Attachment 1, Section 2.2, “Mitigating Systems Cornerstone,” of NEI 99-02, “Regulatory Assessment Performance Indicator Guideline” (Draft)

MITIGATING SYSTEM PERFORMANCE INDEX

Purpose

The purpose of the mitigating system performance index is to monitor the performance of selected systems based on their ability to perform risk-significant functions as defined herein. It is comprised of two elements - system unavailability and system unreliability. The index is used to determine the significance of performance issues for single demand failures and accumulated unavailability. Due to the limitations of the index, the following conditions will rely upon the inspection process for determining the significance of performance issues:

1. Multiple concurrent failures of components
2. Common cause failures
3. Conditions not capable of being discovered during normal surveillance tests
4. Failures of non-active components

Indicator Definition

Mitigating System Performance Index (MSPI) is the sum of changes in a simplified core damage frequency evaluation resulting from changes in unavailability and unreliability relative to baseline values.

Unavailability is the ratio of the hours the train/system was unavailable to perform its risk-significant functions due to planned and unplanned maintenance or test on active and non-active components during the previous 12 quarters while critical to the number of critical hours during the previous 12 quarters. (Fault exposure hours are not included; unavailable hours are counted only for the time required to recover the train's risk-significant functions.)

Unreliability is the probability that the system would not perform its risk-significant functions when called upon during the previous 12 quarters.

Baseline values are the values for unavailability and unreliability against which current changes in unavailability and unreliability are measured. See Appendix F for further details.

The MSPI is calculated separately for each of the following five systems for each reactor type.

BWRs

- emergency AC power system
- high pressure injection systems (high pressure coolant injection, high pressure core spray, or feedwater coolant injection)
- heat removal systems (reactor core isolation cooling)
- residual heat removal system (or their equivalent function as described in the Additional Guidance for Specific Systems section.)

- cooling water support system (includes risk significant direct cooling functions provided by service water and component cooling water or their cooling water equivalents for the above four monitored systems)

PWRs

- emergency AC power system
- high pressure safety injection system
- auxiliary feedwater system
- residual heat removal system (or their equivalent function as described in the Additional Guidance for Specific Systems section.)
- cooling water support system (includes risk significant direct cooling functions provided by service water and component cooling water or their cooling water equivalents for the above four monitored systems)

Data Reporting Elements

The following data elements are reported for each system

- Unavailability Index (UAI) due to unavailability for each monitored system
- Unreliability Index (URI) due to unreliability for each monitored system

During the pilot, the additional data elements necessary to calculate UAI and URI will be reported monthly for each system on an Excel spreadsheet. See Appendix F.

Calculation

The MSPI for each system is the sum of the UAI due to unavailability for the system plus URI due to unreliability for the system during the previous twelve quarters.

MSPI = UAI + URI.

See Appendix F for the calculational methodology for UAI due to system unavailability and URI due to system unreliability.

Definition of Terms

A train consists of a group of components that together provide the risk significant functions of the system as explained in the additional guidance for specific mitigating systems. Fulfilling the risk-significant function of the system may require one or more trains of a system to operate simultaneously. The number of trains in a system is generally determined as follows:

- for systems that provide cooling of fluids, the number of trains is determined by the number of parallel heat exchangers, or the number of parallel pumps, or the minimum number of parallel flow paths, whichever is fewer.

- for emergency AC power systems the number of trains is the number of class 1E emergency (diesel, gas turbine, or hydroelectric) generators at the station that are installed to power shutdown loads in the event of a loss of off-site power. (This does not include the diesel generator dedicated to the BWR HPCS system, which is included in the scope of the HPCS system.)

Risk Significant Functions: those at power functions, described in the "Additional Guidance for Specific Systems," that were determined to be risk-significant in accordance with NUMARC 93-01, or NRC approved equivalents (e.g., the STP exemption request….) The system functions described in the "Additional Guidance for Specific Systems" must be modeled in the plant's PRA/PSA. ~~of risk-significant SSCs as modeled in the plant-specific PRA. Risk metrics for identifying risk-significant functions are:~~

~~Risk Achievement Worth > 2.0, or~~

~~Risk Reduction Worth >0.005, or~~

~~PRA cutsets that account for 90% of core damage frequency90% of core damage frequency accounted for.~~

Risk-Significant Mission Times: The mission time modeled in the PRA for satisfying the risk-significant function of reaching a stable plant condition where normal shutdown cooling is sufficient. Note that PRA models typically analyze an event for 24 hours, which may exceed the time needed for the risk-significant function captured in the MSPI. However, other intervals as justified by analyses and modeled in the PRA may be used.

Success criteria are the plant specific values of parameters the train/system is required to achieve to perform its risk-significant function. Default values of those parameters are the plant's design bases values unless other values are modeled in the PRA.

Clarifying Notes

Documentation

Each licensee will have the system boundaries, active components, risk-significant functions and success criteria readily available for NRC inspection on site. Additionally, plant-specific information used in Appendix F should also be readily available for inspection.

Success Criteria

Individual component capability must be evaluated against train/system level success criteria (e.g., a valve stroke time may exceed an ASME requirement, but if the valve still strokes in time to meet the PRA success criteria for the train/system, the component has not failed for the purposes of this indicator because the risk-significant train/system function is still satisfied). Important plant specific performance factors that can be used to identify the required capability of the train/system to meet the risk-significant functions include, but are not limited to:

- Actuation
  - Time

- Auto/manual
- Multiple or sequential

- Success requirements
    - Numbers of components or trains
    - Flows
    - Pressures
    - Heat exchange rates
    - Temperatures
    - Tank water level
- Other mission requirements
    - Run time
    - State/configuration changes during mission
- Accident environment from internal events
    - Pressure, temperature, humidity
- Operational factors
    - Procedures
    - Human actions
    - Training
    - Available externalities (e.g., power supplies, special equipment, etc.)

System/Component Interface Boundaries

For active components that are supported by other components from both monitored and unmonitored systems, the following general rules apply:

- For control and motive power, only the last relay, breaker or contactor necessary to power or control the component is included in the active component boundary. For example, if an ESFAS signal actuates a MOV, only the relay that receives the ESFAS signal in the control circuitry for the MOV is in the MOV boundary. No other portions of the ESFAS are included.

- For water connections from systems that provide cooling water to an active component, only the final active connecting valve is included in the boundary. For example, for service water that provides cooling to support an AFW pump, only the final active valve in the service water system that supplies the cooling water to the AFW system is included in the AFW system scope. This same valve is not included in the cooling water support system scope.

Water Sources and Inventory

Water tanks are not considered to be active components. As such, they do not contribute to URI. However, periods of insufficient water inventory contribute to UAI if they result in loss of the risk-significant train function for the required mission time. Water inventory can include operator recovery actions for water make-up provided the actions can be taken in time to meet the mission times and are modeled in the PRA. If additional water sources are required to satisfy train mission times, only the connecting active valve from the additional water source is considered as an active component for calculating URI. If there are valves in the primary water source that must change state to permit use of the additional water source, these valves are considered active and should be included in URI for the system.

Monitored Systems

Systems have been generically selected for this indicator based on their importance in preventing reactor core damage. The systems include the principal systems needed for maintaining reactor coolant inventory following a loss of coolant accident, for decay heat removal following a reactor trip or loss of main feedwater, and for providing emergency AC power following a loss of plant off-site power. One risk-significant support function (cooling water support system) is also monitored. The cooling water support system monitors the risk significant cooling functions provided by service water and component cooling water, or their direct cooling water equivalents, for the four front-line monitored systems. No support systems are to be cascaded onto the monitored systems, e.g., HVAC room coolers, DC power, instrument air, etc.

Diverse Systems

Except as specifically stated in the indicator definition and reporting guidance, no credit is given for the achievement of a risk-significant function by an unmonitored system in determining unavailability or unreliability of the monitored systems.

Common Components

Some components in a system may be common to more than one train or system, in which case the unavailability/unreliability of a common component is included in all affected trains or systems. (However, see "Additional Guidance for Specific Systems" for exceptions; for example, the PWR High Pressure Safety Injection System.)

Short Duration Unavailability

Trains are generally considered to be available during periodic system or equipment realignments to swap components or flow paths as part of normal operations. Evolutions or surveillance tests that result in less than 15 minutes of unavailable hours per train at a time need not be counted as unavailable hours. Licensees should compile a list of surveillances/evolutions that meet this criterion and have it available for inspector review. In addition, equipment misalignment or mispositioning which is corrected in less than 15 minutes need not be counted as unavailable hours. The intent is to minimize unnecessary burden of data collection, documentation, and verification because these short durations have insignificant risk impact.

If a licensee is required to take a component out of service for evaluation and corrective actions for greater than 15 minutes (for example, related to a Part 21 Notification), the unavailable hours must be included.

Treatment of Demand /Run Failures and Degraded Conditions

1. Treatment of Demand and Run Failures
Failures of active components (see Appendix F) on demand or failures to run, either actual or test, while critical, are included in unreliability. Failures on demand or failures to run at any other time~~with the reactor shutdown~~ must be evaluated to determine if the failure would have resulted in the train not being able to perform its risk-significant at power functions, and must therefore be included in unreliability. Unavailable hours are included only for the time required to recover the train's risk-significant functions and only when the reactor is critical.

2. Treatment of Degraded Conditions

   a) Capable of Being Discovered By Normal Surveillance Tests
   Normal surveillance tests are those tests that are performed at a frequency of a refueling cycle or more frequently.

   Degraded conditions, even if~~where~~ no actual demand existed, that render an active component incapable of performing its risk-significant functions are included in unreliability as a demand and a failure. The appropriate failure mode must be accounted for. For example, for valves, a demand and a demand failure would be assumed and included in URI. For pumps and diesels, if the degraded condition would have prevented a successful start demand, a demand and a failure is included in URI, but there would be no run time hours or run failures. If it was determined that the pump/diesel would start and load run, but would fail sometime during the 24 hour run test or its surveillance test equivalent, the evaluated failure time would be included in run hours and a run failure would be assumed. A start demand and start failure would not be included. If a running component is secured from operation due to observed degraded performance, but prior to failure, then a run failure shall be counted unless evaluation of the condition shows that the component would have continued to operate for the risk-significant mission time starting from the time the component was secured. Unavailable hours are included for the time required to recover the risk-significant function(s).

   Degraded conditions, or actual unavailability due to mispositioning of non-active components that render a train incapable of performing its risk-significant functions are only included in unavailability for the time required to recover the risk-significant function(s).

   Loss of risk significant function(s) is assumed to have occurred if the established success criteria has not been met. If subsequent analysis identifies additional margin for the success criterion, future impacts on URI or UAI for degraded conditions may be determined based on the new criterion. However, URI and UAI must be based on the success criteria of record at the time the degraded condition is discovered. If the degraded condition is not addressed by any of the pre-defined success criteria, an engineering evaluation to determine the impact of the degraded condition on the risk-significant function(s) should be completed and documented. The use of component failure analysis, circuit analysis, or event investigations is acceptable. Engineering judgment may be used in conjunction with analytical techniques to determine the impact of the degraded condition on the risk-significant function. The engineering evaluation should be completed as soon as practicable. If it cannot be completed in time to support submission of the PI report for the current quarter, the comment field shall note that an evaluation is pending. The evaluation must be completed in time to accurately account for unavailability/unreliability in the next quarterly report. Exceptions to this guidance are expected to be rare and will be treated on a case-by-case basis. Licensees should identify these situations to the resident inspector.

b) Not Capable of Being Discovered by Normal Surveillance Tests
These failures or conditions are usually of longer exposure time. Since these failure modes have not been tested on a regular basis, it is inappropriate to include them in the performance index statistics. These failures or conditions are subject to evaluation through the inspection process. Examples of this type are failures due to pressure locking/thermal binding of isolation valves, blockages in lines not regularly tested, or inadequate component sizing/settings under accident conditions (not under normal test conditions). While not included in the calculation of the index, they should be reported in the comment field of the PI data submittal.

Credit for Operator Recovery Actions to Restore the Risk-Significant Function

1. *During testing or operational alignment*:
Unavailability of a risk-significant function during testing or operational alignment need not be included if the test configuration is automatically overridden by a valid starting signal, or the function can be promptly restored either by an operator in the control room or by a designated operator[1] stationed locally for that purpose. Restoration actions must be contained in a written procedure[2], must be uncomplicated (*a single action or a few simple actions*), must be capable of being restored in time to satisfy PRA success criteria and must not require diagnosis or repair. Credit for a designated local operator can be taken only if (s)he is positioned at the proper location throughout the duration of the test for the purpose of restoration of the train should a valid demand occur. The intent of this paragraph is to allow licensees to take credit for restoration actions that are virtually certain to be successful (i.e., probability nearly equal to 1) during accident conditions.

[1] Operator in this circumstance refers to any plant personnel qualified and designated to perform the restoration function.

[2] Including restoration steps in an approved test procedure.

The individual performing the restoration function can be the person conducting the test and must be in communication with the control room. Credit can also be taken for an operator in the main control room provided (s)he is in close proximity to restore the equipment when needed. Normal staffing for the test may satisfy the requirement for a dedicated operator, depending on work assignments. In all cases, the staffing must be considered in advance and an operator identified to perform the restoration actions independent of other control room actions that may be required.

Under stressful, chaotic conditions, otherwise simple multiple actions may not be accomplished with the virtual certainty called for by the guidance (e.g., lifting test leads and landing wires; or clearing tags). In addition, some manual operations of systems designed to operate automatically, such as manually controlling HPCI turbine to establish and control injection flow, are not virtually certain to be successful. These situations should be resolved on a case-by-case basis through the FAQ process.

2. *During Maintenance*
Unavailability of a risk-significant function during maintenance need not be included if the risk-significant function can be promptly restored either by an operator in the control room or by a designated operator[3] stationed locally for that purpose. Restoration actions must be contained in a written procedure[4], must be uncomplicated (*a single action or a few simple actions*), must be capable of being restored in time to satisfy PRA success criteria and must not require diagnosis or repair. Credit for a designated local operator can be taken only if (s)he is positioned at a proper location throughout the duration of the maintenance activity for the purpose of restoration of the train should a valid demand occur. The intent of this paragraph is to allow licensees to take credit for restoration of risk-significant functions that are virtually certain to be successful (i.e., probability nearly equal to 1). The individual performing the restoration function can be the person performing the maintenance and must be in communication with the control room. Credit can also be taken for an operator in the main control room provided (s)he is in close proximity to restore the equipment when needed. Under stressful chaotic conditions otherwise simple multiple actions may not be accomplished with the virtual certainty called for by the guidance (e.g., lifting test leads and landing wires, or clearing tags). These situations should be resolved on a case-by-case basis through the FAQ process.

3. Satisfying ~~PRA success criteria~~Risk Significant Mission Times
Risk significant operator actions to satisfy pre-determined train/system risk-significant mission times can only be credited if they are modeled in the PRA.

Swing trains and components shared between units

[3] Operator in this circumstance refers to any plant personnel qualified and designated to perform the restoration function.

[4] Including restoration steps in an approved test procedure.

Swing trains/components are trains/components that can be aligned to any unit. To be credited as such, their swing capability should be modeled in the PRA to provide an appropriate Fussell-Vesely value.

Unit Cross Tie Capability

Components that cross tie monitored systems between units should be considered active components if they are modeled in the PRA and meet the active component criteria in Appendix F. Such active components are counted in each unit's performance indicators.

Maintenance Trains and Installed Spares

Some power plants have systems with extra trains to allow preventive maintenance to be carried out with the unit at power without impacting the risk-significant function of the system. That is, one of the remaining trains may fail, but the system can still perform its risk significant function. To be a maintenance train, a train must not be needed to perform the system's risk significant function.

An "installed spare" is a component (or set of components) that is used as a replacement for other equipment to allow for the removal of equipment from service for preventive or corrective maintenance without impacting the risk-significant function of the system. To be an "installed spare," a component must not be needed for the system to perform the risk significant function.

For unreliability, spare active components are included if they are modeled in the PRA. Unavailability of the spare component/train is only counted in the index if the spare is substituted for a primary train/component. Unavailability is not monitored for a component/train when that component/train has been replaced by an installed spare or maintenance train.

Use of Plant-Specific PRA and SPAR Models

The MSPI is an approximation using some information from a plant's actual PRA and is intended as an indicator of system performance. Plant-specific PRAs and SPAR models cannot be used to question the outcome of the PIs computed in accordance with this guideline.

Maintenance Rule Performance Monitoring

It is the intent that NUMARC 93-01 be revised to require consistent unavailability and unreliability data gathering as required by this guideline.

ADDITIONAL GUIDANCE FOR SPECIFIC SYSTEMS

This guidance provides typical system scopes. Individual plants should include those systems employed at their plant that are necessary to satisfy the specific risk-significant functions described below and reflected in their PRAs.

Emergency AC Power Systems

Scope

The function monitored for the emergency AC power system is the ability of the emergency generators to provide AC power to the class 1E buses upon a loss of off-site power while the reactor is critical, including post-accident conditions. The emergency AC power system is typically comprised of two or more independent emergency generators that provide AC power to class 1E buses following a loss of off-site power. The emergency generator dedicated to providing AC power to the high pressure core spray system in BWRs is not within the scope of emergency AC power.

The electrical circuit breaker(s) that connect(s) an emergency generator to the class lE buses that are normally served by that emergency generator are considered to be part of the emergency generator train.

Emergency generators that are not safety grade, or that serve a backup role only (e.g., an alternate AC power source), are not included in the performance reporting.

Train Determination

The number of emergency AC power system trains for a unit is equal to the number of class 1E emergency generators that are available to power safe-shutdown loads in the event of a loss of off-site power for that unit. There are three typical configurations for EDGs at a multi-unit station:

1. EDGs dedicated to only one unit.
2. One or more EDGs are available to “swing” to either unit
3. All EDGs can supply all units

For configuration 1, the number of trains for a unit is equal to the number of EDGs dedicated to the unit. For configuration 2, the number of trains for a unit is equal to the number of dedicated EDGs for that unit plus the number of “swing” EDGs available to that unit (i.e., The “swing” EDGs are included in the train count for each unit). For configuration 3, the number of trains is equal to the number of EDGs.

Clarifying Notes

The emergency diesel generators are not considered to be available during the following portions of periodic surveillance tests unless recovery from the test configuration during accident conditions is virtually certain, as described in “Credit for operator recovery actions during testing," can be satisfied; or the duration of the condition is less than fifteen minutes per train at one time:

- Load-run testing
- Barring

An EDG is not considered to have failed due to any of the following events:

- spurious operation of a trip that would be bypassed in a loss of offsite power event
- malfunction of equipment that is not required to operate during a loss of offsite power event (e.g., circuitry used to synchronize the EDG with off-site power sources)
- failure to start because a redundant portion of the starting system was intentionally disabled for test purposes, if followed by a successful start with the starting system in its normal alignment

Air compressors are not part of the EDG boundary. However, air receivers that provide starting air for the diesel are included in the EDG boundary.

If an EDG has a dedicated battery independent of the station's normal DC distribution system, the dedicated battery is included in the EDG system boundary.

If the EDG day tank is not sufficient to meet the EDG mission time, the fuel transfer function should be modeled in the PRA. However, the fuel transfer pumps are not considered to be an active component in the EDG system because they are considered to be a support system.

BWR High Pressure Injection Systems

(High Pressure Coolant Injection, High Pressure Core Spray, and Feedwater Coolant Injection)

Scope

These systems function at high pressure to maintain reactor coolant inventory and to remove decay heat following a small-break Loss of Coolant Accident (LOCA) event or a loss of main feedwater event.

The function monitored for the indicator is the ability of the monitored system to take suction from the suppression pool (and from the condensate storage tank, if credited in the plant's accident analysis) and inject into the reactor vessel.

Plants should monitor either the high-pressure coolant injection (HPCI), the high-pressure core spray (HPCS), or the feedwater coolant injection (FWCI) system, whichever is installed. The turbine and governor (or motor-driven FWCI pumps), and associated piping and valves for turbine steam supply and exhaust are within the scope of these systems. Valves in the feedwater line are not considered within the scope of these systems. The emergency generator dedicated to providing AC power to the high-pressure core spray system is included in the scope of the HPCS. The HPCS system typically includes a "water leg" pump to prevent water hammer in the HPCS piping to the reactor vessel. The "water leg" pump and valves in the "water leg" pump flow path are ancillary components and are not included in the scope of the HPCS system. Unavailability is not included while critical if the system is below steam pressure specified in technical specifications at which the system can be operated.

Train Determination

The HPCI and HPCS systems are considered single-train systems. The booster pump and other small pumps are ancillary components not used in determining the number of trains. The effect of these pumps on system performance is included in the system indicator to the extent their failure detracts from the ability of the system to perform its risk-significant function. For the FWCI system, the number of trains is determined by the number of feedwater pumps. The number of condensate and feedwater booster pumps are not used to determine the number of trains.

BWR Heat Removal Systems
(Reactor Core Isolation Cooling or Isolation Condenser)

Scope

This system functions at high pressure to remove decay heat following a loss of main feedwater event. The RCIC system also functions to maintain reactor coolant inventory following a very small LOCA event.

The function monitored for the indicator is the ability of the RCIC system to cool the reactor vessel core and provide makeup water by taking a suction from either the condensate storage tank or the suppression pool and injecting at rated pressure and flow into the reactor vessel.

The Reactor Core Isolation Cooling (RCIC) system turbine, governor, and associated piping and valves for steam supply and exhaust are within the scope of the RCIC system. Valves in the feedwater line are not considered within the scope of the RCIC system. The Isolation Condenser and inlet valves are within the scope of Isolation Condenser system. Unavailability is not included while critical if the system is below steam pressure specified in technical specifications at which the system can be operated.

Train Determination

The RCIC system is considered a single-train system. The condensate and vacuum pumps are ancillary components not used in determining the number of trains. The effect of these pumps on RCIC performance is included in the system indicator to the extent that a component failure results in an inability of the system to perform its risk-significant function.

BWR Residual Heat Removal Systems

Scope

The functions monitored for the BWR residual heat removal (RHR) system are the ability of the RHR system to remove heat from the suppression pool, provide low pressure coolant injection, and provide post-accident decay heat removal. The pumps, heat exchangers, and associated piping and valves for those functions are included in the scope of the RHR system.

Train Determination

The number of trains in the RHR system is determined by the number of parallel RHR heat exchangers.

PWR High Pressure Safety Injection Systems

Scope

These systems are used primarily to maintain reactor coolant inventory at high pressures following a loss of reactor coolant. HPSI system operation following a small-break LOCA involves transferring an initial supply of water from the refueling water storage tank (RWST) to cold leg piping of the reactor coolant system. Once the RWST inventory is depleted, recirculation of water from the reactor building emergency sump is required. The function monitored for HPSI is the ability of a HPSI train to take a suction from the primary water source (typically, a borated water tank), or from the containment emergency sump, and inject into the reactor coolant system at rated flow and pressure.

The scope includes the pumps and associated piping and valves from both the refueling water storage tank and from the containment sump to the pumps, and from the pumps into the reactor coolant system piping. For plants where the high-pressure injection pump takes suction from the residual heat removal pumps, the residual heat removal pump discharge header isolation valve to the HPSI pump suction is included in the scope of HPSI system. Some components may be included in the scope of more than one train. For example, cold-leg injection lines may be fed from a common header that is supplied by both HPSI trains. In these cases, the effects of testing or component failures in an injection line should be reported in both trains.

Train Determination

In general, the number of HPSI system trains is defined by the number of high head injection paths that provide cold-leg and/or hot-leg injection capability, as applicable.

For Babcock and Wilcox (B&W) reactors, the design features centrifugal pumps used for high pressure injection (about 2,500 psig) and no hot-leg injection path. Recirculation from the containment sump requires operation of pumps in the residual heat removal system. They are typically a two-train system, with an installed spare pump (depending on plant-specific design) that can be aligned to either train.

For two-loop Westinghouse plants, the pumps operate at a lower pressure (about 1600 psig) and there may be a hot-leg injection path in addition to a cold-leg injection path (both are included as a part of the train).

For Combustion Engineering (CE) plants, the design features three centrifugal pumps that operate at intermediate pressure (about 1300 psig) and provide flow to two cold-leg injection paths or two hot-leg injection paths. In most designs, the HPSI pumps take suction directly from the containment sump for recirculation. In these cases, the sump suction valves are included within the scope of the HPSI system. This is a two-train system (two trains of combined cold-leg and hot-leg injection capability). One of the three pumps is typically an installed spare that can be aligned to either train or only to one of the trains (depending on plant-specific design).

For Westinghouse three-loop plants, the design features three centrifugal pumps that operate at high pressure (about 2500 psig), a cold-leg injection path through the BIT (with two trains of redundant valves), an alternate cold-leg injection path, and two hot-leg injection paths. One of the pumps is considered an installed spare. Recirculation is provided by taking suction from the RHR pump discharges. A train consists of a pump, the pump suction valves and boron injection tank (BIT) injection line valves electrically associated with the pump, and the associated hot-leg injection path. The alternate cold-leg injection path is required for recirculation, and should be included in the train with which its isolation valve is electrically associated. This represents a two-train HPSI system.

For Four-loop Westinghouse plants, the design features two centrifugal pumps that operate at high pressure (about 2500 psig), two centrifugal pumps that operate at an intermediate pressure (about 1600 psig), a BIT injection path (with two trains of injection valves), a cold-leg safety injection path, and two hot-leg injection paths. Recirculation is provided by taking suction from the RHR pump discharges. Each of two high pressure trains is comprised of a high pressure centrifugal pump, the pump suction valves and BIT valves that are electrically associated with the pump. Each of two intermediate pressure trains is comprised of the safety injection pump, the suction valves and the hot-leg injection valves electrically associated with the pump. The cold-leg safety injection path can be fed with either safety injection pump, thus it should be associated with both intermediate pressure trains. This HPSI system is considered a four-train system for monitoring purposes.

PWR Auxiliary Feedwater Systems

Scope

The AFW system provides decay heat removal via the steam generators to cool down and depressurize the reactor coolant system following a reactor trip. The AFW system is assumed to be required for an extended period of operation during which the initial supply of water from the condensate storage tank is depleted and water from an alternative water source (e.g., the service water system) is required. Therefore components in the flow paths from both of these water sources are included; however, the alternative water source (e.g., service water system) is not included.

The function monitored for the indicator is the ability of the AFW system to take a suction from the primary water source (typically, the condensate storage tank) or, if required, from an emergency source (typically, a lake or river via the service water system) and inject into at least one steam generator at rated flow and pressure.

The scope of the auxiliary feedwater (AFW) or emergency feedwater (EFW) systems includes the pumps and the components in the flow paths from the condensate storage tank and, if required, the valve(s) that connect the alternative water source to the auxiliary feedwater system. Startup feedwater pumps are not included in the scope of this indicator.

<u>Train Determination</u>

The number of trains is determined primarily by the number of parallel pumps. For example, a system with three pumps is defined as a three-train system, whether it feeds two, three, or four injection lines, and regardless of the flow capacity of the pumps. Some components may be included in the scope of more than one train. For example, one set of flow regulating valves and isolation valves in a three-pump, two-steam generator system are included in the motor-driven pump train with which they are electrically associated, but they are also included (along with the redundant set of valves) in the turbine-driven pump train. In these instances, the effects of testing or failure of the valves should be reported in both affected trains. Similarly, when two trains provide flow to a common header, the effect of isolation or flow regulating valve failures in paths connected to the header should be considered in both trains.

PWR Residual Heat Removal System

<u>Scope</u>

The functions monitored for the PWR residual heat removal (RHR) system are those that are required to be available when the reactor is critical. These typically include the low-pressure injection function ~~(if risk-significant)~~ and the post-accident recirculation mode used to cool and recirculate water from the containment sump following depletion of RWST inventory to provide post-accident decay heat removal. The pumps, heat exchangers, and associated piping and valves for those functions are included in the scope of the RHR system. Containment spray function should be included if it is identified ~~in the PRA~~ as a risk-significant post accident decay heat removal function. Containment spray systems that only provide containment pressure control are not included.

<u>Train Determination</u>

The number of trains in the RHR system is determined by the number of parallel RHR heat exchangers. Some components are used to provide more than one function of RHR. If a component cannot perform as designed, rendering its associated train incapable of meeting one of the risk-significant functions, then the train is considered to be failed. Unavailable hours would be reported as a result of the component failure.

Cooling Water Support System

Scope

The function of the cooling water support system is to provide for direct cooling of the components in the other monitored systems. It does not include indirect cooling provided by room coolers or other HVAC features.

Systems that provide this function typically include service water and component cooling water or their cooling water equivalents. Pumps, valves, heat exchangers and line segments that are necessary to provide cooling to the other monitored systems are included in the system scope up to, but not including, the last valve that connects the cooling water support system to the other monitored systems. This last valve is included in the other monitored system boundary.

Valves in the cooling water support system that must close to ensure sufficient cooling to the other monitored system components to meet risk significant functions are included in the system boundary.

Train Determination

The number of trains in the Cooling Water Support System will vary considerably from plant to plant. The way these functions are modeled in the plant-specific PRA will determine a logical approach for train determination. For example, if the PRA modeled separate pump and line segments, then the number of pumps and line segments would be the number of trains.

Clarifying Notes

Service water pump strainers and traveling screens are not considered to be active components and are therefore not part of URI. However, clogging of strainers and screens due to expected or routinely predictable environmental conditions that render the train unavailable to perform its risk significant cooling function (which includes the risk-significant mission times)are included in UAI.

Unpredictable extreme environmental conditions that render the train unavailable to perform its risk significant cooling function should be addressed through the FAQ process to determine if resulting unavailability should be included in UAI.

Attachment 2
RIS 2002-14

NEI 99-02, Appendix F, “ Methodologies For Computing the Unavailability Index, the Unreliability Index and Determining Performance Index Validity” (Draft).

APPENDIX F

METHODOLOGIES FOR COMPUTING THE UNAVAILABILITY INDEX, THE UNRELIABILITY INDEX AND DETERMINING PERFORMANCE INDEX VALIDITY

This appendix provides the details of three calculations, calculation of the System Unavailability Index, the System Unreliability Index, and the criteria for determining when the Mitigating System Performance Index is unsuitable for use as a performance index.

System Unavailability Index (UAI) Due to Changes in Train Unavailability

Calculation of System UAI due to changes in train unavailability is as follows:

$$UAI = \sum_{j=1}^{n} UAI_{tj} \qquad \text{Eq. 1}$$

where the summation is over the number of trains (n) and UAI_t is the unavailability index for a train.

Calculation of UAI_t for each train due to changes in train unavailability is as follows:

$$UAI_t = CDF_p \left[\frac{FV_{UAp}}{UA_p} \right]_{\max} (UA_t - UA_{BLt}), \qquad \text{Eq. 2}$$

where:

CDF_p is the plant-specific, internal events, at power Core Damage Frequency,

FV_{UAp} is the train-specific Fussell-Vesely value for unavailability,

UA_P is the plant-specific PRA value of unavailability for the train,

UA_t is the actual unavailability of train t, defined as:

$$UA_t = \frac{\text{Unavailable hours during the previous 12 quarters while critical}}{\text{Critical hours during the previous 12 quarters}}$$

and,

UA_{BLt} is the historical baseline unavailability value for the train determined as described below.

UA_{BLt} is the sum of two elements: planned and unplanned unavailability. Planned unavailability is the actual, plant-specific three-year total planned unavailability for the train for the years 1999 through 2001 (see clarifying notes for details). This period is chosen as the most representative of how the plant intends to perform routine maintenance and surveillances at power. Unplanned unavailability is the historical industry average for unplanned unavailability for the years 1999 through 2001. See Table 1 for historical train values for unplanned unavailability.

Calculation of the quantity inside the square bracket in equation 2 will be discussed at the end of the next section. See clarifying notes for calculation of UAI for cooling water support system.

System Unreliability Index (URI) Due to Changes in Component Unreliability

Unreliability is monitored at the component level and calculated at the system level.

Calculation of system URI due to changes in component unreliability is as follows:

$$URI = CDF_p \sum_{j=1}^{m} \left[\frac{FV_{URcj}}{UR_{pcj}} \right]_{\max} (UR_{Bcj} - UR_{BLcj}) \qquad \text{Eq. 3}$$

Where the summation is over the number of active components (m) in the system, and:

CDF_p is the plant-specific internal events, at power, core damage frequency,

FV_{URc} is the component-specific Fussell-Vesely value for unreliability,

UR_{Pc} is the plant-specific PRA value of component unreliability,

UR_{Bc} is the Bayesian corrected component unreliability for the previous 12 quarters,

and

UR_{BLc} is the historical industry baseline calculated from unreliability mean values for each monitored component in the system. The calculation is performed in a manner similar to equation 4 below using the industry average values in Table 2.

Calculation of the quantity inside the square bracket in equation 3 will be discussed at the end of this section.

Component unreliability is calculated as follows.

$$UR_{Bc} = P_D + \lambda T_m \qquad \text{Eq 4}$$

where:

P_D is the component failure on demand probability calculated based on data collected during the previous 12 quarters,

λ is the component failure rate (per hour) for failure to run calculated based on data collected during the previous 12 quarters,

and

T_m is the risk-significant mission time for the component based on plant specific PRA model assumptions. ~~Add acceptable methodologies for determining mission time.~~

NOTE:

For valves only the P_D term applies

For pumps $P_D + \lambda\, T_m$ applies

For diesels $P_{D\,start} + P_{D\,load\,run} + \lambda\, T_m$ applies

The first term on the right side of equation 4 is calculated as follows.[1]

$$P_D = \frac{(N_d + a)}{(a + b + D)} \qquad \text{Eq. 5}$$

where:

N_d is the total number of failures on demand during the previous 12 quarters,

D is the total number of demands during the previous 12 quarters (actual ESF demands plus estimated test and estimated operational/alignment demands. An update to the estimated demands is required if a change to the basis for the estimated demands results in a >25% change in the estimate),

and

a and b are parameters of the industry prior, derived from industry experience (see Table 2).

In the calculation of equation 5 the numbers of demands and failures is the sum of all demands and failures for similar components within each system. Do not sum across units for a multi-unit plant. For example, for a plant with two trains of Emergency Diesel Generators, the demands and failures for both trains would be added together for one evaluation of P_D which would be used for both trains of EDGs.

In the second term on the right side of equation 4, λ is calculated as follows.

$$\lambda = \frac{(N_r + a)}{(T_r + b)} \qquad \text{Eq. 6}$$

where:

N_r is the total number of failures to run during the previous 12 quarters,

T_r is the total number of run hours during the previous 12 quarters (actual ESF run hours plus estimated test and estimated operational/alignment run hours. An update to the estimated run hours is required if a change to the basis for the estimated hours results in a >25% change in the estimate).

and

[1] Atwood, Corwin L., Constrained noninformative priors in risk assessment, *Reliability Engineering and System Safety*, 53 (1996; 37-46)

a and *b* are parameters of the industry prior, derived from industry experience (see Table 2).

In the calculation of equation 6 the numbers of demands and run hours is the sum of all run hours and failures for similar components within each system. Do not sum across units for a multi-unit plant. For example, a plant with two trains of Emergency Diesel Generators, the run hours and failures for both trains would be added together for one evaluation of λ which would be used for both trains of EDGs.

<u>Fussell-Vesely, Unavailability and Unreliability</u>

Equations 2 and 3 include a term that is the ratio of a Fussell-Vesely importance value divided by the related unreliability or unavailability. Calculation of these quantities is generally complex, but in the specific application used here, can be greatly simplified.

The simplifying feature of this application is that only those components (or the associated basic events) that can fail a train are included in the performance index. Components within a train that can each fail the train are logically equivalent and the ratio FV/UR is a constant value for any basic event in that train. It can also be shown that for a given component or train represented by multiple basic events, the ratio of the two values for the component or train is equal to the ratio of values for any basic event within the train. Or:

$$\frac{FV_{be}}{UR_{be}} = \frac{FV_{URc}}{UR_{Pc}} = \frac{FV_{t}}{UR_{t}} = \text{Constant}$$

and

$$\frac{FV_{be}}{UA_{be}} = \frac{FV_{UAp}}{UA_{p}} = \text{Constant}$$

Note that the constant value may be different for the unreliability ratio and the unavailability ratio because the two types of events are frequently not logically equivalent. For example recovery actions may be modeled in the PRA for one but not the other.

Thus, the process for determining the value of this ratio for any component or train is to identify a basic event that fails the component or train, determine the failure probability or unavailability for the event, determine the associated FV value for the event and then calculate the ratio. Use the basic event in the component or train with the largest failure probability (hence the maximum notation on the bracket) to minimize the effects of truncation on the calculation. Exclude common cause events, which are not within the scope of this performance index

Some systems have multiple modes of operation, such as PWR HPSI systems that operate in injection as well as recirculation modes. In these systems all active components are not logically equivalent, unavailability of the pump fails all operating modes while unavailability of the sump suction valves only fails the recirculation mode. In cases such as these, if unavailability events exist separately for the components within a train, the appropriate ratio to use is the maximum.

Determination of systems for which the performance index is not valid

The performance index relies on the existing testing programs as the source of the data that is input to the calculations. Thus, the number of demands in the monitoring period is based on the frequency of testing required by the current test programs. In most cases this will provide a sufficient number of demands to result in a valid statistical result. However, in some cases, the number of demands will be insufficient to resolve the change in the performance index (1.0×10^{-6}) that corresponds to movement from a green performance to a white performance level. In these cases, one failure is the difference between baseline performance and performance in the white performance band. The performance index is not suitable for monitoring such systems and monitoring is performed through the inspection process.

This section will define the method to be used to identify systems for which the performance index is not valid, and will not be used.

The criteria to be used to identify an invalid performance index is:

> If, for any failure mode for any component in a system, the risk increase (ΔCDF) associated with the change in unreliability resulting from single failure is larger than 1.0×10^{-6}, then the performance index will be considered invalid for that system.

The increase in risk associated with a component failure is the sum of the contribution from the decrease in calculated reliability as a result of the failure and the decrease in availability resulting from the time required to affect the repair of the failed component. The change in CDF that results from a demand type failure is given by:

$$MSPI = CDF_p \times \sum_{N\ similar\ comp} \left\{ \frac{FV_{URc}}{UR_{pc}} \times \frac{1}{a+b+D} \right\} + CDF_p \times \frac{FV_{UAp}}{UA_p} \times \frac{T_{Mean\ \mathrm{Repair}}}{T_{CR}} \qquad \text{Eq. 7}$$

Likewise, the change in CDF per run type failure is given by:

$$MSPI = CDF_p \times \sum_{N\ similar\ comp} \left\{ \frac{FV_{URc}}{UR_{pc}} \times \frac{T_m}{b+T_r} \right\} + CDF_p \times \frac{FV_{UAp}}{UA_p} \times \frac{T_{\mathrm{Mean\ Repair}}}{T_{CR}} \qquad \text{Eq. 8}$$

In these expressions, the variables are as defined earlier and additionally

T_{MR} is the mean time to repair for the component

and

T_{CR} is the number of critical hours in the monitoring period.

The summation in the equations is taken over all similar components within a system. With multiple components of a given type in one system, the impact of the failure on CDF is included in the increased unavailability of all components of that type due to pooling the demand and failure data.

The mean time to repair can be estimate as one-half the Technical Specification Allowed Outage Time for the component and the number of critical hours should correspond to the 1999 – 2001 actual number of critical hours.

These equations are be used for all failure modes for each component in a system. If the resulting value of ΔCDF is greater than 1.0×10^{-6} for any failure mode of any component, then the performance index for that system is not considered valid.

Definitions

Train Unavailability: Train unavailability is the ratio of the hours the train was unavailable to perform its risk-significant functions due to planned or unplanned maintenance or test during the previous 12 quarters while critical to the number of critical hours during the previous 12 quarters. (Fault exposure hours are not included; unavailable hours are counted only for the time required to recover the train's risk-significant functions.)

Train unavailable hours: The hours the train was not able to perform its risk significant function due to maintenance, testing, equipment modification, electively removed from service, corrective maintenance, or the elapsed time between the discovery and the restoration to service of an equipment failure or human error that makes the train unavailable (such as a misalignment) while the reactor is critical.

Fussell-Vesely (FV) Importance:

The Fussell-Vesely importance for a feature (component, sub-system, train, etc.) of a system is representative of the fractional contribution that feature makes to the to the total risk of the system.

The Fussell-Vesely importance of a basic event or group of basic events that represent a feature of a system is represented by:

$$FV = 1 - \frac{R_i}{R_0}$$

Where:

R_0 is the base (reference) case overall model risk,

R_i is the decreased risk level with feature *i* completely reliable.

In this expression, the second term on the right represents the fraction of the reference risk remaining assuming the feature of interest is perfect. Thus 1 minus the second term is the fraction of the reference risk attributed to the feature of interest.

The Fussell-Vesely importance is calculated according to the following equation:

$$FV = 1 - \frac{\bigcup_{j=1,n} C_{i\,j}}{\bigcup_{j=1,m} C_{0\,j}},$$

where the denominator represents the union of m minimal cutsets C_0 generated with the reference (baseline) model, and the numerator represents the union of n minimal cutsets C_i generated assuming events related to the feature are perfectly reliable, or their failure probability is False.

Critical hours: The number of hours the reactor was critical during a specified period of time.

Component Unreliability: Component unreliability is the probability that the component would not perform its risk-significant functions when called upon during the previous 12 quarters.

Active Component: A component whose failure to change state renders the train incapable of performing its risk-significant functions. In addition, all pumps and diesels in the monitored systems are included as active components. (See clarifying notes.)

Manual Valve: A valve that can only be operated by a person. An MOV or AOV that is remotely operated by a person may be an active component.

Start demand: Any demand for the component to successfully start to perform its risk-significant functions, actual or test. (Exclude post maintenance tests, unless in case of a failure the cause of failure was independent of the maintenance performed.)

Post maintenance tests: Tests performed following maintenance but prior to declaring the train/component operable, consistent with Maintenance Rule implementation.

Run demand: Any demand for the component, given that it has successfully started, to run/operate for its mission time to perform its risk-significant functions. (Exclude post maintenance tests, unless in case of a failure the cause of failure was independent of the maintenance performed.)

EDG failure to start: A failure to start includes those failures up to the point the EDG has achieved rated speed and voltage. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

EDG failure to load/run: Given that it has successfully started, a failure of the EDG output breaker to close, loads successfully sequence and to run/operate for one hour to perform its risk-significant functions. This failure mode is treated as a demand failure for calculation purposes. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

EDG failure to run: Given that it has successfully started and loaded and run for an hour, a failure of an EDG to run/operate.~~ for its mission time to perform its risk-significant functions.~~ (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

Pump failure on demand: A failure to start and run for at least one hour is counted as failure on demand. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

Pump failure to run: Given that it has successfully started and run for an hour, a failure of a pump to run/operate.~~ for its mission time to perform its risk-significant functions.~~ (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

Valve failure on demand: A failure to open or close is counted as failure on demand. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

Clarifying Notes

Train Boundaries and Unavailable Hours

Include all components that are required to satisfy the risk-significant function of the train. For example, high-pressure injection may have both an injection mode with suction from the refueling water storage tank and a recirculation mode with suction from the containment sump. Some components may be included in the scope of more than one train. For example, one set of flow regulating valves and isolation valves in a three-pump, two-steam generator system are included in the motor-driven pump train with which they are electrically associated, but they are also included (along with the redundant set of valves) in the turbine-driven pump train. In these instances, the effects of unavailability of the valves should be reported in both affected trains. Similarly, when two trains provide flow to a common header, the effect of isolation or flow regulating valve failures in paths connected to the header should be considered in both trains

Cooling Water Support System Trains

The number of trains in the Cooling Water Support System will vary considerably from plant to plant. The way these functions are modeled in the plant-specific PRA will determine a logical approach for train determination. For example, if the PRA modeled separate pump and line segments, then the number of pumps and line segments would be the number of trains. A separate value for UAI and URI will be calculated for each of the systems in this indicator and then they will be added together to calculate the MSPI.

Active Components

For unreliability, use the following criteria for determining those components that should be monitored:

- Components that are normally running or have to change state to achieve the risk significant function will be included in the performance index. Active failures of check valves and manual valves are excluded from the performance index and will be evaluated in the NRC inspection program.
- Redundant valves within a train are not included in the performance index. Only those valves whose failure alone can fail a train will be included. The PRA success criteria are to be used to identify these valves.
- Redundant valves within a multi-train system, whether in series or parallel, where the failure of both valves would prevent all trains in the system from performing a risk-significant function are included. (See Figure F-5)
- All pumps and diesels are included in the performance index

Table 3 defines the boundaries of components, and Figures F-1, F-2, F-3 and F-4 provide examples of typical component boundaries as described in Table 3. Each plant will determine their system boundaries, active components, and support components, and have them available for NRC inspection.

Failures of Non-Active Components

Failures of SSC's that are not included in the performance index will not be counted as a failure or a demand. Failures of SSC's that cause an SSC within the scope of the performance index to fail will not be counted as a failure or demand. An example could be a manual suction isolation valve left closed which causes a pump to fail. This would not be counted as a failure of the pump. Any mispositioning of the valve that caused the train to be unavailable would be counted as unavailability from the time of discovery. The significance of the mispositioned valve prior to discovery would be addressed through the inspection process.

Baseline Values

The baseline values for unreliability are contained in Table 2 and remain fixed.

The baseline values for unavailability include both plant-specific planned unavailability values and unplanned unavailability values. The unplanned unavailability values are contained in Table 1 and remain fixed. They are based on ROP PI industry data from 1999 through 2001. (Most baseline data used in PIs come from the 1995-1997 time period. However, in this case, the 1999-2001 ROP data are preferable, because the ROP data breaks out systems separately (some of the industry 1995-1997 INPO data combine systems, such as HPCI and RCIC, and do not include PWR RHR). It is important to note that the data for the two periods is very similar.)

Support cooling baseline data is based on plant specific maintenance rule ~~unplanned and planned~~ unavailability for years 1999 to 2001. (Maintenance rule data does not distinguish between planned and unplanned unavailability. There is no ROP support cooling data.)

The baseline planned unavailability is based on actual plant-specific values for the period 1999 through 2001. These values are expected to remain fixed unless the plant maintenance philosophy is substantially changed with respect to on-line maintenance or preventive maintenance. In these cases, the planned unavailability baseline value can be adjusted. A comment should be placed in the comment field of the quarterly report to identify a substantial change in planned unavailability. To determine the planned unavailability:

1. Record the total train unavailable hours reported under the Reactor Oversight Process for 1999 through 2001.
2. Subtract any fault exposure hours still included in the 1999-2001 period.
3. Subtract unplanned unavailable hours
4. Add any on-line overhaul hours and any other planned unavailability excluded in accordance with NEI 99-02. [2]
5. Add any planned unavailable hours for functions monitored under MSPI which were not monitored under SSU in NEI 99-02.
6. Subtract any unavailable hours reported when the reactor was not critical.
7. Subtract hours cascaded onto monitored systems by support systems.
8. Divide the hours derived from steps 1-6 above by the total critical hours during 1999-2001. This is the baseline planned unavailability

Baseline unavailability is the sum of planned unavailability from step 7 and unplanned unavailability from Table 1.

[2] Note: The plant-specific PRA should model significant on-line overhaul hours.

Table 1. Historical Unplanned Maintenance Unavailability Train Values

(Based on ROP Industrywide Data for 1999 through 2001)

SYSTEM	UNPLANNED UNAVAILABILITY/TRAIN
EAC	1.7 E-03
PWR HPSI	6.1 E-04
PWR AFW (TD)	9.1 E-04
PWR AFW (MD)	6.9 E-04
PWR AFW (DieselD)	7.6 E-04
PWR (except CE) RHR	4.2 E-04
CE RHR	1.1 E-03
BWR HPCI	3.3 E-03
BWR HPCS	5.4 E-04
BWR RCIC	2.9 E-03
BWR RHR	1.2 E-03
Support Cooling	~~No Data Available~~ Use plant specific Maintenance Rule data for 1999-2001

Table 2. Industry Priors and Parameters for Unreliability

Component	Failure Mode	a [a]	b [a]	Industry Mean Value [b]	Source(s)
Motor-operated valve	Fail to open (or close)	5.0E-1	2.4E+2	2.1E-3	NUREG/CR-5500, Vol. 4,7,8,9
Air-operated valve	Fail to open (or close)	5.0E-1	2.5E+2	2.0E-3	NUREG/CR-4550, Vol. 1
Motor-driven pump, standby	Fail to start	5.0E-1	2.4E+2	2.1E-3	NUREG/CR-5500, Vol. 1,8,9
	Fail to run	5.0E-1	5.0E+3h	1.0E-4/h	NUREG/CR-5500, Vol. 1,8,9
Motor-driven pump, running or alternating	Fail to start	4.9E-1	1.6E+2	3.0E-3	NUREG/CR-4550, Vol. 1
	Fail to run	5.0E-1	1.7E+4h	3.0E-5/h	NUREG/CR-4550, Vol. 1
Turbine-driven pump, AFWS	Fail to start	4.7E-1	2.4E+1	1.9E-2	NUREG/CR-5500, Vol. 1
	Fail to run	5.0E-1	3.1E+2	1.6E-3/h	NUREG/CR-5500, Vol. 1
Turbine-driven pump, HPCI or RCIC	Fail to start	4.6E-1	1.7E+1	2.7E-2	NUREG/CR-5500, Vol. 4,7
	Fail to run	5.0E-1	3.1E+2h	1.6E-3/h	NUREG/CR-5500, Vol. 1,4,7
Diesel-driven pump, AFWS	Fail to start	4.7E-1	2.4E+1	1.9E-2	NUREG/CR-5500, Vol. 1
	Fail to run	5.0E-1	6.3E+2h	8.0E-4/h	NUREG/CR-4550, Vol. 1
Emergency diesel generator	Fail to start	4.8E-1	4.3E+1	1.1E-2	NUREG/CR-5500, Vol. 5
	Fail to load/run	5.0E-1	2.9E+2	1.7E-3 [c]	NUREG/CR-5500, Vol. 5
	Fail to run	5.0E-1	2.2E+3h	2.3E-4/h	NUREG/CR-5500, Vol. 5

a. A constrained, non-informative prior is assumed. For failure to run events, a = 0.5 and b = (a)/(mean rate). For failure upon demand events, a is a function of the mean probability:

Mean Probability	a
0.0 to 0.0025	0.50
>0.0025 to 0.010	0.49
>0.010 to 0.016	0.48
>0.016 to 0.023	0.47
>0.023 to 0.027	0.46

Then b = (a)(1.0 - mean probability)/(mean probability).

b. Failure to run events occurring within the first hour of operation are included within the fail to start failure mode. Failure to run events occurring after the first hour of operation are included within the fail to run failure mode. Unless otherwise noted, the mean failure probabilities and rates include the probability of non-recovery. Types of allowable recovery are outlined in the clarifying notes, under “Credit for Recovery Actions.”

c. Fail to load and run for one hour was calculated from the failure to run data in the report indicated. The failure rate for 0.0 to 0.5 hour (3.3E-3/h) multiplied by 0.5 hour, was added to the failure rate for 0.5 to 14 hours (2.3E-4/h) multiplied by 0.5 hour.

Table 3. Component Boundary Definition

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 receiver, exhaust and combustion air system, dedicated diesel battery (which is not part of the normal DC distribution 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, and breaker closure interlocks) .
Motor-Driven 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, turbo-pump seal, cooling components, and local turbine control system (speed).
Motor-Operated Valves	The valve boundary inc1udes the valve body, motor/actuator, the voltage supply breaker (both motive and control power) 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).

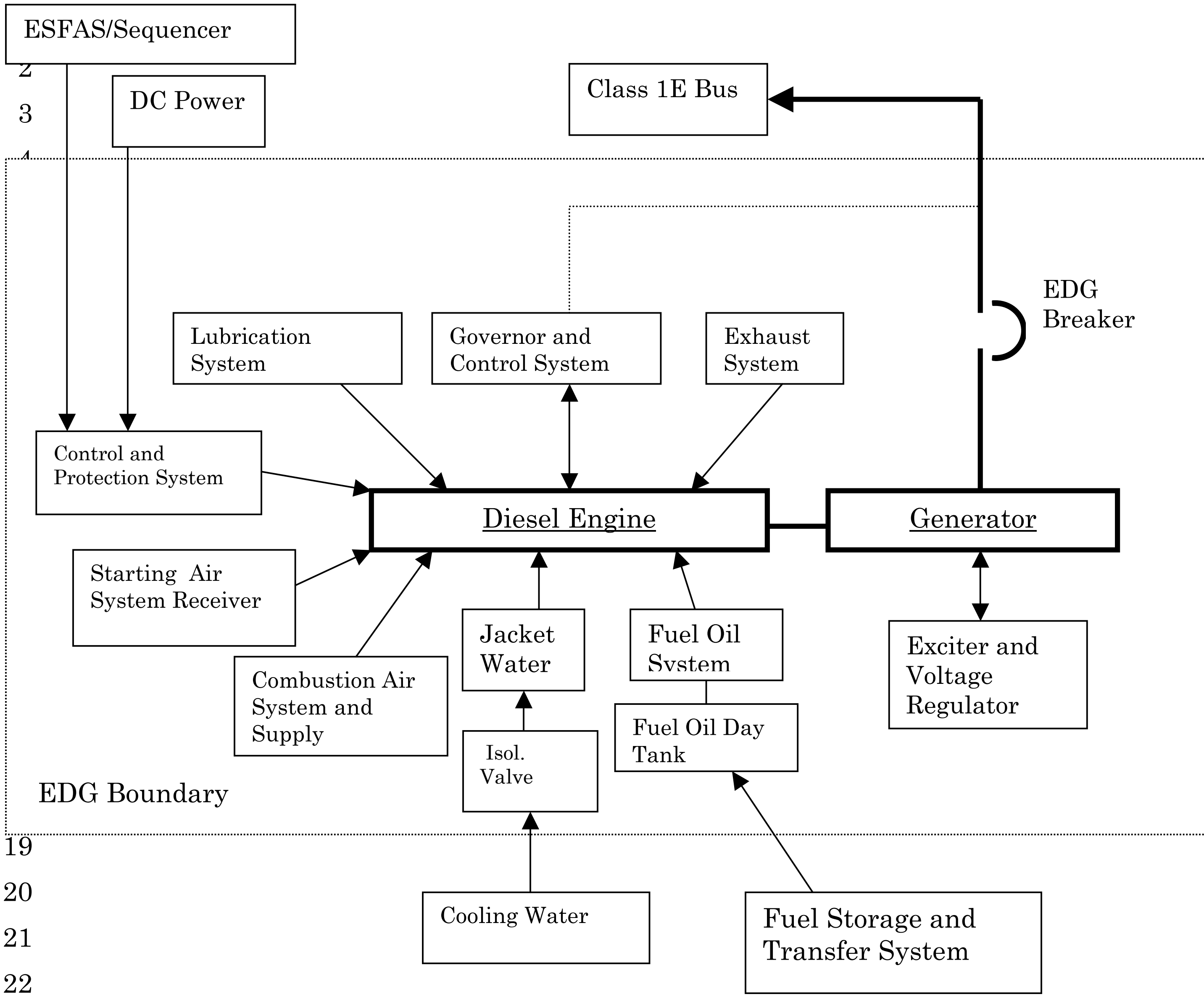
ESFAS/Sequencer
DC Power
Class 1E Bus
EDG Breaker
Lubrication System
Governor and Control System
Exhaust System
Control and Protection System
Diesel Engine
Generator
Starting Air System Receiver
Combustion Air System and Supply
Jacket Water
Fuel Oil System
Exciter and Voltage Regulator
Fuel Oil Day Tank
Isol. Valve
EDG Boundary
Cooling Water
Fuel Storage and Transfer System

Figure F-1

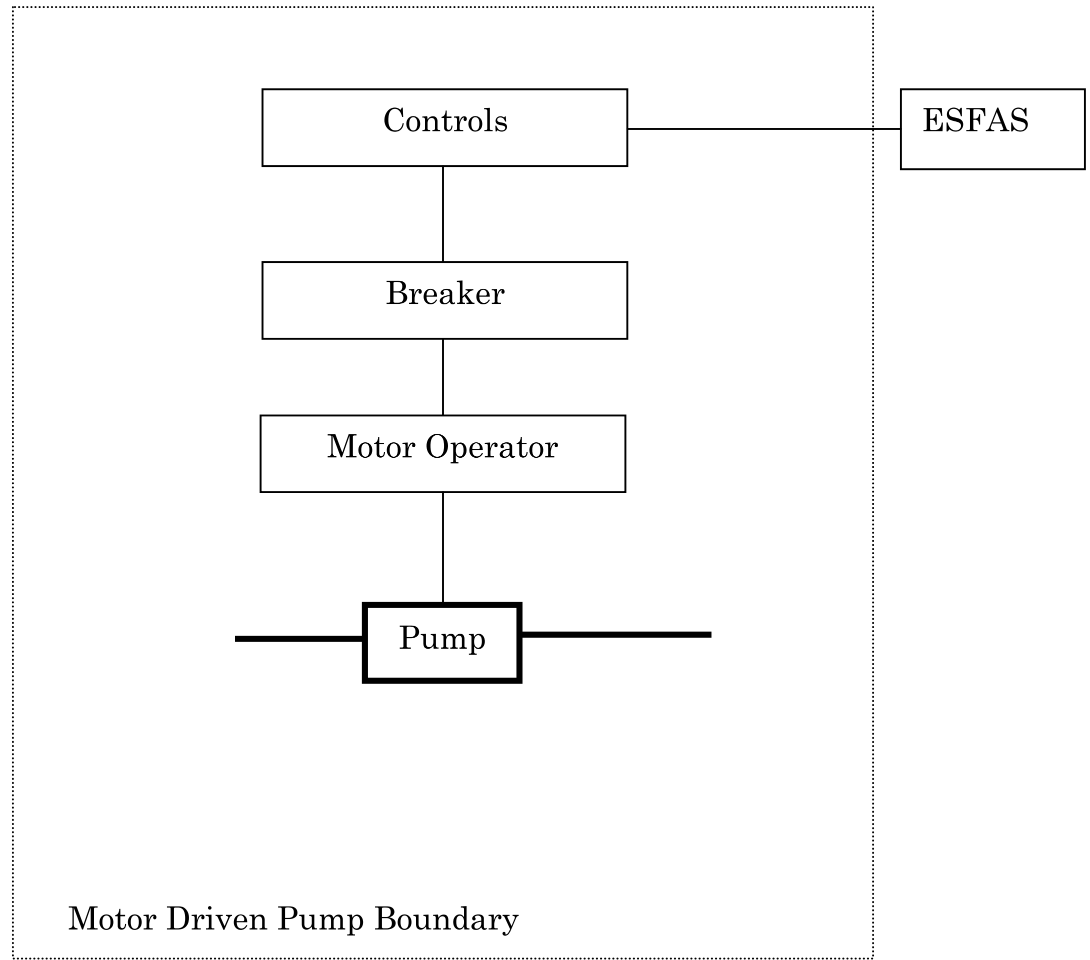
Controls
ESFAS
Breaker
Motor Operator
Pump
Motor Driven Pump Boundary

Figure F-2

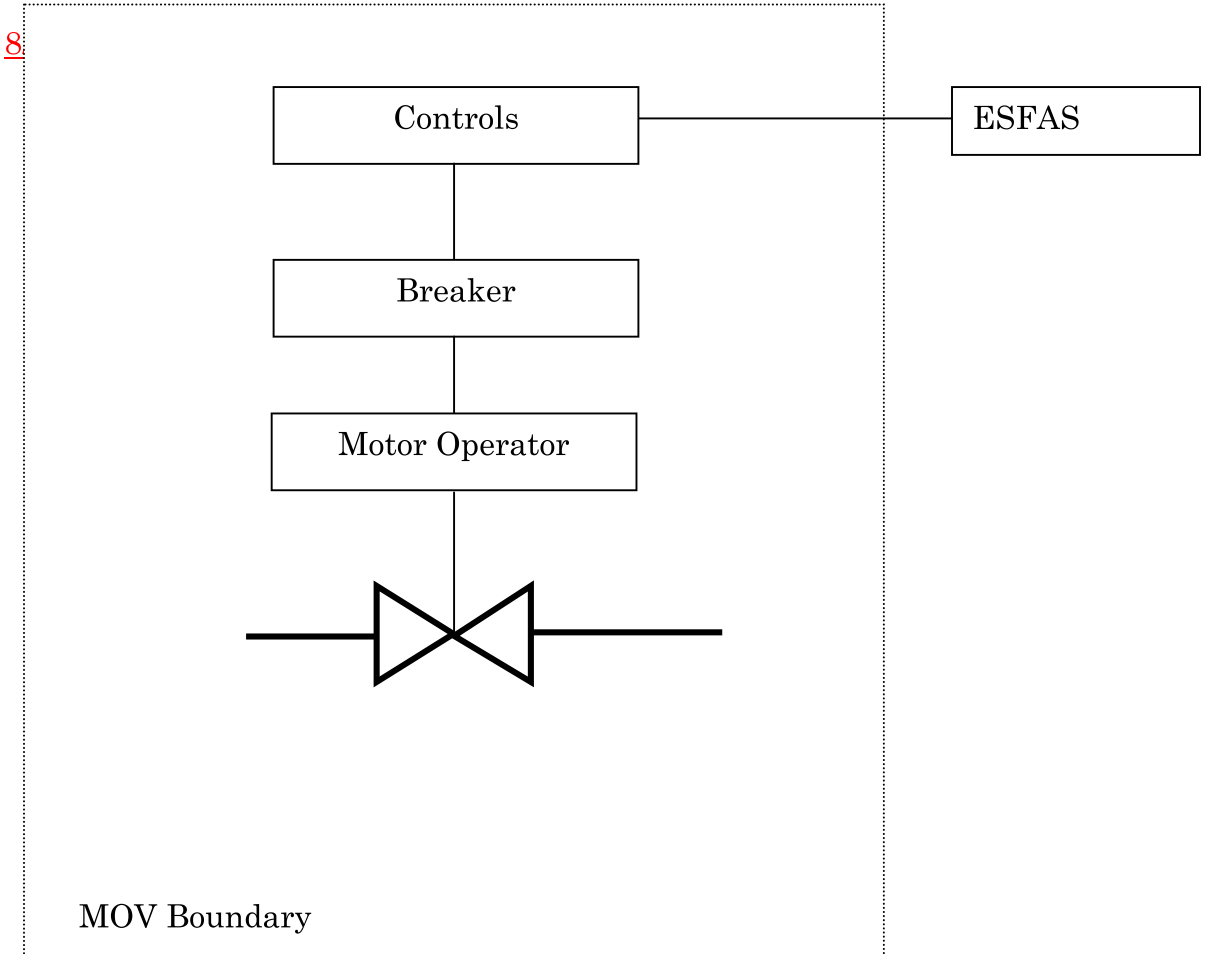

Figure F-3

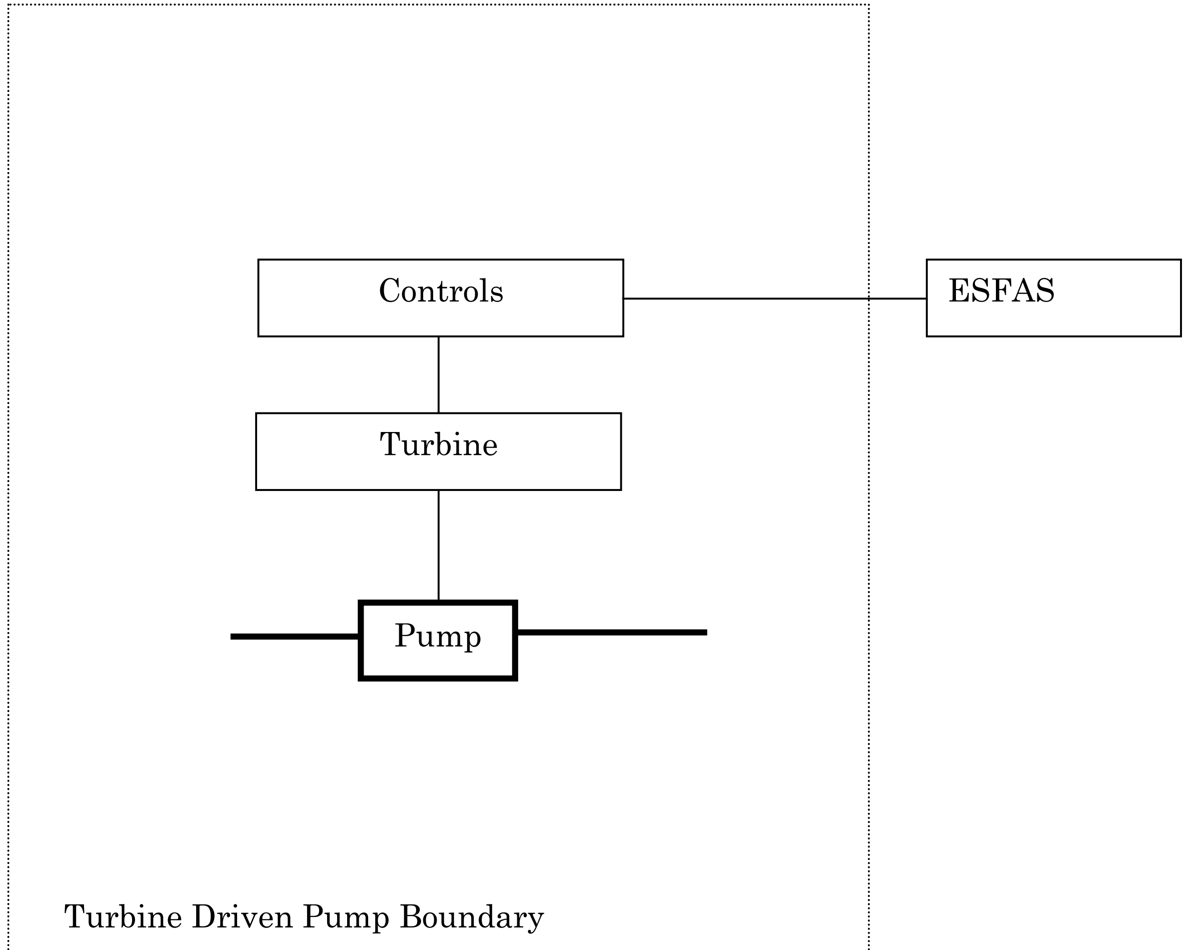

Figure F-4

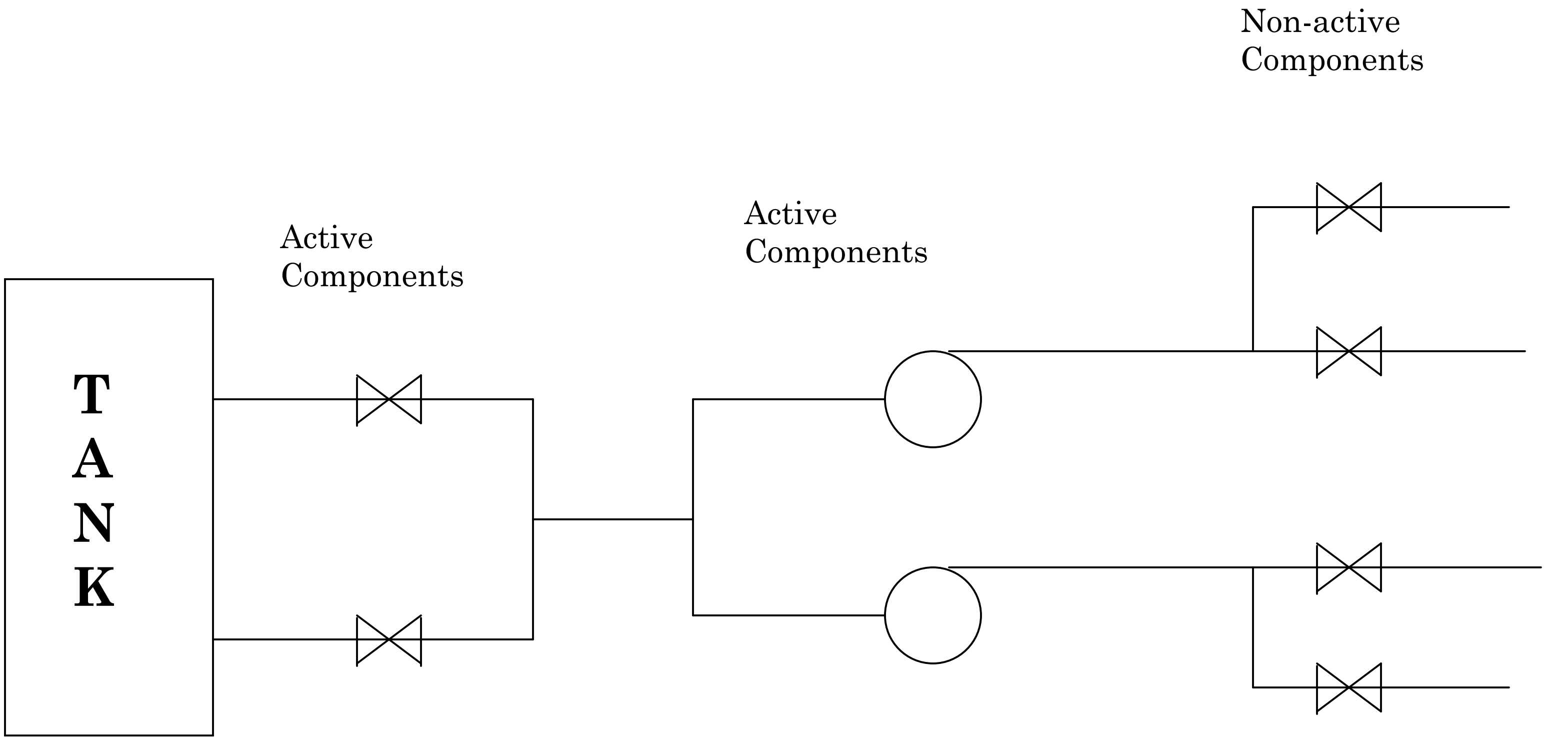
Non-active
Components
Active
Components
Active
Components
T
A
N
K

Figure F-5