Attachment 4

# APPENDIX F

## METHODOLOGIES FOR COMPUTING THE UNAVAILABILITY INDEX, THE UNRELIABILITY INDEX AND COMPONENT PERFORMANCE LIMITS

This appendix provides the details of three calculations: the System Unavailability Index, the System Unreliability Index, and component performance limits.

## 1. System Unavailability Index (UAI) Due to Train Unavailability

Unavailability is monitored at the train level for the purpose of calculating UAI. The process for calculation of the System Unavailability Index has three major steps:

- Identification of system trains
- Collection of plant data
- Calculation of UAI

The first of these steps is performed for the initial setup of the index calculation (and if there are significant changes to plant configuration). The second step has some parts that are performed initially and then only performed again when a revision to the plant specific PRA is made or changes are made to the normal preventive maintenance practices. Other parts of the calculation are performed periodically to obtain the data elements reported to the NRC. This section provides the detailed guidance for the calculation of UAI.

### 1.1. Identification of System Trains

The identification of system trains is accomplished in two steps:

- Determine the system boundaries
- Identify the trains within the system

The use of simplified P&IDs can be used to document the results of this step and will also facilitate the completion of the directions in section 2.1.1 later in this document.

### 1.1.1. System Boundaries

The first step in the identification of system trains is to define the system boundaries. Include all components that are required to satisfy those functions in section 5 of this appendix that have been determined to be risk-significant functions per NUMARC 93-01.

If none of the functions listed in section five for a system are determined to be risk significant, then:

- If only one function is listed for a system, then this function must be monitored (for example, CE NSSS designs use the Containment Spray system for RHR but this system is redundant to the containment coolers and may not be risk significant. It would be monitored.)

Attachment 4

- If multiple functions are listed for a system, then monitor the most risk significant one. (For example BWR Residual Heat Removal systems lists three functions. If none of them are determined to be risk significant, monitor the function that is determined to be the most risk significant of the three.) Use the Birnbaum Importance values to determine which function is most important.

For fluid systems the boundary should extend from the water source (e.g., tanks, sumps, etc.) to the injection point (e.g., RCS, Steam Generators). 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. For Emergency AC systems, the system consists of all class 1E generators at the station.

Additional system specific guidance on system boundaries can be found in section 5 titled "Additional Guidance for Specific Systems" at the end of this appendix.

Some common conditions that may occur are discussed below.

System Interface Boundaries

For water connections from systems that provide cooling water to a single component in a monitored system, the final connecting valve is included in the boundary of the frontline system rather than the cooling water system. For example, for service water that provides cooling to support an AFW pump, only the final 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 monitored 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. If additional water sources are required to satisfy train mission times, only the connecting active valve from the additional water source is considered as a monitored component for calculating UAI. 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 monitored and should be included in UAI for the system.

Common Components

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

### 1.1.2. Identification of Trains within the System

Each monitored system shall then be divided into trains to facilitate the monitoring of unavailability.

*A train* consists of a group of components that together provide the risk significant functions of the system described in the "additional guidance for specific mitigating systems". The number of trains in a system is generally determined as follows:

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 number of trains available to achieving the risk-significant function of the system. To be an "installed spare," a component must not be needed for any train of the system to perform the risk significant function. A typical installed spare configuration is a two train system with a third pump that can be aligned to either train (both from a power and flow perspective), but is normally not aligned and when it is not aligned receives no auto start signal. In a two train system where each train has two 100% capacity pumps that are both normally aligned, the pumps are not considered installed spares, but are redundant components within that train.

Unavailability of an installed spare is not monitored. Trains in a system with an installed spare are not considered to be unavailable when the installed spare is aligned to that train. In the example above, a train would be considered to be unavailable if neither the normal component nor the spare component is aligned to the train.

~~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.~~

## 1.2.Collection of Plant Data

Plant data for the UAI portion of the index includes:

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

Each of these data inputs to UAI will be discussed in the following sections.

### 1.2.1. Actual Train Unavailability

The Consolidated Data Entry (CDE) inputs for this parameter are Train Planned Unavailable Hours and Train Unplanned Unavailable Hours. Critical hours are derived from reactor startup and shutdown occurrences. The actual calculation of Train Unavailability is performed by CDE.

*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.

*Train unavailable hours*: The hours the train was not able to perform its risk significant function while critical. Fault exposure hours are not included; unavailable hours are counted only for the time required to recover the train's risk-significant functions. Unavailability must be by train; do not use average unavailability for each train because trains may have unequal risk weights.

*Planned unavailable hours:* These hours include time the train was out of service for maintenance, testing, equipment modification, or any other time equipment is electively removed from service and the activity is planned in advance.

*Unplanned unavailable hours:* These hours include corrective maintenance time or elapsed time between the discovery and the restoration to service of an equipment failure or human error (such as a misalignment) that makes the train unavailable. Unavailable hours to correct discovered ~~degraded~~ conditions that render a monitored component incapable of performing its risk-significant function are counted as unplanned unavailable hours. An example of this is a condition discovered by an operator on rounds, such as an obvious oil leak, that resulted in the equipment being non-functional even though no demand or failure actually occurred.

Additional guidance on the following topics for counting train unavailable hours is provided below.

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

## 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 or evolutions that meet this criterion and have it available for inspector review. The intent is to minimize unnecessary burden of data collection, documentation, and verification because these short durations have insignificant risk impact

## Credit for Operator Recovery Actions to Restore the Risk-Significant Functions

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*

---

[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.

MSPI. Short duration unavailability, for example, would not be added back in because it is excluded under both SSU and MSPI.

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. (However, do not subtract any hours already subtracted in the above steps.)
8) Divide the hours derived from steps 1-7 above by the total critical hours during 2002-2004. This is the baseline planned unavailability.

Support cooling planned unavailability baseline data is based on plant specific maintenance rule unavailability for years 2002-2004. Maintenance Rule practices do not typically differentiate planned from unplanned unavailability. However, best efforts will be made to differentiate planned and unplanned unavailability during this time period.

If maintenance practices at a plant have changed since the baseline years (e.g. increased planned online maintenance due to extended AOTs), then the baseline values should be adjusted to reflect the current maintenance practices and the basis for the adjustment documented in the plant's MSPI Basis Document.

### 1.2.3. Generic Baseline Unplanned Unavailability

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.)

**Table 1. Historical Unplanned Unavailability Train Values**

**(Based on ROP Industry wide 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 |

*Pump failure to run:* Given that it has successfully started and run for an hour, a failure of a pump to run/operate. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

*Valve failure on demand*: A failure to transfer to the required risk significant state (open, close, or throttle to the desired position as applicable) is counted as failure on demand. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

*Breaker failure on demand*: A failure to transfer to the required risk significant state (open or close as applicable) is counted as failure on demand. (Exclude post maintenance tests, unless the cause of failure was independent of the maintenance performed.)

### Treatment of Demand and Run Failures

Failures of monitored components on demand or failures to run, either actual or test are included in unreliability. Failures on demand or failures to run while not critical are included unless an evaluation determines the failure would not have affected the ability of the component to perform its risk-significant at power function. In no case can a postulated action to recover a failure be used as a justification to exclude a failure from the count.

### Treatment of ~~Degraded~~ Discovered Conditions that Result in the Inability to Perform a Risk Significant Function ~~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~~ Discovered conditions, even if no actual demand or test existed, that render a monitored 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~~ discovered condition would have prevented a successful start, 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~~ prior to completing its mission time, 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) and only while critical.

~~Degraded~~ Discovered conditions, or actual unavailability due to mispositioning of non-monitored 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) and only while critical.

Loss of risk significant function(s) is assumed to have occurred if the established success criteria have 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, the current quarter's URI and UAI must be based on the success criteria of record at the time the degraded condition is discovered. If the new success criteria causes a revision to the PRA affecting the numerical results (i.e. CDF and FV), then the change must be included in the PRA model and the appropriate new values calculated and incorporated in the MSPI Basis Document prior to use in the calculation of URI and UAI. If the change in success criteria has no effect on the numerical results of the PRA (representing only a change in margin) then only the MSPI Basis Document need be revised prior to using the revised success criteria.

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.

~~Treatment of Degraded Conditions 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, unforeseen sequences not incorporated into the surveillance test, 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.~~

Failures of Non-Monitored Structures, Systems, and Components (SSC)

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 would have caused 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 would have caused 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. (Note, however, in the above example, if the shut manual suction isolation valve resulted in an actual pump failure, the pump failure would be counted as a demand and failure of the pump.)

## 3. Establishing Statistical Significance

This performance indicator establishes an acceptable level of performance for the monitored systems that is reflected in the baseline reliability values in Table 4. Plant specific differences from this acceptable performance are interpreted in the context of the risk significance of the difference from the acceptable performance level. It is expected that a system that is performing at an acceptable performance level will see variations in performance over the monitoring period. For example a system may, on average, see three failures in a three year period at the accepted level of reliability. It is expected, due to normal performance variation, that this system will sometimes experience two or four failures in a three year period. It is not appropriate that a system should be placed in a white performance band due to expected variation in measured performance. This problem is most noticeable for risk sensitive systems that have few demands in the three year monitoring period.

This problem is resolved by applying a limit of 5.0e-07 to the magnitude of the most significant failure in a system. This ensures that one failure beyond the expected number of failures alone cannot result in MSPI > 1.0e-06. A MSPI > 1.0e-06 will still be a possible result if there is significant system unavailability, or failures in other components in the system.

This limit on the maximum value of the most significant failure in a system is only applied if the MSPI value calculated without the application of the limit is less than 1.0e-05.

This calculation will be performed by the CDE software, no additional input values are required.

## 4. Calculation of System Component Performance Limits

The mitigating systems chosen to be monitored are generally the most important systems in nuclear power stations. However, in some cases the system may not be as important at a specific station. This is generally due to specific features at a plant, such as diverse methods of achieving the same function as the monitored system. In these cases a significant degradation in performance could occur before the risk significance reached a point where the MSPI would cross the white boundary. In cases such as this it is not likely that the performance degradation would be limited to that one system and may well involve cross cutting issues that would potentially affect the performance of other mitigating systems.

A performance based criterion for determining ~~degraded~~ declining performance is used as an additional decision criteria for determining that performance of a mitigating system has degraded to the white band. This decision is based on deviation of system performance from expected performance. The decision criterion was developed such that a system is placed in the white performance band when there is high confidence that system performance has degraded even though MSPI < 1.0e-06.

The criterion is applied to each component type in a system. If the number of failures in a 36 month period for a component type exceeds a performance based limit, then the system is considered to be performing at a white level, regardless of the MSPI calculated value. The performance based limit is calculated in two steps:

1. Determine the expected number of failures for a component type and
2. Calculate the performance limit from this value.

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.

For Combustion Engineering (CE) plants, the design features two or three centrifugal pumps that operate at intermediate pressure (about 1300 psig) and provide flow to four 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).

## PWR Auxiliary Feedwater Systems

### Scope

The function of the AFW system is to provide decay heat removal via the steam generators to cool down and depressurize the reactor coolant system following a reactor trip. The mitigation of ATWS events with the AFW system is not considered a function to be monitored by the MSPI. (Note, however, that the FV values will include ATWS events). ~~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~~ a ~~primary~~ water source (typically, the condensate storage tank and if required to meet the PRA success criteria and mission time, from an alternate source) ~~or, if required, from an emergency source (typically, a lake or river via the service water system)~~ and to inject into at least one steam generator.

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. The flow path for the steam supply to a turbine driven pump is included from the steam source (main steam lines) to the pump turbine. Pumps included in the Technical Specifications (subject to a Limiting Condition for Operation) are included in the scope of this indicator. Startup feedwater pumps are not included in the scope of this indicator. Some initiating events, such as a feedwater line break, may require isolation of AFW flow to the affected steam generator to prevent flow diversion from the unaffected steam generator. This function should be considered a monitored function if it is required.