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.

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.

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 is generally reviewed for the following types of events:

- The accident initiating events analyzed in the PRA.
- 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 to specify the unavailability at the component, segment, train, or system level
- 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.

Identifying the scope of the plant-specific data analysis is important because the definitions of the component boundaries and the component failure mode definitions have to be consistent with those used in the systems analysis. The collected raw failure data must be consistent with the failure modes identified for that model.

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.

Interpretation and reduction of the raw data is required to obtain the reduced data used in the parameter estimation models described in Chapters 2and 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 8.

Typical sources of raw data available at nuclear power plants are identified in Section 4.1. 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 the 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 1985 and Poloski 1999a). Typical initiating events to consider during low power and shutdown conditions have also been established for both BWRs (Staple 1999) and PWRs (Chu 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 example of screening 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. However, a more rigorous and defensible method for determining initiating event frequencies that are representative of the current plant operation and design is to perform a trend analysis of all 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 be able 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 5.1 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 main steam isolation valves (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 boiling water reactors (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 reduced 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 should be recorded. Criticality factors for each plant is provided in Appendix H of NUREG/CR-5750 (Poloski 1999a) for the years 1987 through 1995. Alternatively, the generic frequencies 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.

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 some type of computerized file. The most useful raw data sources will 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 the 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 establish 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

5.

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 generic data bases failure rates. However, the analyst is cautioned in the use of this data since a usually reliable component may not be 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 $l0^{-3}$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), and the medium they carry (e.g., air, pure water, or borated water). Tests for poolability of data are described in Section 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
- 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 demand probabilities. Information on catastrophic failures occurring during critical operation are 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 outage 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 as 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 1 failure in estimating the failure rate is much more than the difference between 10 and 11 failures. Thus, the data analyst must be careful in 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.

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 process is to correlate each event report with one or more basic events of the PRA model. This requires that 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 generally is 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 in 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 it's 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 when estimating the 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 that 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 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. Because it is difficult to identify whether a component failed on the demand or prior to the demand, it is recommended that all failures to start (and failures of components such as valves to change positions) be analyzed using the demand failure model.

3. The maintenance of a standby component initiated by a catastrophic or degraded failure that is revealed while the component is in the standby mode 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 leakage event is not a failure of the pump to start or run.

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

5. Degraded failures that are not serious enough to prevent the component from performing it's 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 it's 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 as 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 can not 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 ran 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 disregarded. Similarly, failures of a component during post-maintenance testing where the failure is related to the maintenance or to the earlier failure that the maintenance was trying to correct should be considered as a continuation of the original failure and also 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 may lead to a maintenance unavailability. For example, while the failure of a diesel generator to start and pick up loads with in 10 seconds might be a reportable failure for regulatory purposes. However, in the PRA sense it is not a failure if the diesel did 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. 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. For example, actual failures of electrical components following a loss of a 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.

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.

5.

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 is 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 from review of 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 as compared with 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 criteria 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. 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 RHR system in both BWR and PWRs are 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.

<u>Test demands</u>. 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 criteria 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 components boundary which is not tested along with the rest of the component, it is desirable to analyze it as a separate component.

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 are another source of unplanned demands that needs to be accounted for in the exposure evaluation. The occurrence of such demands are generally recorded in LERs, control room logs, and monthly operating reports.

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.**

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 much smaller as compared with 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.

Exposure data are normally developed from review of plant documents; e.g., test procedures and the knowledge of component function (standby, normally operating, etc.), and systems lineup. In some cases, the equipment operation time meter provides information about the cumulative hours of operation of the component. However, this procedure only leads to an approximate value for the exposure data, which may differ substantially from the actual experience.

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 in 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 other 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 causing 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, 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 reflect 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 off chute 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 and 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 as 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.