Attachment 4

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.

Fussell-Vesely, Unavailability and Unreliability

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:

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

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

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

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:

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

Where:

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

R_1 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:

$$FV = 1 - \frac{\bigcup\limits_{j=1,n} C_{1j}}{\bigcup\limits_{j=1,m} C_{0j}},$$

where the denominator represents the union of <u>m</u> minimal cutsets C_0 generated with the reference (baseline) model, and the numerator represents the union of <u>n</u> minimal cutsets C_1 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.

~~The determination of trains for the cooling water support system may be difficult. In this case, the system should be defined in segments, and each segment treated in the calculation of UAI as if it were a train. A segment may be as small as an individual component in a system. The general approach should be to divide the system into as few segments as possible and still describe the functionality of the system. In no case should a segment be larger than a single train of a system.~~

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 is based on~~...p~~plant specific unplanned and planned unavailability for years 1999 to 2001. ~~Need to review support cooling pump and valve characteristics to those in Table 2 to determine if they are representative]....~~

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.~~7~~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

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 includes 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).

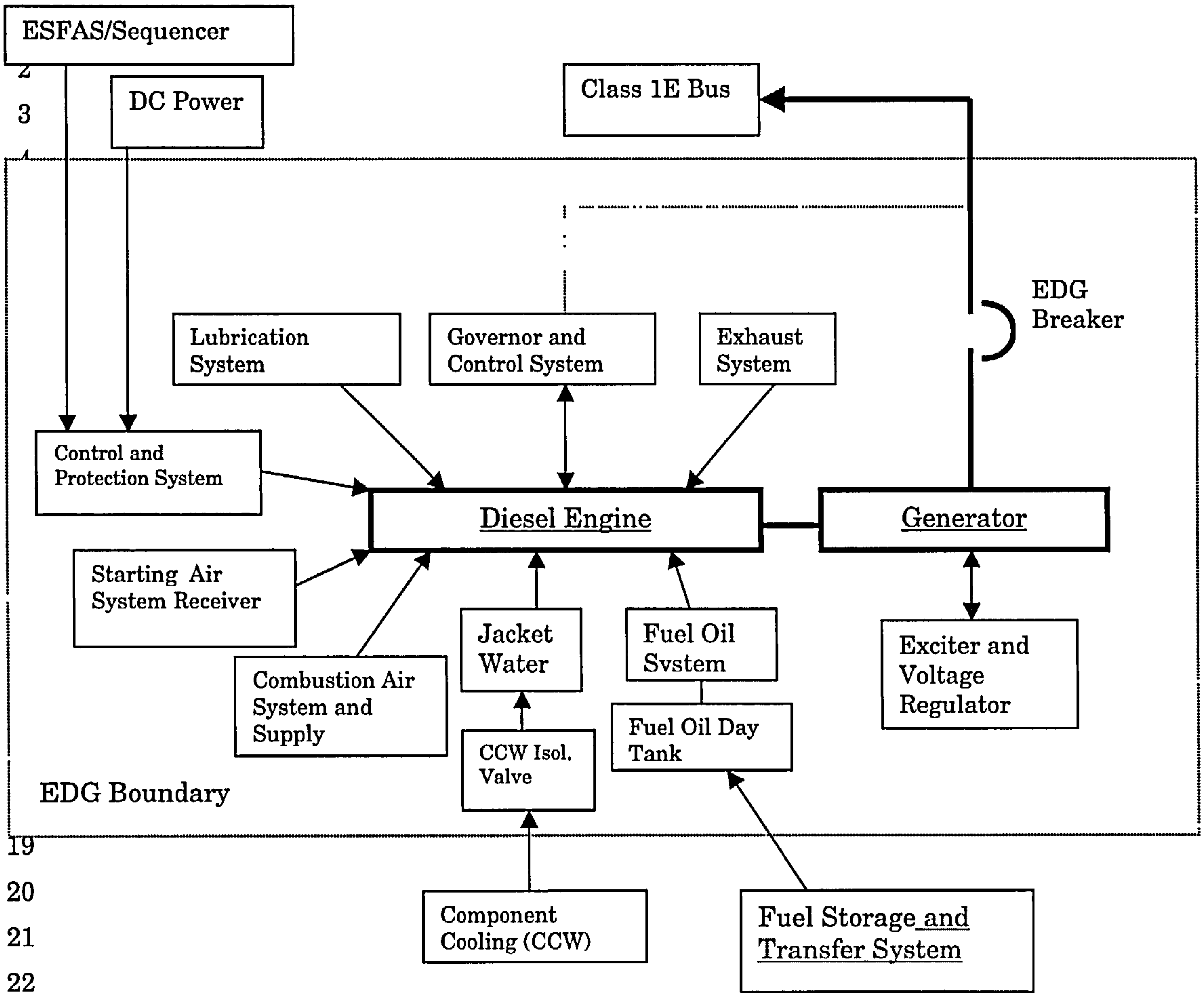
ESFAS/Sequencer
DC Power
Class 1E Bus
EDG
Breaker
Lubrication
System
Governor and
Control System
Exhaust
System
Control and
Protection System
Diesel Engine
Generator
Starting Air
System Receiver
Combustion Air
System and
Supply
Jacket
Water
Fuel Oil
System
Exciter and
Voltage
Regulator
CCW Isol.
Valve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

Figure F-1

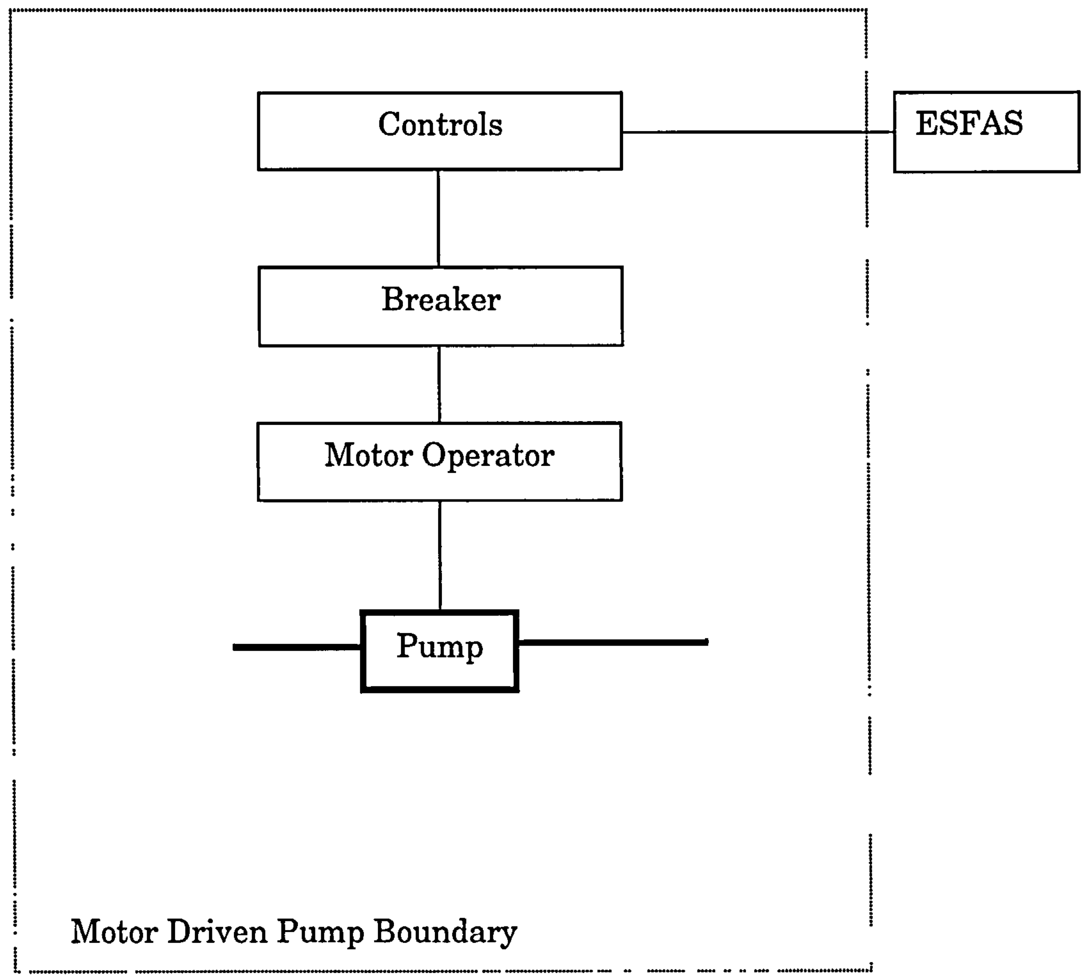
Controls
ESFAS
Breaker
Motor Operator
Pump
Motor Driven Pump Boundary

Figure F-2

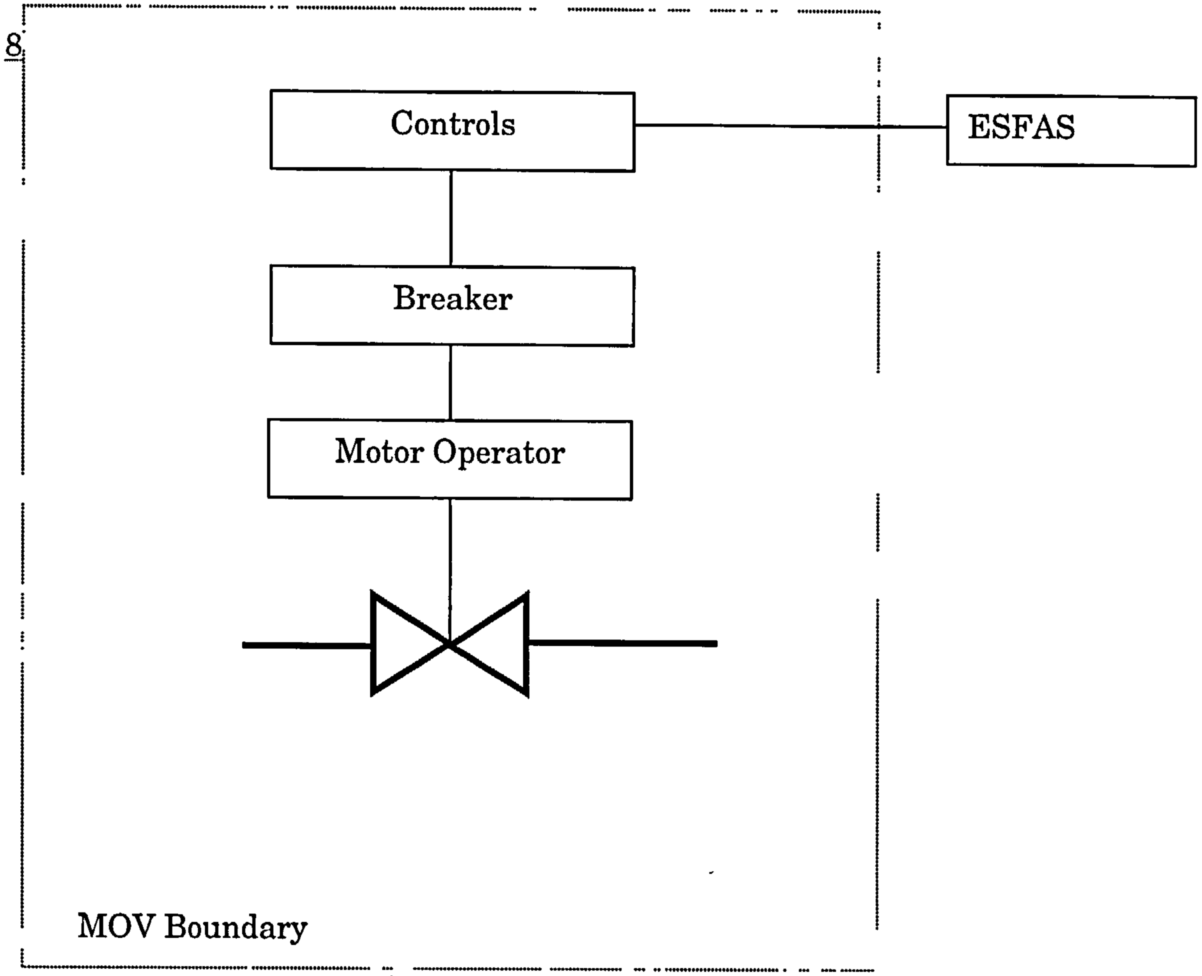

Figure F-3

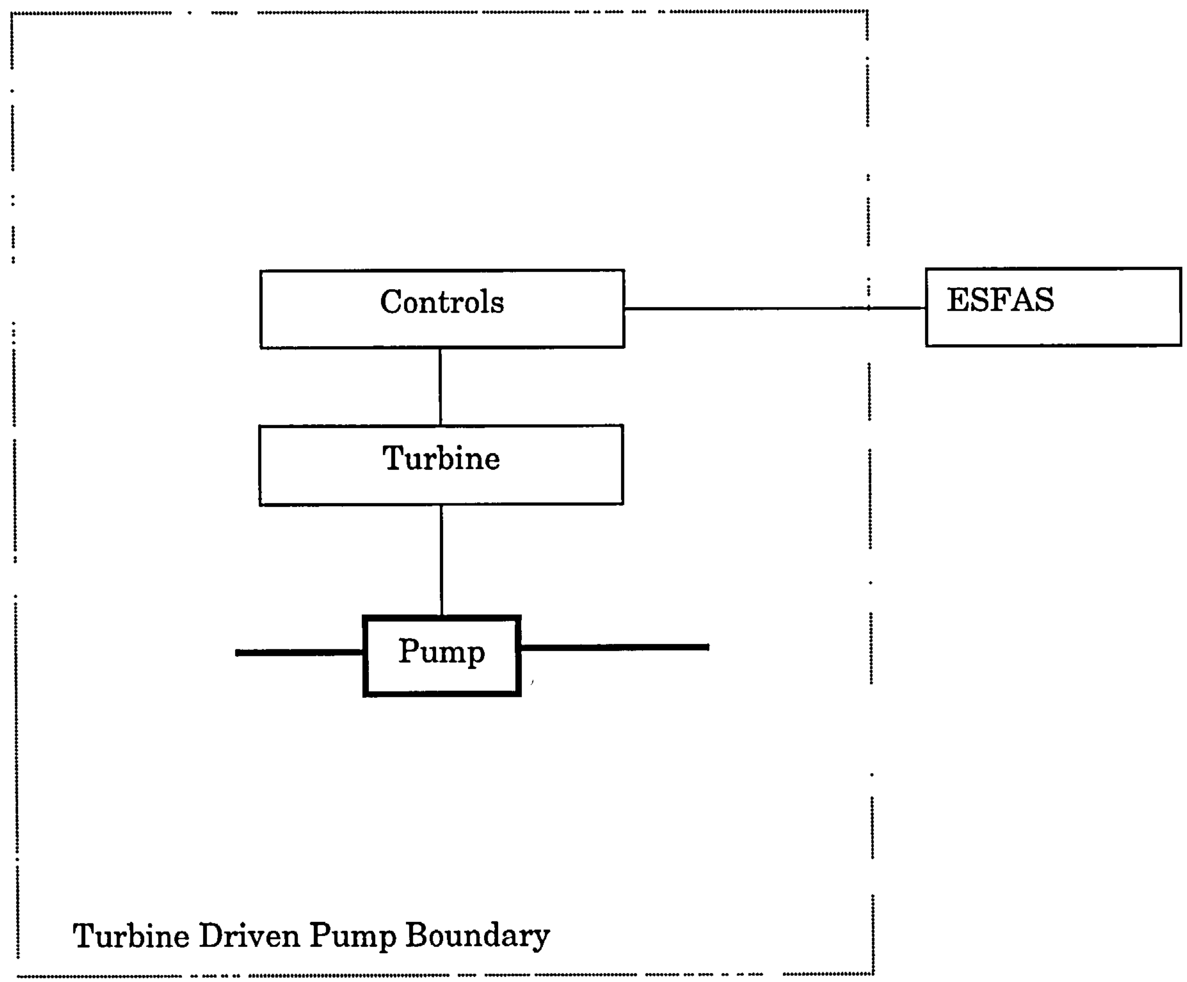

Figure F-4

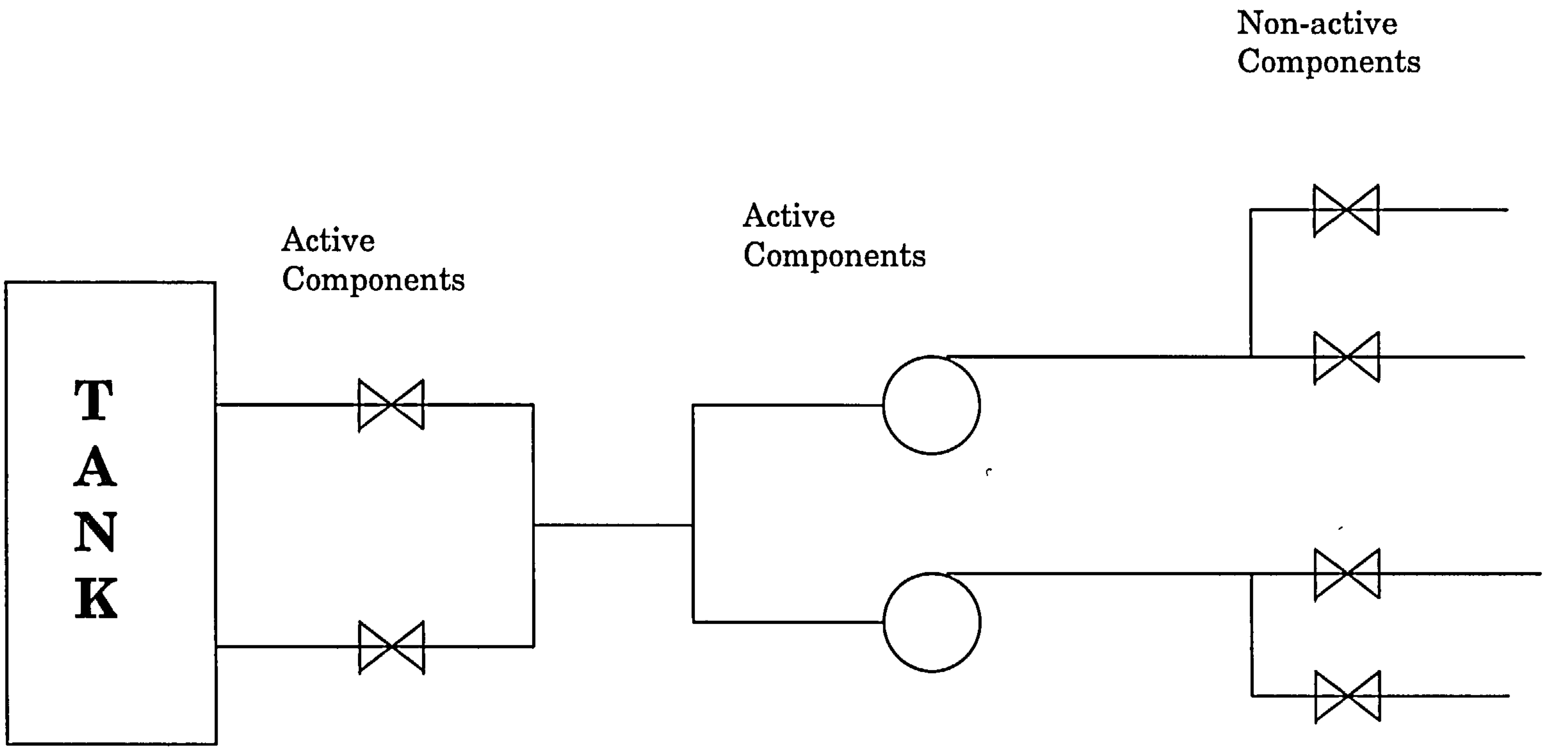
Non-active
Components
Active
Components
Active
Components
T
A
N
K

Figure F-5