water Reactor Data Base

EPRI's Advanced Light Water Reactor (ALWR) Utility Requirements Document (EPRI 1989) contains a reliability data base for use in ALWR PRAs. Several data sources were reviewed and representative failure rates and event probabilities were compiled from these data sources. A best estimate value was selected for each component type and failure mode based on judgment regarding the applicability of the data source to the expected ALWR design. The primary sources used in the data survey were the Oconee PRA (Duke 1984), the Seabrook Probabilistic Safety Study (PLG 1983), parameter estimates from licensee-event reports documented in NUREG/CR-1363 (Battle 1983) for valves, NUREG/CR-1205 (Trojovsky 1982) for pumps, and NUREG/CR-1362 for diesel generators (Poloski and Sullivan 1980).

Limitations in the Data Available from the ALWR Data Base

The ALWR data base lists only best estimates for each initiating event, failure rate, and event probability. The survey is well documented in that all estimates collected for each parameter estimate are shown. However, only a cursory statement of rationale for deriving the best estimate value is given. No uncertainty bounds or probability density functions are given.

4.2.4 Foreign Sources

Two sources of data from Nordic nuclear power plants are available. The I-Book documents initiating event frequency data and the T-Book documents component failure data.

4.2.4.1 Sweden's T-Book for Nordic Nuclear Power Plants

Since the early 1980s a Reliability Data Handbook, the T-Book (ATV 1992), has been developed and used for nuclear power plant of Swedish design. The T-Book provides failure data for the calculation of component reliability for use in regulatory safety analyses of Nordic nuclear power plants. The 3rd edition is based on operation statistics from 12 Swedish and 2 Finnish nuclear power plants, including approximately 110 reactor years of experience.

The failure characteristics incorporated into the parameter estimations in the T-Book are based on Licensee Event Reports for Nordic plants delivered to the Swedish Nuclear Power Inspectorate (SKi) and from failure reports in ATV's central data base. Only critical failures, those that actually caused a component's function to stop or fail, are incorporated into the parameter estimations. A multistage empirical Bayesian approach is used to develop the component parameter estimates from the raw data (Pörn 1996).

Limitations in the Data Available from the T-Book

Data for the T-Book are collected from LERs delivered to the SKi; thus, the parameter estimates derived from the data are based only on data of reportable incidents. It is not understood how representative such data may be of actual operational experience.

4.2.4.2 Sweden's I-Book for Nordic Nuclear Power Plants

The I-Book (Pörn et al. 1994) contains a compilation of initiating events that have occurred in Nordic nuclear power plants. The data reflects 215 reactor years of operating experience prior to 1994. In the first edition of the I-Book, issued in 1993 (Pörn et al. 1993), initiating event groups were identified and frequencies generated. The operating experience from two additional plants in Finland were included in the second edition (Pörn et al. 1994).

The I-Book includes the development of a statistical model for performing a trend analysis. The model is based on nonhomogeneous Poisson (Power Law) processes and includes a complete treatment of parametric uncertainty using Bayesian methods.

Limitations in the Data Available from the I-Book

Data for the I-Book are collected from operating experience at Nordic plants. It is not understood how representative such data may be of operational experience in nuclear power plants in the United States.

4.2.5 Non-Nuclear Power Data Bases

There are many non-nuclear data bases that contain failure data that can potentially be used in nuclear power plant PRAs. Several of these data bases are described below. When using data from non-commercial nuclear sources, care must be taken to ensure that the data are for components and conditions representative of those that exist in nuclear power plants.

4.2.5.1 Reliability Analysis Center

The Reliability Analysis Center (RAC) in Rome, New York, maintains two data bases on electronic and non-electronic component reliability. The data bases are:

- Electronic Parts Reliability Data (Denson et al. 1996), and
- Non-Electronic Parts Reliability Data (Denson et al. 1995).

These RAC databases provide empirical field failure rate data on a wide range of electronic components and electrical, mechanical, and electro-mechanical parts and assemblies. The failure rate data contained in these documents represent cumulative compilation from the early 1970s up to the publication year for each document. Data are collected from sources such as:

- published reports and papers,
- government-sponsored studies,
- military maintenance data collection systems,
- commercial/industrial maintenance databases, and
- direct submittals to the RAC from military or commercial organizations that maintain failure data bases.

Limitations in the Data Available from the RAC Handbooks

The RAC handbooks provide point estimate parameter estimations for failure rates (or demand probabilities). No treatment of uncertainty is provided.

4.2.5.2 Offshore Reliability Data Project

The Offshore Reliability Data (OREDA) project has collected and processed data from offshore oil platforms operated by 10 different companies off the coasts of the U.K., Italy, and Norway. Reliability data collected and processed by OREDA has been published in the Offshore Reliability Data Handbook (OREDA 1997). The main objective of OREDA is to collect reliability data for safety important equipment in the offshore oil industry.

Components and systems for which data are collected are:

- Machinery
  - Compressors
  - Gas turbines
  - Pumps
- Electric generators
- Mechanical Equipment
  - Heat exchangers
  - Vessels
- Control and Safety Equipment
  - Control Logic Units
  - Fire and Gas Detectors
  - Process sensors
- Valves
- Subsea Equipment
  - Control Systems
  - Well completions

Data have been collected from 7,629 individual equipment units (e.g., individual pumps, valves, motors) over a total observation period of 22,373 years. The records include 11,154 failures.

Under each category of equipment (e.g., machinery) information is collected on each type of component (e.g., centrifugal compressors). Data are further sorted by a component's driving mechanism (e.g., electric motor-driven), by failure mode (e.g., fails-to-start, fails-while-running), and by the criticality of each failure (e.g., critical - terminates the operation of the component, degraded - component still operates).

The OREDA-97 handbook presents failure rate and demand failure probability estimates for various combinations of component function, application, capacity, operating fluid, and size.

Limitations in the Data Available from the OREDA Data Base

Certain data quality issues have arisen in the development of OREDA (Sandtorv et al. 1996). The quality and availability of data can vary significantly among the 10 participating companies. Interpretations of equipment definitions and failure mode specifications can vary among the participants as well, affecting the quality of data. The effect of preventive maintenance on equipment reliability is difficult to measure. Since preventive maintenance practices vary among the participating companies it is unclear as to what would be the baseline rate of a generic type of equipment.

4.2.5.3 IEEE-500 Standard

The Institute of Electrical and Electronics Engineers (IEEE), Inc. Standard 500-1984 (IEEE 1983) contains failure estimates for various electrical, electronic, sensing, and mechanical components. Delphi procedures (an elicitation process) were used in producing component failure estimates. Multiple sources of information, including nuclear, fossil fuel, and industrial, were considered by the experts as part of the Delphi process.

Limitations in the IEEE-500 Data Base

The major limitations associated with the IEEE-500 data base are (1) the data base contains dated material (i.e., the latest information used to develop the data base comes from the early 1980s), and (2) the process used to support development of the failure estimates was an uncontrolled process. (A survey was sent to various individuals requesting them to provide information on selected issues. No inherent controls were placed on the individuals, and no training on how to estimate failure probabilities was provided to the individuals filling out the survey forms.) In addition, it should be noted that IEEE Standard 500-1984 has been withdrawn and is no longer available from IEEE.

4.2.6 Selection of Parameter Estimates from Existing Data Bases

The need to select parameter estimates from existing generic data bases may arise when performing a PRA. This can occur when a PRA is being performed on a new plant that has no operating history or it may occur when no plant-specific information exists for a specific component. Whatever the reason, when it becomes necessary to select parameter estimates from generic data bases, certain cautions should be observed:

1. The generic data base should contain failure probability estimates for components that are identical or comparable to the ones in the PRA model in terms of size, component boundary definition, intended operational history (e.g., normally operating versus standby), and expected or postulated operating environment.

2. The generic data base should contain a recommended point estimate and an uncertainty distribution for each identified failure.

3. If possible, the primary sources of information used to develop the generic data base's failure probabilities and distributions should be information from other nuclear power plants. Supplemental information from non-nuclear sources should be used only when necessary to provide failure probabilities and distributions for components that cannot be obtained from nuclear power plant generic data sources.

4. Where possible, the generic data base's failure probabilities and distributions should be derived from actual failure events. If such information is not available, then failure probabilities and distributions generated by other techniques (e.g., expert elicitation) are acceptable.

5. Generic data base failure probabilities and distributions should reflect current trends. If significant trends exist within the failure data indicating either an increase or decrease in the failure probabilities, the underlying event failure information used to generate the failure probabilities should represent these recent events.

However, if no significant trends exist, then data from all years can be used to estimate the failure probabilities.

6. The failure probability estimates contained within the generic data base should not be based on incestuous sources, i.e., the estimates should not be derived from two different sources that employed similar or different analysis techniques to the same ultimate set of failure information.

5. PLANT-SPECIFIC DATA COLLECTION AND INTERPRETATION

The incorporation of plant-specific data in the parameter estimates used in a PRA produces risk estimates that reflect the actual plant experience. A plant-specific data analysis also allows comparison of plant equipment performance relative to an industry average (the generic value). A plant-specific data analysis will identify those components or systems whose performance is worse than the industry average. It may also identify components or systems with better-than-average performance.

As indicated in Chapter 4, the raw failure data needed for a plant-specific data analysis is dependent upon the scope the analysis. The scope can include accident initiating events, component failure events and unavailablilities due to maintenance or testing, and recovery events. Typical sources of raw data available at nuclear power plants for each of these type of events are identified in Section 4.1. The information needed may have to come from multiple sources.

Interpretation and reduction of the raw data is required to obtain the reduced data used in the parameter estimation models described in Chapters 2 and 6. The reduction of the raw data includes consideration of issues such as pooling of identical component data, the mode of operation the plant was in when a failure occurred, and the severity of the event. Additional issues concerning data reduction, such as aging and time impacts, are addressed in Chapter 7.

This chapter describes a process for collecting and reducing raw data for the purpose of generating plant-specific data for use in a PRA. Because nuclear power plants collect and record raw data in different ways, the process described is general in nature but, sufficient to successfully collect and reduce available date for use in a PRA. Some practical concerns and issues related to the scope and performance of plant-specific data analysis are also presented.

A process for reducing the data necessary to calculate initiating event frequencies, component failure data, and recovery event data are presented in Sections 5.1, 5.2, and 5.3, respectively. The reduced data obtained in this process are combined according to the guidance provided in Chapters 2 and 6 to obtain the parameters necessary to quantify PRA models.

5.1 Initiating Event Data

The methods for evaluating plant-specific initiating event frequencies provided in Chapter 6 require the number of initiating events of interest and the time period over which these events occurred. Guidance is provided in this section for collecting and interpreting this required data.

5.1.1 Initiating Event Categories

The initiating events of interest in nuclear power plant PRAs are dependent upon the mode of operation that the plant is in. For power operation, the events of interest are generally reactor scrams but can also include unplanned forced shutdowns. Typical initiating events during power operation include multiple categories of plant transients and loss-of-coolant accidents (LOCAs). Trips from zero power or low power may be excluded as valid initiating events in a full power PRA if their occurrence is precluded during full power operation. However, low power events should be considered as valid initiating events at full power if they can occur during full power. For shutdown modes of operation, the reactor is already subcritical and thus the events of interest are somewhat different. Typical initiating events modeled in shutdown PRAs include loss of decay heat removal events, reactivity insertion events, and LOCAs or drain-down events.

It is a standard practice in PRAs to group initiating events into categories based on their impact on certain plant systems, and according to the demands they make on other plant systems needed for accident mitigation. Examples of typical initiating event categories include loss of offsite power, loss of feedwater, main steam isolation valve (MSIV) closure, and large, medium, and small LOCAs. Lists of typical transients that have occurred at nuclear power plants while at full power have been categorized by EPRI (1982) and the INEEL (Mackowiak et al. 1985 and Poloski et al. 1999a). Typical initiating events to consider during low power and shutdown conditions have also been established for both boiling water reactors (BWRs) (Staple et al. 1999) and pressurized water reactors (PWRs) (Chu et al. 1993).

5.1.2 Data Window

The time period for collecting initiating event data should be as broad as possible. In general, data from all of the years of plant operation should be considered. However, screening of the data can be performed to eliminate unrepresentative events (see the next section). One screening technique used in general practice is to eliminate the first year of operational data as unrepresentative.

Since the number of plant events can decrease over time due to improvements in the design and operation of the plant, it is desirable to have the data reflect the most recent operating experience. This can be accomplished by considering only the data from the most recent years of operation. Alternatively, an analyst could perform a trend analysis of the data (see Chapter 7).

5.1.3 Initiating Event Data Allocation and Screening

To allocate plant-specific event data to the initiating event categories modeled in the plant PRA, it is necessary to establish the status of the plant, including its power level at the time of the event and the impact of the event on the plant systems. Such information is generally available in the raw data sources discussed in Section 4.1 that are available to identify initiating events (i.e., LERs, scram reports, and monthly operating reports).

For initiating events during power operation, the events of concern are those that result in a reactor trip or forced shutdown. To allocate these events to the appropriate initiating event category, a data analyst must examine the sequence of events prior to and immediately following the reactor trip/shutdown. The initial plant fault leading to a sequence of events that eventually result in an automatic or manul reactor trip or unplanned shutdown is used in categorizing the event. For example, one plant trip may have been initiated by spurious closure of the MSIVs and be identified as an MSIV closure transient. Another event may be initiated by a loss of condenser vacuum which produces a closure of the MSIVs. This event may also be placed in the MSIV closure transient category, unless some significant difference in the plant response is identified.

The initiating event data analysis can also be used to help establish the conditional probability of events subsequent to the event actually leading to the plant trip. Examples of this include the failure of the reactor protection system leading to an anticipated transient without scram (ATWS), and the occurrence of a relief valve sticking open leading to a transient-induced LOCA.

It is possible that some events leading to plant scrams (or loss of heat removal during a shutdown mode of operation) can be eliminated from the data analysis. One acceptable reason for eliminating initiating event data involves design or operational changes that may have been made to reduce the frequency of reactor scrams. Such changes to the plant design or operation can eliminate the occurrence of failures that have occurred in the past. For example, a plant may have experienced a significant number of loss of feedwater events due to the design of the feedwater control system. As a result, a utility may have replaced the feedwater controller with a new, more reliable design that eliminated the occurrence of loss of feedwater due to controller faults. The data analyst can thus eliminate past events initiated by faults in the old feedwater controller from consideration.

Changes in the plant design or operation can also affect the classification of events. The following example, provided in EPRI TR-100381 (EPRI 1992), illustrates this point. The MSIV vessel level closure set point at some BWRs has been lowered from Level 2 to Level 1. As a result, the fraction of initiating events that lead to MSIV closure may be different before and after the design change implementation and the total historical count of MSIV closure events may not be valid for the current condition of the plant. One approach for dealing with such a design change is to eliminate all events prior to the design change that result in MSIV closure due to the generation of a low vessel level. This approach has the undesirable impact of reducing the sample size. An alternative is to review the past events to determine if the MSIVs would have closed with the revised closure set point in place. However, this may be difficult to determine from the available information.

5.1.4 Selection of Exposure Time

For estimating the frequencies of initiating events that occur during any plant operating mode, the appropriate exposure time is the number of calendar years of operation corresponding to the period of time the initiating event data is collected. Expressing the frequency of initiating events on a calender year basis allows for evaluation of risk in each mode on a consistent and average basis.

However, it may be necessary to generate the initiating event frequencies based on the time the plant is in the particular mode of operation. For example, initiating events during power operation are often expressed in terms of events per critical year (one critical year represents 8760 hours of reactor criticality). Since generic initiating event frequencies are often expressed in events per critical year (Poloski 1999a), calculation of the plant-specific frequencies in this same unit is required for combining the two values using Bayesian techniques (see Section 6.2.2). To determine at-power initiating event frequencies, the plant-specific frequencies expressed as events per calender year have

to be increased by dividing by the fraction of time the plant was at power. This fraction is called the **criticality factor** and may be determined from the control room logs or the Grey Books where the residence times in each of the operational modes are recorded. Criticality factors for each plant are provided in Appendix H of NUREG/CR-5750 (Poloski 1999a) for the years 1987 through 1995. Alternatively, the generic frequencies may be divided by the average criticality factor (0.75 for the data reported in NUREG/CR-5750) to obtain generic data expressed in the same units as the plant-specific data (i.e., events per calender year. For example, suppose an event is expected to occur 1.6 times every calender year, on average, and that the criticality factor for a specific plant is 0.8 (i.e., the reactor has been critical 80% of the time). Then, the same event correlated to units of critical years is 2 events per critical year (1.6 events/calender year divided by 0.8 critical years/calender year).

5.2 Component Failure Data

The raw data sources containing equipment operating records in a nuclear power plant typically document tens of thousands of component malfunctions over the plant's lifetime. The records may be kept in various forms including hard copies of maintenance work orders or a computerized file. The most useful raw data sources provide information on the specific component affected, the observed problem, and the action taken. To calculate plant-specific component failure rates and unavailability from the data in these records, the data analyst must identify those malfunctions that cause component functional failures and also determine the corresponding number of demands or operating time. This section describes this process and some of the practical concerns required to extract the necessary data.

5.2.1 Component Data Identification

The first step in evaluating plant-specific component failure rates is to identify the components and their failure modes that will be analyzed. This step is usually done in coordination with other PRA analysts (typically those analysts that generate system models such as fault trees). This coordination is critical because it focuses the component data analysis on only those components and their failure modes that appear in the PRA models and establishes the definitions of the component boundaries.

It should be noted that extremely reliable components may never have failed in the history of the plant. This lack of failure history makes it difficult to estimate the true failure rate or probability. Reliable components can generally be identified by reviewing failure rates in generic data bases. However, the analyst is cautioned in the use of this data since a usually reliable component may not be reliable at a particular plant. In addition, it is often impossible to identify the number of demands or run times for certain components (for example, the number of demands placed on a relay) using the existing plant records.

5.2.1.1 Data Window

Plant-specific data is selected over a sufficient time period to provide statistically meaningful results. Use of data from throughout the plant history is preferred since they will be less subject to random variability. The following examples from EPRI TR-100381 (EPRI 1992) illustrates the amount of data required to achieve an acceptable sample size.

> "With no failures, the statistical significance can be measured by the 95th upper confidence limit. To establish a 95th confidence limit on a failure rate of 1E-3/hr, the required cumulative run time for the population is 3,000 hours, to establish a 95th confidence limit of 1E-4/hr requires 30,000 hours. Thus, if a failure rate is believed from generic data to be relatively low, one should expect to have to collect a significant amount of run time before making an impact on the generic values.
>
> "When failures are recorded the statistical significance can be measured by the range from the 5th to the 95th percentile confidence bounds. This decreases with the number of failures. For a Poisson distribution, the range from the 5th to the 95th percentile is on the order of 10, with 2 failures. Thus, for greater than 2 failures the sample is very loosely comparable to the lognormal with an error factor of 3. Thus, for a population of components, a total number of failures of 2 or more is a reasonable sample when compared with typical generic data bases. This is true for the binomial distribution also, as it approximates the Poisson distribution when the parameter, p, is on the order of 10^{-3}. These considerations can be used to establish a reasonable time frame for data collection. Suppose, the generic data is on the order of 10^{-3} per demand, and there are four components in

the population with approximately one demand per component per month per ISI tests. To get 2 failures, we would expect to require about $2/p$ demands, or 2,000 demands. There are 48 demands per year, therefore data from 41 years would be required to produce this statistically meaningful data. This illustrates the importance of making sure that all the demands are counted and also of increasing the size of the population if at all possible."

5.2.1.2 Data Collection

For the list of components and their failure modes selected for data analysis, the system analyst must retrieve all failure, maintenance, and test records for each component from the raw data sources generated during the data window. The required records are generally obtained based on the component identification number. Because the component boundary can include multiple piece parts, the required records may be kept under multiple identification numbers. However, for some components, the data records for the different piece parts may all be kept under the same identification number. Thus, it is necessary to list the identification numbers for all the piece parts included in the component boundary definition.

Because component failures are generally infrequent, it is preferable to pool the data from several components to obtain a larger data base. For example, it is common to group like pumps within a single system into one population, but less common to group the pumps of different systems (although it can be acceptable to group pumps of different systems with similar characteristics together into one population). Any grouping of components requires careful consideration of the similarity of their design (e.g., size or manufacturer), the frequency of operation, their environmental operating conditions (e.g., temperature, humidity, and radiation), operating modes (e.g., standby versus normally operating or intermittently operating), and the medium they carry (e.g., air, pure water, or borated water). Tests for poolability of data are described in Chapter 6.

5.2.2 Event Screening and Severity Classification

The raw data for a specific component will contain some events that are not relevant to the component failure modes being analyzed. These events can be screened from further analysis. Some of the events will be component failures that should be included in the data assessment. The type of component failures will determine how they are classified and subsequently used to generate the required component failure data. Guidance for both event screening and classification is provided below.

5.2.2.1 Event Screening

One consideration in the identification of plant-specific data is whether design changes have been made to the plant or its components that invalidate some of the historical data. For example, changing the type of flow controller could impact the operation of a particular turbine-driven pump. Thus, the total historical count of the turbine-driven pump events is not valid for the current condition of the plant. Typically, the turbine-driven pump data prior to the design change would be deleted from the data analysis. However, this has the undesirable impact of reducing sample size. Another approach is to investigate whether there is indeed a significant difference in the fraction of events before and after the design change. Not all the failures may be invalidated by the design change and so the historical data prior to the design change implementation may have partial validity and could be included in the data analysis.

Consideration of design changes is one example of where censoring of data can and should be performed. Other reasons can be used for data censoring if they are well supported and valid. For example, it is not uncommon to eliminate data from the first year of plant operation since it represents failures that occurred during the plant break-in period. However, any data censoring should be approached carefully to avoid losing important information and biasing results (eliminating the first year of data actually makes the results less biased).

5.2.2.2 Event Severity Classification

As discussed in Chapter 3, component malfunction events are commonly classified into one of the following three event severity categories:

- catastrophic failures,
- degraded failures, and
- incipient failures.

Catastrophic failures require some kind of repair or replacement action on the component in order to restore the component to operability. Events that are classified as catastrophic failures are used in calculating plant-specific component failure rates and probabilities of

failure on demand. Information on catastrophic failures occurring during critical operation is also used in calculating maintenance outage unavailabilities.

Degraded failures can prevent a system or train from meeting the success criteria modeled in the PRA. An incipient failure is such that there is no significant degradation in performance but there are indications of a developing fault. The difference between the two is generally a matter of severity. Events classified as incipient or degraded failures are generally used in calculating plant-specific maintenance unavailabilities. Although both degraded and incipient failures will typically lead to a corrective action, the corrective action may or may not make the component unavailable to perform its function. For example, maintenance on the operator of a valve that is normally open will not lead to the unavailability of the valve if is required to open for system operation. This illustrates the importance of ascertaining from event records the modes of a component operation that a corrective action would prevent.

Sometimes the event information is so unclear and incomplete that a definite classification of the severity of a component malfunction event is not possible. The data analyst in this situation is faced with the difficult task of deciding whether to call a malfunction a failure or not. The inability to distinguish between severity levels of failures is particularly important. The difference between the probabilities of catastrophic and degraded modes of failures can be significant especially when dealing with highly reliable components that rarely fail. The difference between no failures and one failure in estimating the failure rate is much more than the difference between 10 and 11 failures. Thus, the data analyst must be careful when classifying the few failures that may have occurred. In the absence of sufficient information, the tendency is to conservatively record such events as catastrophic failures. This is reasonable as long as the impact on the final PRA results is not significant. For cases where the judgement of the data analyst is important to the PRA results, it could be incorporated explicitly into the PRA quantification as a source of uncertainty. This issue is discussed further in Section 6.1.2.2.

5.2.3 Component Data Allocation

This section gives guidelines on the allocation of plant specific events to each component failure mode of interest. This includes the allocation of events contributing to the unavailability of components or systems due to test and maintenance actions. The goal of this allocation process is to correlate each event report with one or more basic events of the PRA model. This requires that the event report be identified with a specific component, and that the severity of the event be determined and associated with the proper component failure mode(s).

The use of component identification numbers in event reports is generally sufficient to allocate the event to a particular component. The description of the event can also guide the data analyst to a particular component failure mode (i.e., a basic event in a fault tree), or in some cases, to a particular gate in a fault tree. However, a thorough review of the cause of the event together with a knowledge of the boundaries of the basic events of the fault trees is generally needed for a correct allocation to be made. For example, an event report identified with a specific motor-operated valve (MOV) that involves the deenergization of a 480V bus should be associated with the bus unavailability and not the MOV. If the event is a local fault of the MOV or its breaker, it is associated with MOV itself.

As discussed previously, the severity of the event is important in allocating the event to specific component failure modes. A catastrophic component failure will generally result in an extended period during which the component is unavailable while it is being repaired. Thus, an event involving a catastrophic failure must be counted in estimating the failure of the component to operate and in estimating its unavailability due to maintenance. Degraded and incipient failures are used in calculating plant-specific maintenance unavailabilities. Some degraded failures may result in sufficient degradation that it can not meet its required success criteria (e.g., the flow rate for a pump is reduced to 300 gpm when 500 gpm is required for success). In such cases, a degraded failure is also included as a component failure to operate.

5.2.3.1 Component Failure Event Allocation

Because of the variability in the level of reporting associated with maintenance events, the allocation of event reports to specific PRA model events can be a subjective process. The following are some ground rules to help perform the component failure event allocation. The majority of these ground rules have been identified and published in EPRI TR-100381 (EPRI 1992). Additional guidelines are based on the experience of PRA vendors and NRC data analysts.

1. For standby components such as pumps, diesel generators, and fans, PRA models generally distinguish between failure to start and failure to run modes. It is important to understand the definition of each failure mode in order to associate historical maintenance events with the different basic event types. For example, if a fault tree basic event represents a failure of a pump to start, it usually means exactly that. However, it is not unusual in PRAs to define "diesel generator fails to start" as encompassing a failure to start or a failure during the first hour given that the start was successful. Whatever definitions are used, the event allocation must be performed to match them.

2. As indicated in Chapter 2, there are two ways to model failures to start: the demand failure and standby failure models. In the demand failure model, the equipment is ready to operate but for some reason, does not start or change state when demanded. In the standby failure model, the equipment has developed an unannounced condition that will prevent it from starting when demanded. When reviewing raw data, it can be difficult to identify whether a component failed on the demand or prior to the demand. Thus, as indicated in Section 2.3.4, either model could be used in this situation. The demand failure model provides the higher failure probability.

3. A catastrophic or degraded failure that is revealed while a component is in the standby mode, and that results in a maintenance action, is accounted for in the unavailability due to maintenance event for that component. If the failure is such that it could also occur while the component is performing its mission, it should also be counted as a component failure. For example, external leakage above allowable amounts from a standby pump that requires isolation of the pump to repair it, contributes to the unavailability of the pump due to maintenance. Since such leakage could occur during pump operation, the event should also be used to determine the failure rate for pump leakage. The amount of leakage would have to be sufficient to prevent the pump train from delivering the required flow.

4. Catastrophic failures of standby equipment to start (or run) that occur during an actual component demand, contribute to that failure mode. Similarly, failures to start (or run) during tests that closely mimics the conditions that the component would be subjected to during an unplanned demand should also be included in the evaluation for the component failure mode.

5. Degraded failures that are not serious enough to prevent the component from performing its function are not included as failures of the component. Expressed in another way, the failure of the component must match the definition of the failure in the PRA model. For example, vibration in a pump that results in the pump only delivering 500 gpm instead of the rated flow of 600 gpm is not a failure event if 500 gpm is sufficient to meet its function and the pump continued to supply that flow for a period at least equal to the mission time required in the PRA model. However, such failures would be included in the unavailability due to maintenance since their effect is to induce maintenance activity.

   There is a caveat to this guideline to consider. If the degraded failure is revealed in a short test duration, an analyst cannot be sure the component would have succeeded over its mission time. In this case, the analyst can attempt to extrapolate the rate of degradation to determine if the component would meet its failure criteria sometime during its mission time. For example: a pump develops a slow oil leak during a test. If the rate of leakage is such that the pump would run out of lubricating oil during the required pump mission time as modeled in the PRA, than the event is considered as a pump failure to continue to run.

6. Degraded conditions for which a failure would have occurred if the system had been demanded are considered a failure. For example, if an operator discovers that a pump had no oil in its lubrication reservoir, the pump may have started (unless there was an interlock preventing a pump start on low oil level) but likely would not have run long. In either case, this event would be counted as a failure to start.

7. If the event report identifies that the failure of component A is the result of the failure of another component B that is modeled explicitly in the PRA, the event is associated with component B and not with component A. For example, failures of a pump from plugged suction screens should not be allocated as pump failures if the screens are modeled separately.

   The clear identification of the component boundary is an important factor in these situations. For

example, the allocation of an event that identifies the failure of an emergency pump due to the failure of a safety actuation signal is dependent upon whether the actuation logic is included in the pump boundary or is treated as a separate event in the model. Typically, the components related to the safety actuation signal are not included in the pump boundary definition and this event should not be counted as a pump failure. However, if the safety actuation signal is included in the pump boundary, then the command fault should be included as a failure mode of the pump.

8. An event reporting a degraded or failed state of a redundant piece part should be excluded from the failure events if the component boundary includes the redundant piece parts. For example, if a diesel generator has two redundant air start motors that are included in the diesel generator boundary definition, failure of one air start motor would not be counted as a failure of the diesel generator. This example illustrates how a coarse definition of a component boundary can result in the failure to account for some degraded component states.

9. If a documented failure during a test or actual demand could not be repeated on subsequent tries, it may not have be included as a potential failure. Similarly, events which are very quickly recoverable may also not be considered potential failures (the recovery should not be included in the PRA model). Whether an event meeting either of these situations should be considered a failure is a function of the success criterion for the component in terms of the time window within which it has to operate. For example, the spurious closure of an MOV may prevent the injection of coolant into the core from a particular system. However, the event records may indicate that in all such occurrences, the valve was quickly reopened before coolant levels dropped to unacceptable levels. In such cases, the events should not be considered as failure events for the MOV.

10. Successive failures of the same components over short time intervals should be counted as a single failure. Similarly, failures of a component during post-maintenance testing where the failure is related to the maintenance or to an earlier failure that the maintenance was trying to correct should be considered as a continuation of the original failure and should be disregarded. The successive failures are because proper maintenance was not performed to fix the initial problem, and the component is still in the failed state.

11. If failures resulting from human errors after testing, maintenance, and instrument miscalibrations are explicitly included in system models, these events should not be included as component hardware failure events. Such events are typically quantified using human reliability analysis methods. However, some PRAs have not explicitly included these human errors in the models. In such cases, the contribution from human-related failures should be incorporated into the appropriate component failure rate or probability.

12. An event reported as a failure to meet technical specifications, but which would not result in a catastrophic failure in the PRA sense should not be included, but it may lead to a maintenance unavailability. For example, the failure of a diesel generator to start and pick up loads within 10 seconds might be a reportable failure for regulatory purposes. However, in the PRA sense it is not a failure if the diesel did not pick up loads in 10 seconds and the "failure" did not have a discernible effect on the ability of the plant to mitigate an initiating event. However, this failure would require maintenance to alleviate the fast loading failure.

13. Failures that occur under abnormal environmental conditions should be segregated from failures that occur under normal conditions. These failures can identify important interactions between systems and thresholds for failure that should be accounted for in the PRA. In general, PRAs assume components fail under harsh conditions. Under this assumption, actual failure events in harsh environments can be eliminated from consideration. For example, actual failures of electrical components following a loss of a heating, ventilation, or air-conditioning (HVAC) system should be eliminated from the data analysis if the HVAC dependency is modeled explicitly in the PRA model and the component is always assumed to fail under those conditions. However, if there are also many component successes under the same harsh environments, than a component failure probability under those conditions can be calculated and used in the PRA model conditional on the occurrence of the harsh environment.

5.2.3.2 Allocation of Unavailability Data

Unavailability occurs primarily due to maintenance activities but some minor contributions can also result from testing performed during periodic surveillance activities. These unavailability contributions can be

included in a system model at a component, segment, or train level. In addition, separate basic events for maintenance and testing unavailabilities, or for planned and unplanned unavailabilities can be included in system models. In a data analysis, the allocation of unavailability data must be performed to match the basic events in the system models. The following guidelines are useful in allocating events for determining unavailabilities due to test and maintenance. These ground rules have been extracted from EPRI TR-100381 (EPRI 1992) and from the experience of PRA vendors and NRC data analysts.

1. A maintenance event must result in the component not being capable of performing its function, as modeled in the PRA, in order to contribute to the component or train unavailability. For example, maintenance performed on a normally open MOV (that is required to stay open during its mission time) with the valve locked in the open position is not an event of interest. Similarly, a maintenance event involving some electrical repairs on an MOV that do not necessitate moving it from the position required for successful system operation is also not an event of interest. However, in either case, if the valve were required to close for any reason, then both events would be of interest.

2. Some testing procedures may result in component, train, or system unavailability. For example, a full flow test of a system through a test path could require that a normally closed injection valve be disabled in order to prevent inadvertent injection. The injection valve would be unavailable during the test period. However, systems often have logic which would actuate the system even if it was being tested. In this situation, there would be no system unavailability due to the test. A review of testing procedures coupled with knowledge of system actuation logic is required to determine if testing can result in component, train, or system unavailability.

3. If a maintenance report indicates that one or more trains of front line systems are unavailable due to maintenance activities of a support system, the unavailability is associated only with the support system.

4. If while performing maintenance on a support system, maintenance is also performed on the front line system it supports, the unavailability of the front line system should be counted if the two maintenance activities are not always performed together.

5. If an unavailability on one component is actually due to maintenance activity on another component that is included in the PRA model, the unavailability is associated with the second component only. For example, a declared unavailability of a pump due to maintenance on a room cooler should be included only as a maintenance on the room cooler if the dependence of the pump on the room cooler was modeled explicitly. As another example, if the maintenance results in the unavailability of a source of suction to a pump (e.g., maintenance on a supply tank), then it is better to model this as an unavailability of the source rather than the pump. Assigning the event to the source unavailability is absolutely required if the source is shared with other pumps. In general, maintenance unavailability should be allocated consistent with the component boundaries and system modeling.

6. There may be events where the unavailability of a component in a system model is due to maintenance on a component that is not included in any system model. In such cases, the event should be included as an unavailability of all the modeled components removed from service. For example, the contribution of maintenance on a drain valve for a pump train will likely not be modeled in the PRA but should be included as a contributor to the unavailability of the entire pump train since it would likely result in isolation of the train.

7. Coincident outage times for redundant equipment (both intra- and inter-system) should reflect actual plant experience. For some systems, the available redundancy may be higher than that limited by technical specifications. In this case, maintenance may be performed on two out of three trains at the same time. The modeling of dual component maintenance events in the PRA should be consistent with the actual plant experience. Note that because of the allowed outage time limitations in technical specifications, the maintenance unavailability may be lower when two trains are taken out for maintenance.

8. The maintenance data at the plant most likely will contain planned and forced maintenance. Most of the maintenance events will be forced type. If the PRA models the two types of maintenance separately and it is possible to distinguish between the two types in the data, these should be recorded separately.

9. In some cases, more than one maintenance activity may be recorded on an event report. When this occurs, each separate maintenance activity must be considered at the highest possible component level. For example, if the suction or discharge valve of a pump requires maintenance, the pump would be tagged out for the duration of the work. As previously discussed, the maintenance unavailability should be associated with the valve. If during this maintenance outage, some minor maintenance was performed on the pump, than the entire maintenance outage can be recorded as a pump maintenance event. The duration of the maintenance would be the time between when the first component is tagged out and when the last component is tagged in.

   However, if the maintenance unavailability is being modeled in the PRA at the train level, all maintenance activities on any component are included. In this situation, each maintenance event on any component in the train is included. If multiple components are tagged out during the maintenance event, the duration of the maintenance would be the time between when the first component is tagged out and when the last component is tagged in.

10. Functional dependencies represented in the PRA models must be considered in the allocation of maintenance events. For example, if a chilled water pump is taken out for maintenance, together with an HVAC chiller that it supports, only the chilled water pump is counted as being unavailable for maintenance. The functional dependency between the two components in the PRA model will account for the chiller being unavailable when the chilled water pump is under maintenance.

11. The cold shutdown periods in the time window over which data are being collected should be defined. The maintenance performed during shutdown is not included in the determination of component unavailability during power operation.

12. Special attention is required when allocating maintenance events for systems or components shared between units at a site. The technical specifications pertaining to shared systems can be different depending on the status of both units. The PRA model may include basic events to account for the dependence of the system unavailability on the mode of operation for each unit. In such cases, the maintenance events should be allocated to match those event definitions.

5.2.4 Component Exposure Evaluation

The data identification and allocation process discussed in the previous sections results in the identification of the number of events associated with each component failure mode. To generate component failure probabilities and rates, it is also necessary to estimate the operational exposure of the components. The term "exposure" refers to the amount of component operating time when considering failure rates and to the number of demands (or cycles) when considering failure probabilities.

Exposure data are normally developed by reviewing plant documents; e.g., test procedures and the knowledge of component function (standby, normally operating, etc.), and systems lineup. In some cases, an operation time meter provides information about the cumulative hours of operation of a component.

Development of exposure data involves many judgments and assumptions. The guidance provided in this section sometimes leads to an approximate value for the exposure data, which may differ substantially from the actual experience. Although typically the range of uncertainties associated with the exposure data are much smaller than those for the failure data, there may be cases where the combined effect of uncertainty about the exposure and failure has a significant impact on the estimate of the failure rate or probability. The issue of uncertainty in the data (both in the failure and exposure data) is addressed in Section 6.1.2.2 of this handbook.

The following sections outline the process for estimating the number of demands and the operating time for each component. Much of this guidance is taken from EPRI TR-100381 (EPRI 1992).

5.2.4.1 Time-Related Exposures

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

Some plant systems, sometimes called alternating or intermittently operated systems, have multiple redundant trains where only a subset of those trains are required to operate at any one time. A standard practice at nuclear power plants is to alternate the trains that are

operating and in standby at specified intervals. The times of operation and changeover from one train to another are typically recorded in the control room or some other log book. However, since the pumps in different trains of a system are usually grouped together for data analysis, it is not necessary to have an accurate log of how long an individual pump was in operation. Instead, it is only necessary to evaluate the exposure time for the pumps as a group. For example, if two of three pumps are normally operating in a particular plant mode, the total operating time for that pump group is twice the calendar time spent by the plant in that mode.

For a component in a standby system, the operating time is generally given by the time the system is operated during testing. Note that an important criterion for including test data when evaluating both the failure and exposure data is that the test should mimic the component operation that would be required in an unplanned demand. The testing period may be recorded in control room logs or other logs. The operating time during testing for a population of components may also be estimated by summing the product of the component population, test frequency, and test duration for each test during the period where failure data was collected. It should be noted that for most plants, and most components, the cumulative run time during testing is relatively short.

Some systems that are in standby during normal power operation are also used during other modes of operation. For example, the residual heat removal (RHR) system in both BWRs and PWRs is used during shutdown. Similarly, a standby system may be used during power operation for a special purpose. For example, the RHR system in a BWR may be used to increase or decrease the suppression pool level. Thus the operating times during these modes of operation should be included, in addition to the run times during testing, if any failures during these modes are pertinent to the safety function of the system (e.g., the entire RHR pump operating history may be pertinent since the pump must operate when the RHR system is used to respond to an accident). In such situations, the times of startup and shutdown of the standby system may be recorded in the control room logs. Alternatively, if the component is required to continuously operate during shutdown, the operating time can be easily established by directly relating it to the time spent in that plant mode.

5.2.4.2 Demand-Related Exposures

To evaluate the probability of the failure of a component to start or change states, the number of demands experienced by the component must be evaluated. Although this would seem to be a simple process, in practice the number of demands is often one of the most difficult parameters to calculate accurately. Component demands from all contributors should be included. This can include contributions from testing, automatic and manual actuations, and corrective maintenance. The methods of calculating the number of demands from each of these types of demands are explained below.

5.2.4.2.1 Test Demands

Periodic testing is an important source of demands for components in standby systems. The surveillance testing and required frequency for the plant is performed in accordance with the technical specifications. However, some plants may choose to perform testing more frequently than required by the technical specifications.

An important criterion for including test data in evaluating both the failure and exposure data is that the test should mimic the component operation that would be required in an unplanned demand.

Surveillance procedures identify the components that must change state at each test. For each surveillance test pertinent to the system, it is important to identify which components are operated, the unavailability of the system during the test (if applicable), and the frequency and duration of the test. A functional test of a pump often requires the operation of valves as well as the pump and is an important source of information on valve demands. Neglecting demands on components from tests on other components can lead to a significant underestimation of the total number of demands. The number of test demands for individual components may be determined from the actual number of tests as recorded in a control room or test logs or be estimated based on the test frequencies.

It should be noted that the test may not be a valid test for all the components within the component boundary. For example: the automatic initiation portion of a component circuit will not be tested during a test where the component is manually initiated. For components such as diesel generators, tests which start the engine, but do not close the breaker onto the bus are not true tests of the capability of the diesel generator to provide the necessary load. Note that if there is a subcomponent that is included in a component's boundary which is not tested along with the rest of the component, it is desirable to analyze it as a separate component.

5.2.4.2.2 Automatic and Manual Initiation

Actual unplanned demands on components should be included in the demand count. For standby safety system components, some unplanned demands can be traced back to the occurrence of automatic initiation signals (both actual and spurious signals). .These signals include emergency core cooling system (ECCS) initiating signals, turbine trip signals, losses of offsite power, and reactor scrams. Different groups of component may be initiated by different signals or sets of signals, depending on the functions and the system they are in. Information on the components that can be initiated by each signal can be identified through knowledge of the plant. For example, all low-pressure ECCS pumps in a BWR could be initiated by an ECCS signal but the motor-operated valves in the ECCS injection paths would require an additional low vessel pressure signal before they would open. Information on the historical number of occurrences of actual or spurious signals should be available from the plant records such as the monthly operating reports or control room logs.

In addition, manual actuation of systems or components may occur during plant operation. Two examples cited above in the discussion of operating time contributors are also pertinent here. The first is the case where alternating trains are placed in operation and standby. The act of switching operating trains results in demands on components. The second case involves the use of standby systems to perform special functions. For example, the RHR system in a BWR may be used to increase or decrease the suppression pool level. These special uses also result in component demands. In both cases, the times of startup and shutdown of the standby system may be recorded in the control room or other types of logs.

Finally, manual actuation of systems to respond to adverse plant conditions is another source of unplanned demands that needs to be accounted for in the exposure evaluation. The occurrences of such demands are generally recorded in LERs, control room logs, and monthly operating reports.

5.2.4.2.3 Corrective Maintenance

Maintenance can result in demands on components in several ways. Before the maintenance activities are begun, the operating and maintenance staff make the maintenance action safe for both personnel and the system by disabling and tagging out appropriate components. This then requires some components to change state resulting in a demand.

In many instances, demands are placed on components that are not the subject of the corrective maintenance. The most obvious demands occur when a component is returned to service. Before restoring the component to service following maintenance, a complete functional checkout is usually performed on the component and other components in the functional loop. The number of demands on the components resulting from corrective maintenance is obtained from the number of maintenance acts on specific components and an identification of what other components may have to change state to complete the functional test. **Note that per the guidance in the ASME PRA Standard (ASME 2002), demands from post-maintenance testing should be excluded from the exposure evaluation for the component under maintenance.**

Another example of a demand resulting from maintenance involves testing of redundant trains. If equipment fails in some systems, the technical specifications may require that redundant components be checked for operability before maintenance to ensure that they are available for service. In many cases, an increased frequency of surveillance testing of such redundant components is required. A typical example of this is reflected in the technical specifications for emergency diesel generators. These demands need to be included in the data analysis.

As indicated in the discussions presented above, development of exposure data involves many judgments and assumptions. Although typically the magnitude of error or the range of uncertainties associated with the exposure data are small compared with those of the failure data, there are cases where the combined effect of uncertainty about the exposure and failure has a significant impact on the estimate of the failure rate. The data analyst should consider some level of uncertainty in using such estimates.

5.2.5 Determination of Unavailable Time

Following the identification of the maintenance events contributing to the unavailability of a component, train, or system, the time the component is unavailable during each event is determined. The unavailability time is the time between when the component is removed from service until it is actually restored to service. In many cases, maintenance work orders will provide this information by identifying one or more tag-ins and tag-outs for equipment with the date and time of day that both occur. Using these times to determine the unavailability time may be a little conservative because the repair may be completed before the component is declared tagged in.

Some maintenance work orders may contain multiple tag-outs and tag-ins for a given component. If the component was operable between these periods, than the unavailability is the sum of the individual unavailability times for each period. However, if the component was inoperable between the periods, than the unavailability time starts at the first tag-out and ends at the last tag-out.

Unfortunately, the actual time of unavailability may not be recorded in maintenance work order forms. In many cases, the time recorded may reflect a prior estimate of how long the maintenance activity will take, may represent the man-hours taken to complete the task rather than calendar time, or may include time to complete paperwork.

When the unavailability time is not specified in a maintenance work order, other plant documents should be examined for that information. Maintenance activity information may be recorded in other documents such as operator logs or component operating logs. For example, a maintenance activity on a safety-related component will start the clock for a limiting condition of operation (LCO) specified in the technical specifications, and this should be recorded in some place, usually the control room log. The time when the function is restored should also be recorded. Unfortunately, not all maintenance events result in an LCO and thus timing information may not be available.

When reliable estimates of the start and finish times for a maintenance event are not available, one recourse is to ask plant maintenance and operations staff to provide estimates of the ranges in the unavailable time per maintenance act for the components. Another recourse is to use data provided from some maintenance events to estimate the unavailability for other events.

5.3 Recovery Event Data

In PRA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems. Recovery actions involve the use of alternate equipment or means to perform a function when primary equipment fails, or the use of alternate means to utilize equipment that has not responded as required. Examples of recovery actions include opening doors to promote room cooling when an HVAC system fails, recovering grid-related losses of offsite power by rerouting power, manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a handwheel to manually open an MOV when the motor fails to operate. Repair actions involve the actual repair of the mechanism which caused a component or system to fail. Examples of repair actions include repairing weather-related losses of offsite power, repair of a pump that failed to start, or replacement of a failed circuit breaker.

PRA models typically include a number of recovery actions of the type identified above. However, because recovery actions can involve complicated actions that are governed by procedures, most are typically evaluated using HRA methods. A general exception is the treatment of offsite power recovery where the required recovery actions are often not within the jurisdiction of the plant personnel. Thus, offsite power recovery data is collected and reduced for use in PRAs.

The repair of components is generally not modeled in PRAs since:

- the time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed),
- because repair is an action that is not always governed by procedures and thus difficult to justify,
- the availability of spare parts can not always be certain, and
- because abnormal procedures generally direct operators to use alternative equipment as a first priority.

There are always exceptions to these general observations. For example, the replacement of fuses is an action identified in some fire abnormal procedures and can be accomplished rather quickly since spare fuses are available. As with a recovery action, either an HRA or data reduction approach could be utilized to generate a failure probability for a repair action.

The modeling of recovery and repair actions in PRA reflects the need to accomplish the action within some time frame (e.g., before core damage occurs). Thus, the collected data must include both the time of failure and recovery to be utilized in the PRA. This section provides guidance on the process for collecting and reducing recovery and repair data. A description of the type of data that is reviewed in this effort and guidelines for allocating that data.

5.3.1 Recovery Data Identification

Recovery and repair information can generally be extracted from maintenance records and LERs that

identify component and system failures. Thus, the evaluation of recovery and repair information is an offshoot of the component failure data review. In general, only data from actual component and system demands should be included in the recovery/repair data evaluation. When failures occur during actual demands, operators should be strongly motivated to try to recover the component or system.

However, if a component or system fails to start during a surveillance test, the need for repair is not as pressing and thus not reflective of accident conditions. For this reason, recovery and repair information for failures during surveillance tests should be excluded from recovery/repair probability evaluation.

5.3.2 Recovery Data Allocation

Since component recovery data evaluation should be performed in conjunction with the component data allocation, the general rules provided in Section 5.2.3 apply. In addition, the following guidelines are provided to address allocating recovery data for other events modeled in the PRA (e.g., restoring offsite power or reopening main steam isolation valves):

1. Only failures during actual demands are included. Failures during surveillance tests are excluded as being nonrepresentative of accident conditions. For the failures during actual demands, the data analyst should assess whether the recovery/repair action was performed under similar stresses that would occur under accident conditions. Atypical events should be eliminated or considered to be sources of uncertainty.

2. For each failure event, the recovery/repair time is the time between when the failure first occurs and the time when it is returned to service. Using these times ensures that the time of the failure, the time required to recognize it has occurred, the time to obtain spare parts if required, the actual time to repair the component or system, and the time to return the component to service are reflected in the recovery/repair time. Events that do not include either time should be excluded from the evaluation.

3. Recovery information on systems or components resulting from an initiating event can be extracted from LERs or scram reports. For example, reopening MSIVs after their consequential closure (i.e., they are signaled to close following some other failure) may be included in a PRA for some initiators. The recovery time for such events are evaluated from the time the initial failure occurs leading to MSIV closure to until the closure signal is removed (by either fixing the original failure or by bypassing the signal) and the MSIVs in one hot leg are reopened. The time to perform other actions that may be required to maintain the MSIVs open (e.g., starting vacuum pumps) are also included in establishing the recovery time.

4. Recovery information on systems or components causing an initiating event can also be extracted from LERs or scram reports. For example, the time to recover offsite power initiating events can be extracted from LERs. However, LERs should also be searched for occurrences of offsite power failure following other initiating events. Recovery information should also be extracted for these events.