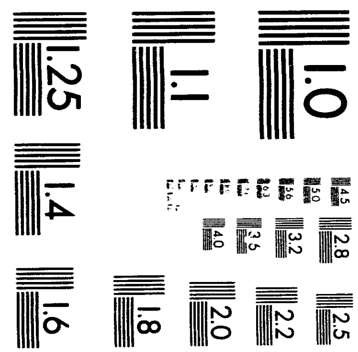

1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3

1 of 2

DOE/OR/00033-T572

THE USE OF PROBABILISTIC RISK ASSESSMENT IN SATISFACTION OF

THE NUCLEAR REGULATORY COMMISSION'S MAINTENANCE RULE

by

RENÉE M. DUBORD
Submitted to the Department of
Nuclear Engineering
in Partial Fulfillment of the
Requirements for the
Degrees of

Bachelor of Science
and
Master of Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 1993

Signature of Author Renée Dubord
Department of Nuclear Engineering
May 7, 1993

Certified by Michael W. Golay
Michael W. Golay
Thesis Co-supervisor

Certified by Norman C Rasmussen
Norman C. Rasmussen
Thesis Co-supervisor

Accepted by ______________________
Allan F. Henry
Chairman, Department Committee
on Graduate Students

THE USE OF PROBABILISTIC RISK ASSESSMENT TO SATISFY THE NUCLEAR REGULATORY COMMISSION'S MAINTENANCE RULE

by

RENÉE DUBORD

Submitted to the Department of Nuclear Engineering
on May 7, 1993, in partial fulfillment of the
requirements for the degrees of Bachelor of Science and Master of Science
in Nuclear Engineering.

ABSTRACT

Maintenance and inspection at nuclear power plants consumes a large portion of a utility's resources, making resource allocation for such procedures vital. The NRC Maintenance Rule, due to be implemented in July of 1996, requires utilities to select systems, structures, and components (SSCs) important to safety and to develop a monitoring program to ensure that these SSCs are capable of fulfilling their intended functions.

In light of these concerns, two ratios were developed to compare the risk significance of individual components with the amount of plant staff time, or burden, associated with inspecting the component. These risk/burden ratios point out existing disparities between current inspection practices and safety concerns. These ratios can be used to develop new inspection schedules constituting a more equitable risk to burden distribution.

ACKNOWLEDGMENTS

I wish to thank my thesis supervisor, Professor Michael W. Golay, for all of his assistance and support throughout the course of this investigation. His help was vital to defining and refining the topic and scope of this work.

I would also like to thank my thesis co-supervisor, Professor Norman C. Rasmussen, for all of his help throughout this project and his personal inspiration.

Special thanks are also due to Mr. Ken J. Vehstedt at NYPA for his untiring explanations and data searches. This thesis would not have been possible without him. Mr. Herschel Specter of NYPA also provided considerable information for which I am grateful.

Thanks are also due to Shari for letting me into the office, and to Rodrigo, Paul, Jeff and Andrew for putting up with my CD player, among other things. Thanks a million to Jonathan for his technical and AmiPro help, to Jen for patiently keeping me sane, and to Tim for keeping me up at night!

The research was performed under appointment to the Nuclear Engineering/Health Physics Fellowship program administered by Oak Ridge Institute for Science and Education for the U.S. Department of Energy.

TABLE OF CONTENTS

			Page
ABSTRACT			2
ACKNOWLEDGMENTS			3
TABLE OF CONTENTS			4
LIST OF TABLES			6
LIST OF FIGURES			7
CHAPTER	I.	RISK-BASED REGULATION	8
	1.1	Introduction	8
	1.2	Approaches to Risk-Based Regulation	9
	1.3	Cautions for Risk-Based Regulation	10
	1.4	Selection of Example Systems	11
		1.4.1 Risk Significant System	
		1.4.2 Risk Insignificant System	
	1.5	Maintenance Rule Applicability to Risk Insignificant SSCs	23
CHAPTER	II.	TESTING AND SURVEILLANCE REQUIREMENTS	30
	2.1	Introduction	30
	2.2	ESW System Description	31
	2.3	LCS System Description	39

			Page
	2.4	System Unavailability	42
		2.4.1 Scheduled Tests and Surveillances	
		2.4.2 Procedures for the ESW System	
		2.4.3 Procedures for the LCS System	
CHAPTER	III.	RISK-BASED RESOURCE ALLOCATION	52
	3.1	Introduction	52
	3.2	ESW and LCS Resource Allocation per Component	54
	3.3	Ratio of Time Burden Versus Risk Reduction and Risk Increase Importances	62
	3.4	Uses of the Risk/Burden Component Ratios	78
CHAPTER	IV.	METHODOLOGY ACCEPTABILITY AND UNCERTAINTY	80
	4.1	Introduction	80
	4.2	Acceptability of PRA Quantitative Results	80
	4.3	Sources of Uncertainty	83
		4.3.1 Plant and Procedure Modifications	
		4.3.2 Data Estimation	
		4.3.3 Considerations Other Than Risk Reduction and Risk Increase Importances	
CHAPTER	V.	SUMMARY AND CONCLUSIONS	88
	5.1	Summary	88
	5.2	Conclusions	89
REFERENCES			91
APPENDIX A.		THE MAINTENANCE RULE	93
APPENDIX B.		DESCRIPTIONS OF THE 9 DOMINANT CORE DAMAGE ACCIDENT SEQUENCES	95

LIST OF TABLES

Number	Title	Page
1.1	Top Cut Sets for Dominant Accident Sequences	13
1.2	Event Descriptions	16
1.3	Core Damage Frequency Risk Reduction Importance Values	18
1.4	Core Damage Frequency Risk Increase Importance Values	20
1.5	Core Spray System Basic Events in the Set of CDF Cutsets	24
1.6	ESW vs. LCS Component Type Comparison	25
1.7	ESW and LCS Dependent Components	26
2.1	Risk Reduction Importances for ESW Top Events	37
2.2	James A. Fitzpatrick Plant Failure Data	43
3.1	ESW System Time Burden by Component	57
3.2	LCS System Time Burden by Component	59
3.3	ESW System Component Risk Reduction Importance Versus Time Burden	63
3.4	LCS System Component Risk Reduction Importance Versus Time Burden	66
3.5	ESW System Component Risk Increase Importance Versus Time Burden	68
3.6	LCS System Component Risk Increase Importance Versus Time Burden	71
3.7	ESW Component Risk/Burden Ratio Rankings	73
3.8	LCS Component Risk/Burden Ratio Rankings	75

LIST OF FIGURES

Number	Title	Page
1.1	Core Damage Frequency Percent Increase per System	22
2.1.1	Emergency Service Water Schematic Diagram	33
2.1.2	Emergency Service Water Schematic Diagram (continued)	34
2.1.3	Emergency Service Water Schematic Diagram (continued)	35
2.1.4	Schematic Legend	36
2.2	Core Spray System Schematic Diagram	40

CHAPTER I

RISK-BASED REGULATION

1.1 Introduction

Proper systems and component maintenance at nuclear power plants is important both for safety concerns and for ensuring the best allocation of available company resources. The NRC has adopted a Maintenance Rule, 10 CFR 50.65 (appendix A), which requires each holder of an operating license under 50.21 or 50.22 to set safety goals for plant structures, systems, and components (SSCs). These SSCs must either be monitored or be subject to a preventive maintenance program to ensure their proper operation. The rule is targeted for SSCs important to safety, such as those necessary to avoid reactor scrams, ensure reactor shutdown in the event of an accident, or mitigate the effects of an accident.

The first step in implementing the NRC Maintenance Rule is to identify those SSCs which fall into the safety and risk-significant category. One method of ranking the importance of SSCs is the use of probabilistic risk assessment technology. PRA techniques can be used to prioritize SSCs into risk-significant and risk-insignificant categories. Once a system's components have been placed in a risk category, their maintenance needs can be assessed based on their risk significance.

Since the NRC's Maintenance Rule is due to be implemented in July of 1996, there is currently a great deal of interest in establishing a sound PRA-based methodology for SSC selection. It is also important to determine how maintenance procedures should be changed for SSCs in different categories of risk significance. The New York Power Authority's James A. Fitzpatrick plant's PRA data was selected to serve as an illustration of a possible approach to this problem.

1.2 Approaches to Risk-Based Regulation

There are several ways to use PRA data to prioritize SSCs that are contributors to risk. One of the most important risk measurements for a plant is the core damage frequency (CDF). Event scenarios that will lead to core damage can be ranked by their probability of occurrence and expressed in terms of their minimal cutsets. A minimal cutset is the smallest combination of basic top events that will lead to the undesired scenario. The minimal cutsets can then be ranked in terms of their frequency of occurrence in the total set of risk significant event scenarios. The SSCs that correspond to high-frequency minimal cutsets are the most risk significant.

Another way to measure risk significance is through risk increase and risk reduction importances. Risk increase importance is the increase in risk (CDF) that occurs if the basic event is assumed to occur. This is calculated as the difference in CDF when the basic event probability of occurrence is set equal to unity:

Risk Increase = TEF(evaluated with EV(J) = 1) - TEF

TEF = frequency of top event core damage

EV(J) = probability of event J for base events.

Risk reduction importance is the decrease in CDF that occurs if the basic event is eliminated by setting the probability of occurrence to zero:

$$\text{Risk Reduction} = \text{TEF} - \text{TEF(evaluated with EV(J)} = 0).$$

The basic events that contribute the most to the CDF risk are those with the highest risk reduction importances. Proper maintenance and surveillance of the SSCs corresponding to high risk reduction importances will be the most beneficial and lead to the greatest overall reduction in risk. Conversely, risk insignificant basic events can be identified as those with the lowest risk increase importances. These SSCs cause negligible risk increases even if inoperable, and thus maintenance on them is risk insignificant.

A broader systems-based approach can also be used to identify risk significant systems as a whole. The change in total CDF when an entire system's unavailability is changed can be calculated and used to compare the risk significance of various systems. This comparison can be used to identify risk significant systems, but does not provide information as to which components in each system are the most important for maintenance and surveillance.

1.3 Cautions for Risk-Based Regulation

A study of only the SSCs that can be identified by cutsets and importance rankings dealing with the plant's CDF will almost certainly miss some risk significant items. As suggested by Specter[1], the PRA rankings for containment failure frequency and source terms should also be analyzed. Such a level 2 search should turn up components that do not directly affect CDF but are important for preventing radioactive releases.

Secondly, a distinction must be made between truly risk insignificant SSCs and those that have been effectively regulated to the point where they show up as being risk insignificant in a CDF ranking. Obviously, many components in the plant are unimportant in terms of preventing or mitigating an accident. Various PRA SSC ranking studies have estimated that only several hundred components are needed to control 99.9% of the CDF for light water reactors. However, some plant components currently show up as risk insignificant because they have been effectively regulated. Specter[1] (denotes ref. 1) gives reactor vessel failure as an example. The reactor vessel reliability will not show up in CDF rankings as risk significant. However, this is because this particular plant component has been strictly regulated in its design, not because it is inherently safe. It is important that such distinctions be identified and addressed.

1.4 Selection of Example Systems

Two systems in the James A. Fitzpatrick plant were selected for examination in order to illustrate the relationship between risk significance and surveillance practices. One risk significant and one risk insignificant system were examined to illustrate the differing surveillance needs between the two. In this study only the events leading to core damage were investigated. A level 2 analysis would be necessary to identify less obvious SSCs. The top nine core damage accident sequences are detailed in Appendix B.

1.4.1 Risk Significant System

The emergency service water (ESW) system was selected as the example risk significant system for several reasons. First, it falls into the risk significant category using all three of the suggested selection methods, as detailed below. It also has a reasonably straightforward configuration, simplifying data analysis and the amount of component data required from NYPA. Lastly, the ESW system contains several components known to require inspection, which gives a clear illustration of possible beneficial changes in practices.

The ESW system components have very high cutset frequencies, meaning the system is extremely pervasive and comes into play in many of the CDF dominant scenarios. The top cutsets for the CDF dominant accident scenarios are listed in Table 1.1. These cutsets have the highest probabilities of occurrence and are thus the most important. Each cutset basic event is explained in Table 1 2. Cutsets involving an ESW event have been highlighted in Table 1.1. Forty out of the fifty-two listed cutsets involve an ESW event, a very high proportion. Out of a total of 271 basic events, only 22 occurred more than 100 times in the total set of all CDF cutsets. Seven of these involve ESW components. Such a high cutset rate of occurrence in the CDF scenarios indicates that the ESW system is very risk significant.

The ESW system can also be shown to be risk significant by examining the Fitzpatrick CDF risk reduction importances. The fifteen highest risk reduction importances are listed in Table 1.3. Of the top fifteen basic events, eight of them involve the ESW system. Furthermore, no ESW components show up in the risk insignificant list of the bottom fifteen risk increase importances (Table 1.4)

NYPA performed a sensitivity analysis on the change in CDF when an entire system's unavailability is changed. The study doubled the total unavailability, including maintenance, for eleven different systems. The results are shown in Figure 1.1. The ESW

TABLE 1.1

TOP CUT SETS FOR DOMINANT ACCIDENT SEQUENCES

Sequence T1-35-T3C-84 Total Sequence Frequency: 7.13E-08 yr^{-1}

INDIVIDUAL SEQUENCE FREQUENCY:	INDIVIDUAL SEQUENCE DESCRIPTION:
3.0697E-08	T1 * XHE-ASP-MC-RPTXR * P1 * /C * NR-MANVLV-15V +

Cutset explanation (/ indicates success):

The initiating event, loss of offsite power (T1), occurs. Reactor pressure sensors fail due to human error causing miscalibration (XHE-ASP-MC-RPTXR). Safety relief valves open and one fails to reclose (P1). The reactor scrams (/C). There is no recovery due to a failure to open an injection valve manually (NR-MANVLV-15V).

FREQUENCY:	DESCRIPTION:
9.9458E-09	T1 * ESF-TRU-DN-T252A * ESF-TRU-DN-T252B * P1 * /C * NR-MANVLV-15V +
9.9458E-09	T1 * ESF-TRU-DN-T252C * ESF-TRU-DN-T252D * P1 * /C * NR-MANVLV-15V +
2.6854E-09	T1 * ESF-TRU-DN-T252A * ESF-ASP-DN-PT52B * P1 * /C * NR-MANVLV-15V +
2.6854E-09	T1 * ESF-TRU-DN-PT52C * ESF-ASP-DN-T252D * P1 * /C * NR-MANVLV-15V +
2.6854E-09	T1 * ESF-TRU-DN-T252C * ESF-ASP-DN-PT52D * P1 * /C * NR-MANVLV-15V +
2.6854E-09	T1 * ESF-TRU-DN-PT52A * ESF-ASP-DN-T252B * P1 * /C * NR-MANVLV-15V +

SEQUENCE T1-38-TB-1 Total Sequence Frequency: 6.17E-07 yr^{-1}

FREQUENCY:	DESCRIPTION:
7.8721E-08	**T1 * ESW-CCF-FR-PUMPS * /P * /U1X * NR-LOSP-13HR-TB1+**
6.0689E-08	**T1 * ESW-CCF-FS-PUMPS * /P * /U1X * NR-LOSP-13HR-TB1+**
2.9903E-08	**T1 * ESW-MDP-FR-P2A * ESW-MAI-MA-LOOPB * /P * /U1X * NR-LOSP-13HR-TB1+**
2.0917E-08	**T1 * ESW-MAI-MA-LOOPA * ESW-MDP-FR-P2B * /P * /U1X * NR-LOSP-13HR-TB1+**
1.9882E-08	**T1 * ESW-MAI-MA-LOOPB * AC4-XHE-MC-UVRLA * /P * /U1X * NR-LOSP-13HR-TB1+**
1.9882E-02	**T1 * ESW-XHE-RE-ESW3A * ESW-MAI-MA-LOOPB * /P * /U1X * NR-LOSP-13HR-TB1+**

SEQUENCE T1-38-TB-2 Total Sequence Frequency: 6.06E-08 yr^{-1}

FREQUENCY:	DESCRIPTION:
7.9761E-09	**T1 * ESW-CCF-FR-PUMPS * U1X * /P * NR-LOSP-13HR-TB2+**
6.1491E-09	**T1 * ESW-CCF-FS-PUMPS * U1X * /P * NR-LOSP-13HR-TB2+**
3.0298E-09	**T1 * ESW-MDP-FR-P2A * ESW-MAI-MA-LOPB * U1X * /P * NR-LOSP-13HR-TB2+**
2.1193E-09	**T1 * ESW-MAI-MA-LOOPA * ESW-MDP-FR-P2B * U1X * /P * NR-LOSP-13HR-TB2+**
2.0145E-09	**T1 * ESW-MAI-MA-LOOPB * AC4-XHE-MC-UVRLA * U1X * /P * NR-LOSP-13HR-TB2+**
2.0145E-09	**T1 * ESW-XHE-RE-ESW3A * ESW-MAI-MA-LOOPB * U1X * /P * NR-LOSP-13HR-TB2+**

SEQUENCE T1-38-TB-4 Total Sequence Frequency: 4.63E-08 yr^{-1}

FREQUENCY:	DESCRIPTION:
1.8380E-09	**T1 * ESW-MAI-MA-LOOPA * DC1-BAT-HW-BATTB * /P * NR-LOSP-13HR-TB4+**
1.6472E-09	**T1 * ESW-CCF-FR-PUMPS * HCI-MAI-MA-HPCIU * /P * NR-LOSP-13HR-TB4+**
1.2699E-09	**T1 * ESW-CCF-FS-PUMPS * HCI-MAI-MA-HPCIU * /P * NR-LOSP-13HR-TB4+**
1.2036E-09	**T1 * ESW-MDP-FR-P2A * DC1-BAT-HW-BATTB * /P * NR-LOSP-13HR-TB4+**
8.0028E-09	T1 * AC4-XHE-MC-UVRLA * DC1-BAT-HW-BATTB * /P * NR-LOSP-13HR-TB4+
8.0028E-09	**T1 * ESW-XHE-RE-ESW3A * DC1-BAT-HW-BATTB * /P * NR-LOSP-13HR-TB4+**

SEQUENCE T1-38-TB-5 Total Sequence Frequency: 2.96E-07 yr^{-1}

FREQUENCY:	DESCRIPTION:
1.1970E-07	T1 * DC1-CCF-HW-BATTS * /P+
7.3872E-09	T1 * DC1-BAT-HW-BATTA * DC1-BAT-HW-BATTB * /P+
3.9292E-09	**T1 * ESW-MAI-MA-LOOPB * DC1-BAT-HW-BATTA * ESF-ASL-DN-LT72D * /P+**
3.9292E-09	**T1 * ESW-MAI-MA-LOOPB * DC1-BAT-HW-BATTA * ESF-ASL-DN-LT72B * /P+**
3.8403E-09	**T1 * ESW-MAI-MA-LOOPB * DC1-BAT-HW-BATTA * HCI-MAI-MA-HPCIU * /P+**

SEQUENCE T1-38-TB-6 Total Sequence Frequency: 2.53E-07 yr^{-1}

FREQUENCY:	DESCRIPTION:
3.2651E-08	**T1 * ESW-CCF-FR-PUMPS * P1 * NR-LOSP-5HR-TB6+**
2.5172E-08	**T1 * ESW-CCF-FS-PUMPS * P1 * NR-LOSP-5HR-TB6+**
1.2403E-08	**T1 * ESW-MDP-FR-P2A * ESW-MAI-MA-LOOPB * P1 * NR-LOSP-5HR-TB6+**
8.6757E-08	**T1 * ESW-MAI-MA-LOOPA * ESW-MDP-FR-P2B * P1 * NR-LOSP-5HR-TB6+**
8.2466E-08	**T1 * ESW-MAI-MA-LOOPB * AC4-XHE-MC-UVRLA * P1 * NR-LOSP-5HR-TB6+**
8.2466E-08	**T1 * ESW-XHE-RE-ESW3A * ESW-MAI-MA-LOOPB * P1 * NR-LOSP-5HR-TB6+**

SEQUENCE T1-38-TB-8 Total Sequence Frequency: 1.71E-08 yr^{-1}

FREQUENCY:	DESCRIPTION:
1.2209E-08	T1 * DC1-CCF-HW-BATTS * P1+
7.5349E-10	T1 * DC1-BAT-HW-BATTA * DC1-BAT-HW-BATTB * P1+
4.0078E-10	**T1 * ESW-MAI-MA-LOOPB * DC1-BAT-HW-BATTA * ESF-ASL-DN-LT72D * P1+**
4.0078E-10	**T1 * ESW-MAI-MA-LOOPB * DC1-BAT-HW-BATTA * ESF-ASL-DN-LT72B * P1+**
3.9171E-10	**T1 * ESW-MAI-MA-LOOPB * DC1-BAT-HW-BATTA * HCI-MAI-MA-HPCIU * P1+**

SEQUENCE T1-38-TB-9 Total Sequence Frequency: 1.16E-08 yr^{-1}

FREQUENCY:	DESCRIPTION:
1.6139E-09	**T1 * ESW-CCF-RF-PUMPS * P2 * NR-LOSP-2HR-TB9+**
1.2442E-09	**T1 * ESW-CCF-FS-PUMPS * P2 * NR-LOSP-2HR-TB9+**
6.1305E-10	**T1 * ESW-MDP-FR-P2A * ESW-MAI-MA-LOOPB * P2 * NR-LOSP-2HR-TB9+**
4.2882E-10	**T1 * ESW-MAI-MA-LOOPA * ESW-MDP-FR-P2B * P2 * NR-LOSP-2HR-TB9+**
4.1761E-10	**T1 * ESW-MAI-MA-LOOPB * AC4-XHE-MC-UVRLA * P2 * NR-LOSP-2HR-TB9+**
4.0761E-10	**T1 * ESW-XHE-RE-ESW3A * ESW-MAI-MA-LOOPB * P2 * NR-LOSP-2HR-TB9+**

SEQUENCE T3A-4-TB-1 Total Sequence Frequency: 2.98E-08 yr^{-1}

FREQUENCY:	DESCRIPTION:
5.0545E-09	**T3A * /C /P * /U1X * AC0-RCS-OC-62BRB * ESW-CCF-FR-PUMPS+**
5.0545E-09	**T3A * /C /P * /U1X * AC0-RCS-OC-871B1 * ESW-CCF-FR-PUMPS+**
5.0545E-09	**T3A * /C /P * /U1X * AC0-RCS-OC-94BR2 * ESW-CCF-FR-PUMPS+**
5.0545E-09	**T3A * /C /P * /U1X * AC0-RCS-OC-94SN8 * ESW-CCF-FR-PUMPS+**
5.0545E-09	**T3A * /C /P * /U1X * AC0-RCS-OC-871A1 * ESW-CCF-FR-PUMPS+**

TABLE 1.2

TOP EVENT DESCRIPTIONS

BASIC EVENT	PROBABILITY	OCCURRENCES**	DESCRIPTION
AC0-RCS-OC-62BRB	1.01E-05	5	115 kVac relay 62BRB normally open, fails to close
AC0-RCS-OC-871B1	1.01E-05	5	115 kVac relay 871B1 normally open, fails to close.
AC0-RCS-OC-94BR2	1.01E-05	5	115 kVac relay 94BR2 normally open, fails to close.
AC0-RCS-OC-94SN8	1.01E-05	5	115 kVac relay 94SN8 normally open, fails to close.
AC0-RCS-OC-871A1	1.01E-05	5	115 kVac relay 871A1 normally open, fails to close.
AC4-XHE-MC-UVRLA	3.00E-03	127	Human error (miscalibration) of 4.16 kVac Bus 10500 undervoltage relay.
/C	1.00E+00	241	Reactor scram
DC1-BAT-HW-BATTA	3.60E-04	121	Hardware (battery) failure of DC (125-Vdc) Electrical Power System.
DC1-BAT-HW-BATTB	3.60E-04	84	Hardware (battery) failure of DC (125-Vdc) Electrical Power System.
DC1-CCF-HW-BATTS	2.10E-06	2	Common-cause failure of hardware batteries) of DC (125-Vdc) Electrical Power System.
ESF-ASL-DN-LT72D	1.94E-02	26	Engineered Safeguard Feature level sensor LT72D does not operate.
ESF-ASL-DN-LT72B	1.94E-02	26	Engineered Safeguard Feature level sensor LT72B does not operate.
ESF-ASP-DN-PT52 A/B/C/D	1.94E-03	11	Engineered Safeguard Feature pressure sensor PT52B/C/D does not operate.
ESF-TRU-DN-T252 A/B/C/D	7.20E-03	21/24/ 21/24	Engineered Safeguard Feature trip unit 2-3-252A/B/C/D does not operate.
ESW-CCF-FR-PUMPS	1.17E-04	111	Common-cause failure to continue running of ESW pumps.
ESW-CCF-FS-PUMPS	9.02E-05	30	Common-cause failure to start of ESW pumps.
ESW-HXE-RE-ESW3A	3.00E-03	127	Human error (failure to restore to correct position following test or maintenance) of ESW manual valve 3A.
ESW-MAI-MA-LOOPA	6.89E-03	153	ESW LOOPA unavailable due to maintenance.
ESW-MAI-MA-LOOPB	9.85E-03	300	ESW LOOPB unavailable due to maintenance.

BASIC EVENT	PROBABILITY	OCCURRENCES**	DESCRIPTION
ESW-MDP-FR-P2A/B	4.51E-03	178/ 194	Failure to continue running of ESW motor-driven pump P2A / P2B.
HCI-MAI-MA-HPCIU	1.90E-02	148	HPCI unavailable due to maintenance.
NR-LOSP-2HR-TB9	1.21E-01	49	No recovery of loss of offsite power after 2 hours.
NR-LOSP-5HR-TB6	4.80E-02	269	No recovery of loss of offsite power after 5 hours.
NR-LOSP-13HR-TB1	1.30E-02	460	No recovery of loss of offsite power after 13 hours.
NR-LOSP-13HR-TB2	1.30E-02	122	No recovery of loss of offsite power after 13 hours.
NR-LOSP-13HR-TB4	1.30E-02	164	No recovery of loss of offsite power after 13 hours.
NR-MANVLV-15V	3.30E-02	68	Failure to manually open injection valve locally.
/P	1.00E+00	1307	SRVs open and reclose.
P1	1.02E-01	409	SRVs open and 1 fails to reclose.
P2	2.00E-03	66	SRVs open and 2 fail to reclose.
T1	5.70E-02*	1747	Initiating event, loss of offsite power transient.
T3A	4.72E+00*	27	Initiating event, transient that causes a turbine trip.
/U1X	9.08E-01	528	Operator bypasses HPCI high-torus-level auto-switchover from CST to torus suction.
U1X	9.20E-02	138	Operator fails to bypass HPCI high-torus-level auto-switchover from CST; HPCI fails when suppression pool temp. exceeds 200°F.
XHE-ASP-MC-RPTXR	1.60E-04	25	Human error in miscalibration of pressure sensors monitoring reactor pressure.

* Probability denotes the probability of failure, except in the case of T1 and T3A. These initiating events are frequencies of occurrence with units of yr^{-1}.

** Number of times the basic event occurs in the total of all top CDF cutsets.

TABLE 1.3

CORE DAMAGE FREQUENCY RISK REDUCTION IMPORTANCE VALUES[5]

Top 15 RRIs** (for most sensitive basic events):

BASIC EVENT	PROBABILITY	RISK REDUCTION* (yr^{-1})	DESCRIPTION
/P	1.00E+00	1.02E-06	Safety relief valve reclosure
P1	1.02E-01	3.39E-07	One SRV fails to reclose
ESW-MAI-MA-LOOPB	**9.85E-03**	**2.42E-07**	**ESW LOOPB unavailable due to maintenance**
/C	1.00E+00	2.25E-07	Reactor protection system success
ESW-CF-FR-PUMPS	**1.17E-04**	**1.78E-07**	**CCF of ESW pumps to run**
ESW-MAI-MA-LOOPA	**6.89E-03**	**1.50E-07**	**ESW LOOPA unavailable due to maintenance**
ESW-MDP-FR-P2A	**4.51E-03**	**1.48E-07**	**Failure to continue running of ESW motor-driven pump P2A**
ESW-MDΓ-FR-P2B	**4.51E-03**	**1.41E-07**	**Failure to continue running of ESW motor-driven pump P2B**
DC1-CCF-HW-BATTS	2.10E-06	1.32E-07	CCF of 125Vdc batteries
RBC-LOW-PRES-EDG	1.00E+00	1.18E-07	ESW divergence through reactor building closed loop cooling system.
ESW-CCF-FS-PUMPS	**9.02E-05**	**9.76E-08**	**CCF of ESW pumps to start**
AC4-XHE-MC-UVRLA	3.00E-03	9.64E-08	Human error (miscalibration) of 4.16 kVac system undervoltage relay.

BASIC EVENT	PROBABILITY	RISK REDUCTION* (yr^{-1})	DESCRIPTION
ESW-XHE-RE-ESW3A	**3.00E-03**	**9.64E-08**	**Human error (failure to restore to correct position following test or maintenance) of ESW manual valve 3A**
AC4-XHE-MC-UVRLB	3.00E-03	8.95E-08	Human error (miscalibration) of 4.16 kVac system undervoltage relay.
ESW-XHE-RE-ESW3B	**3.00E-03**	**8.95E-08**	**Human error (failure to restore to correct position following test or maintenance) of ESW manual valve 3b.**

* Risk Reduction = TEF - TEF(evaluated with EV(J) = 0)
TEF = frequency of top event core damage
EV(J) = probability of event J for base events

** Basic events relating to operator recovery actions have not been included in this table, as they do not relate to maintenance of components.

TABLE 1.4

CORE DAMAGE FREQUENCY RISK INCREASE IMPORTANCE VALUES[5]

Bottom 15 RIIs** (for most sensitive basic events):

BASIC EVENT	PROBABILITY	RISK INCREASE* (yr^{-1})	DESCRIPTION
DGV-MOD-CC-D143B	3.00E-03	4.76E-08	EDG B room ventilation sys. motor operated damper 143B fails to open on demand
DGV-MOD-CC-D149B	3.00E-03	4.76E-08	EDG B room ventilation sys. motor operated damper 149B fails to open on demand
DGV-RCK-NO-FN-1C	2.50E-03	3.97E-08	EDG C fan 92-FN-1C control circuit coil does not remain energized, no output
EDG-ENG-FR-EDGCR	2.62E-03	3.97E-08	EDG C engine fails to run
RSW-MDP-FR-MP-1A	3.50E-03	3.11E-08	RHRSW motor driven pump P-1A stops running given PM start
DGV-RCK-NO-FN-1A	2.50E-03	2.84E-08	EDG A fan 92-FN-1A control circuit coil does not remain energized, no output
EDG-ENG-FR-EDGAR	2.62E-03	2.84E-08	EDG A engine fails to run
DGV-RCK-NO-FN-1B	2.50E-03	2.77E-08	EDG B fan 92-FN-1B control circuit coil does not remain energized, no output
EDG-ENG-FR-EDGBR	2.62E-03	2.77E-08	EDG B engine fails to run
EDG-RLY-FU-EDGDI	4.30E-03	2.77E-08	EDG D faults in engine running interlock relays
DGV-MOD-CC-D150A	3.00E-03	1.98E-08	EDG A room ventilation sys. motor operated damper D150A does not open on demand

BASIC EVENT	PROBABILITY	RISK INCREASE* (yr^{-1})	DESCRIPTION
DGV-MOD-CC-D150C	3.00E-03	1.98E-08	EDG C room ventilation sys. motor operated damper D150C does not open on demand
RSW-MDP-MA-MP-1C	1.03E-02	1.05E-08	RHRSW motor driven pump P-1C in maintenance
NVP-MOV-CC-120	1.00E-03	7.45E-09	Nitrogen ventilation and purge sys. motor operated valve 27MOV-120 does not open on demand
NVP-MOV-CC-121	1.00E-03	7.45E-09	Nitrogen ventilation and purge sys. motor operated valve 27MOV-121 does not open on demand

* Risk Increase = TEF(evaluated with EV(J) = 1) - TEF
TEF = frequency of top event core damage
EV(J) = probability of event J for base events

** Basic events relating to operator recovery actions have not been included in this table, as they do not relate to maintenance of components.

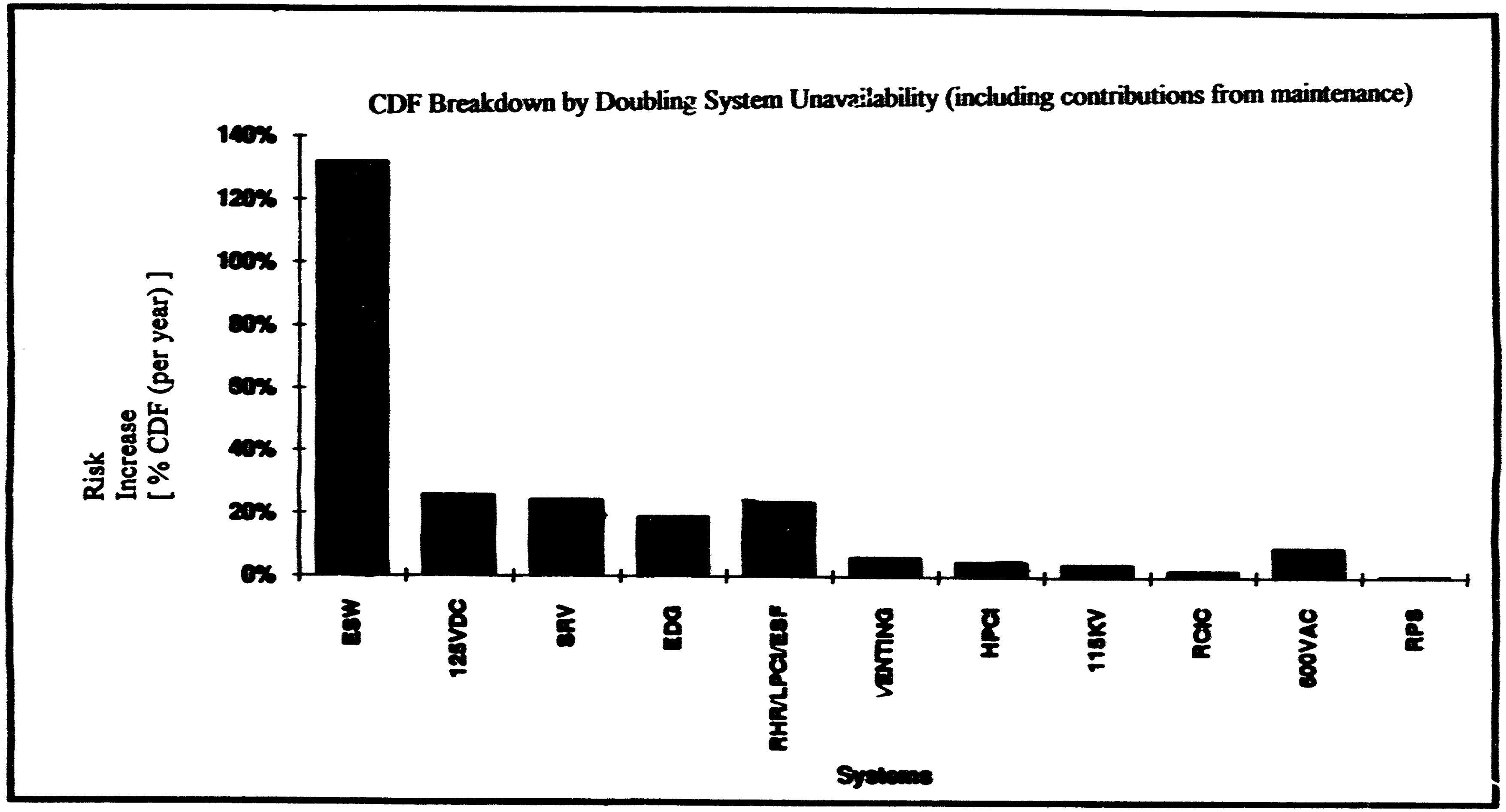


Figure 1.1 Core Damage Frequency Percent Increase per System[2]

system had the greatest change in CDF, an approximately 130% increase in total CDF. The ESW system is obviously one of the most risk significant systems in the plant, and thus it is very easy to identify as such using these methods. However, these methods can be expanded upon to search for less evident risk significant systems.

1.4.2 Risk Insignificant System

The core spray system, designated as LCS (Low Pressure Core Spray System), was selected as the example risk insignificant system based on suggestions from Mr. K. Vehstedt of NYPA. Only four basic events involving LCS are present in the set of the CDF cutsets, and each occurs only three times in the set of all CDF cutsets, as given in Table 1.5. The LCS events also have both low risk reduction importances and low risk increase importances (Table 1.5).

The LCS system also serves as a good comparison with the ESW system. The LCS system, like the ESW system, has a straightforward configuration and several components that require inspection. The two systems have a very similar component list, as shown in Table 1.6. The dependent components of each system are broken down by component category in Table 1.7.

1.5 Maintenance Rule Applicability to Risk Insignificant SSCs

Once the risk significant SSCs have been identified, other systems not in this category may also be subject to regulation under the Maintenance Rule. Three categories of nonsafety related SSCs are included: those that relate to accident mitigation or the

TABLE 1.5

CORE SPRAY SYSTEM BASIC EVENTS IN THE SET OF CDF CUTSETS

Basic Event	Description	Occurrence*	Risk Reduction Importance (yr^{-1}) [Rank]	Risk Increase Importance (yr^{-1}) [Rank]
LCS-RLY-NO-K9BCL	No output from relay K9BCL	3	8.01E-10 (169.5)	1.86E-06 (163.5)
LCS-RLY-NO-K9ACL	No output from relay K9ACL	3	8.01E-10 (169.5)	1.86E-06 (163.5)
LCS-RLY-NO-17BCL	No output from relay 17BCL	3	8.01E-10 (169.5)	1.86E-06 (163.5)
LCS-RLY-NO-17ACL	No output from relay 17ACL	3	8.01E-10 (169.5)	1.86E-06 (163.5)

*Number of times that the basic event occurs in the total of all top CDF cutsets.

TABLE 1.6

ESW VS. LCS COMPONENT TYPE COMPARISON

Component type	Number of ESW Components	Number of LCS Components
Pump	2	2
MOV	6	10
Manual valve	29	4
Check valve	17	4
Relief valve	6	--
Relay	14	--
HFA Relay	4	--
Relay AGASTAT	--	12
Relay GE-HFA	--	22
Control circuit	6	--
Fuse	8	4
Circuit breaker	12	10
Speed switch	4	--
RX lo level txmtr	--	1
RX lo level trip unit	--	1
RX lo pres txmtr	--	1
RX lo pres trip unit	--	1
DW hi pres txmtr	--	1
DW hi pres trip unit	--	1
Pressure switch	1	--
Strainer	2	--

TABLE 1.7

ESW AND LCS DEPENDENT COMPONENTS

Component type	ESW Component Designator	LCS Component Designator
Pump	46P-2A/B	14P-1A/B
Motor operated valve	15MOV-175A/B 46MOV-101A/B 46MOV-102A/B	14MOV-05A/B 14MOV-07A/B 14MOV-11A/B 14MOV-12A/B 14MOV-26A/B
Manual valve	15RBC-36A/B/C/D 15RBC-39A/B 15RBC-4A/B 15RBC-50 46ESW-10A/B 46ESW-12A/B 46ESW-17A/B/C/D 46ESW-3A/B 46ESW-4A/B/C/D 46ESW-5A/B/C/D 46SWS-23 46SWS-25	14CSP-14A/B 14CSP-18A/B
Check valve	46ESW-11A/B 46ESW-13A/B 46ESW-18A/B/C/D 46ESW-1A/B 46ESW-6A/B 46ESW-9A/B 46SWS-22 46SWS-60A/B	14AOV-13A/B 14CSP-10A/B
Relief valve	15RV-113A/B 15RV-114A/B/C/D	
Relay	42C-1ESWA03/B03 420-1ESWA02/B02 420-1RBCA04/B04 63X-1ESWA04/B04 63Y-1ESWA04/B04 EDGA/B/C/D-ESR-400	

Component type	ESW Component Designator	LCS Component Designator
HFA relay	63A-1ESWA04/B04 63B-1ESWA04/B04	
Relay AGASTAT		02-3A-K101A/B 02-3A-K104A/B 02-3A-K121A/B 02-3A-K123A/B 10A-K133A/B 10A-K134A/B
Relay GE-HFA		14A-K10A/B 14A-K13A/B 14A-K14A/B 14A-K15A/B 14A-K17A/B 14A-K18A/B 14A-K5A/B 14A-K6A/B 14A-K7A/B 14A-K8A/B 14A-K9A/B
Control circuit	46MOV-101A/B 46MOV-102A/B 46P-2A/B	
Fuse	FUSE-AR5A/B FUSE-EDGA/B/C/D FUSE-P-2A/B	71DC-A2 CS A 71DC-B2 CS B PM-14P-1A/B
Circuit breaker	71DCA2-19 71DCA3-06 71DCA4-11 71DCA4-12 71DCB3-01 71DCB4-07 71DCB4-11 71DCB4-12 71MCC-152-OD3 71MCC-162-OD3 71MCC-252-OA1/2 71MCC-262-OD1/2	71-10530 71-10630 71DCA5-03 71DCA5-01 71DCB2-05 71DCB2-16 71MCC-152-OF3 71MCC-153-0B1 71MCC-162-OG2 71MCC-163-0H1

Component type	ESW Component Designator	LCS Component Designator
Speed switch	EDGA/B/C/D-SPSW400	
RX lo level txmtr		02-3LT-72A/B/C/D
RX lo level trip unit		02-3MTU-272A/B/C/D
RX lo pres txmtr		02-3PT-52A/B/C/D
RX lo pres trip unit		02-3MTU-252A/B/C/D
DW hi pres txmtr		10PT-101A/B/C/D
DW hi pres trip unit		10MTU-201A/B/C/D
Pressure switch	15PS-122A/B/C/D	
Strainer	46STR-5A/B	

plant's emergency operating procedures (EOPs), those whose failure could lead to the failure of safety related SSCs, and those whose failure could cause a reactor scram or a safety system actuation. Performance criteria will also have to be established for these SSCs.

NUMARC's (Nuclear Management and Resources Council, Inc.) draft guidelines for monitoring effective maintenance suggest that specific performance criteria be established for all risk significant SSCs, as well as for non-risk significant SSCs that are normally in a standby mode. All risk insignificant normally operating systems should be assigned plant level performance criteria. Plant level performance criteria would include unplanned automatic reactor scrams, unplanned capability loss factor, and unplanned safety system actuations.[4]

Establishing criteria for risk insignificant operating systems based on plant level performance criteria is outside the scope of this thesis. The main concerns of this work are demonstrating methods to classify systems as risk significant or insignificant, and then investigating the rationales of the different inspection requirements of such systems.

CHAPTER II

TESTING AND SURVEILLANCE REQUIREMENTS

2.1 Introduction

In order to assess the inspection needs of a system, the dependent components in the system must be separated by the amount of surveillance and testing that they require. Individual system components that show up as high in risk reduction importance can derive the most benefit from a strong testing and surveillance program. However, it is important to compare the benefits gained from testing procedures to the possibly increased system unavailability that such testing may cause. Conversely, components with low risk increase importance values become candidates for reduced testing and surveillance, since overall plant risk, as measured by CDF, should not increase if a risk insignificant component is allowed to run to failure before undergoing repair.

Several things should be looked at to assess surveillance requirements, including: inspection schedules, routine repair and preventive maintenance schedules, special attention paid to certain components, required recalibration, required system realignment, and scheduled tests. It is important to note that other considerations, such as maintaining high operational availability, may also modify the policy actually applied. The first step, however, is to have a sound understanding of how the system functions.

2.2 ESW System Description

The ESW system provides cooling water to safety systems after a reactor shutdown. Only three of these safety systems are considered to be essential and are examined in the Fitzpatrick Individual Plant Examination (IPE): the control rod drive (CRD) coolers, the crescent area coolers, and the emergency diesel generator (EDG) engine coolers. The CRD pump coolers are normally cooled by the reactor building closed loop cooling system (RBCLCS), with ESW providing a backup. The CRD system provides proper fluid pressure to the hydraulic control rod drives, but can also function as an emergency source of coolant or boron injection into the core. The crescent area coolers are normally cooled by the service water system, with the ESW providing a backup. The crescent area cooler's ten cooling coil-fan units provide cooling to RHR loops A and B, core spray loops A and B, and HPCI (High Pressure Coolant Injection). All four EDG's coolant systems use the ESW as their source of heat removal.

One of the main reasons for the importance of ESW is its crucial role in providing backup power in the event of a loss of off-site power (LOSP) scenario. Without the ESW system, the diesels will not run. If the EDGs cannot be started after a LOSP event, a station blackout (SBO) occurs and all emergency systems have to be run off of battery power. Depending on the accident scenario, the batteries will fail at between 2 - 13 hours, leading to a loss of core cooling and eventual core damage.

The ESW system has two completely redundant loops, each with a separate pump. Each loop is powered off of a separate emergency bus. The ESW pumps start up automatically upon a EDG start or low RBCLCS discharge header pressure signal. Each pump can be started manually from the control room, and ESW loop B can also be started or shut down from the alternate shutdown panel ASP-3. The system requires a manual shut down, which can only be performed if the associated EDGs are shut down and the RBCLCS is properly configured in the "lockout matrix". The ESW system schematic diagram is shown in Figures 2.1.1, 2.1.2, and 2.1.3.

Table 2.1 shows the total list of ESW basic events occurring in the set of internal core damage cutsets, ranked by risk reduction importance. This list is a good indicator of the level of risk significance that can be attached to each ESW component. It is interesting to note that the first and third most important risks are the unavailability of loops B and A, respectively, due to maintenance. This points out that increased maintenance is not always the answer to reducing risk, although performing maintenance may be unavoidable if a component has a limited operating lifetime.

The single set of components with the highest risk reduction importances is that of the ESW pumps. There are several important modes of pump failure: common-cause and single failures of the pumps to run, common-cause and single failures of the pump to start, no output from the control circuits associated with the pumps, and human failures to restore the pumps to their correct position.

Another important failure in the ESW system is a human failure to restore the manual supply valves ESW-3A or 3B to their normally locked-open position. It is also possible for these valves to become plugged, although this event is considered less risk significant than human error. The ESW-3A pathway provides cooling water to EDG A

ESW SYSTEM VALVE ALIGNMENTS ARE SHOWN IN THEIR NORMAL STANDBY POSITIONS
NOTE: ONLY CRESCENT AREA COOLERS, RHR, CRD AND EDG'S COOLING LOADS ARE REPRESENTED

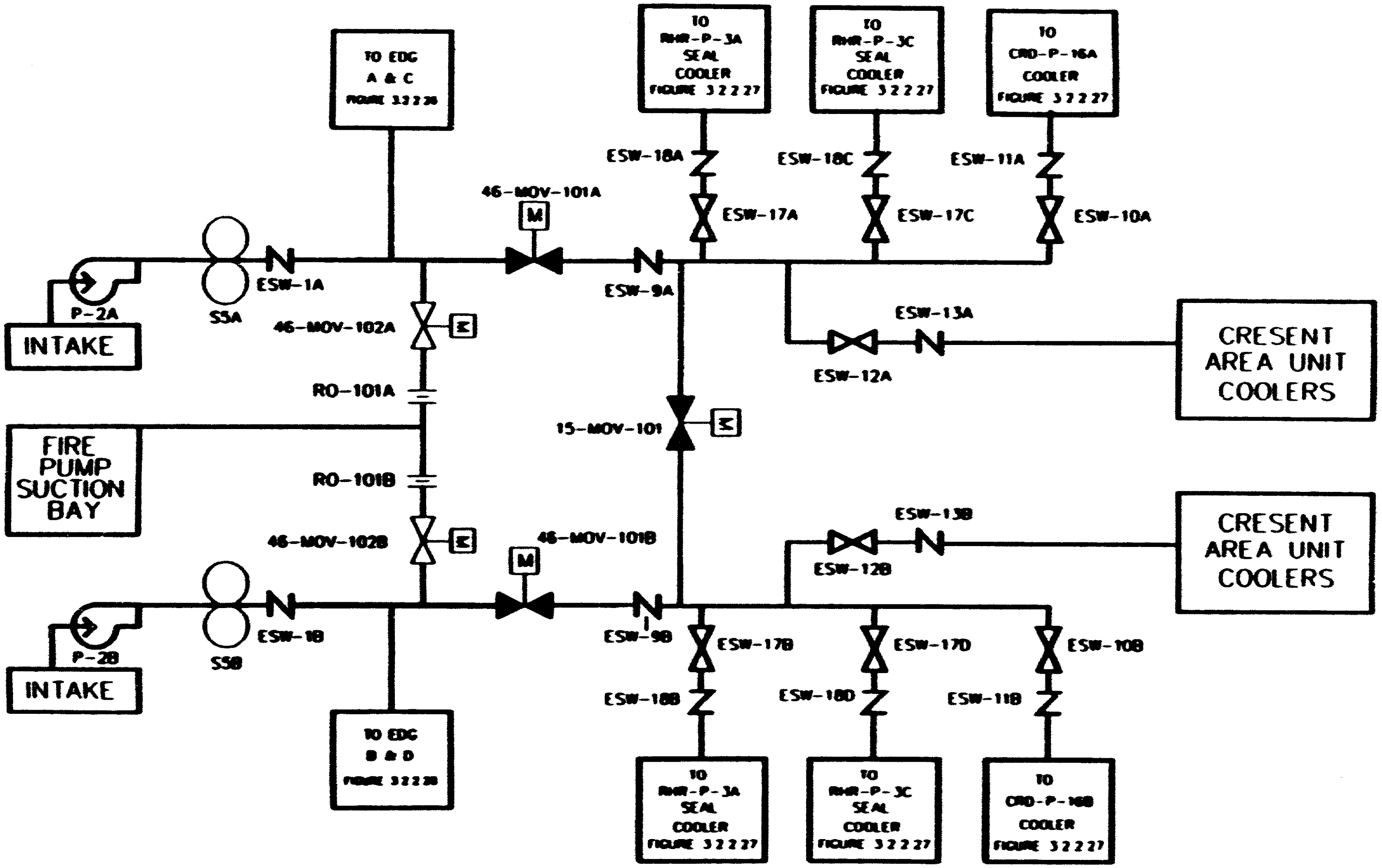


Figure 2.1.1 Emergency Service Water System Schematic Diagram[5]

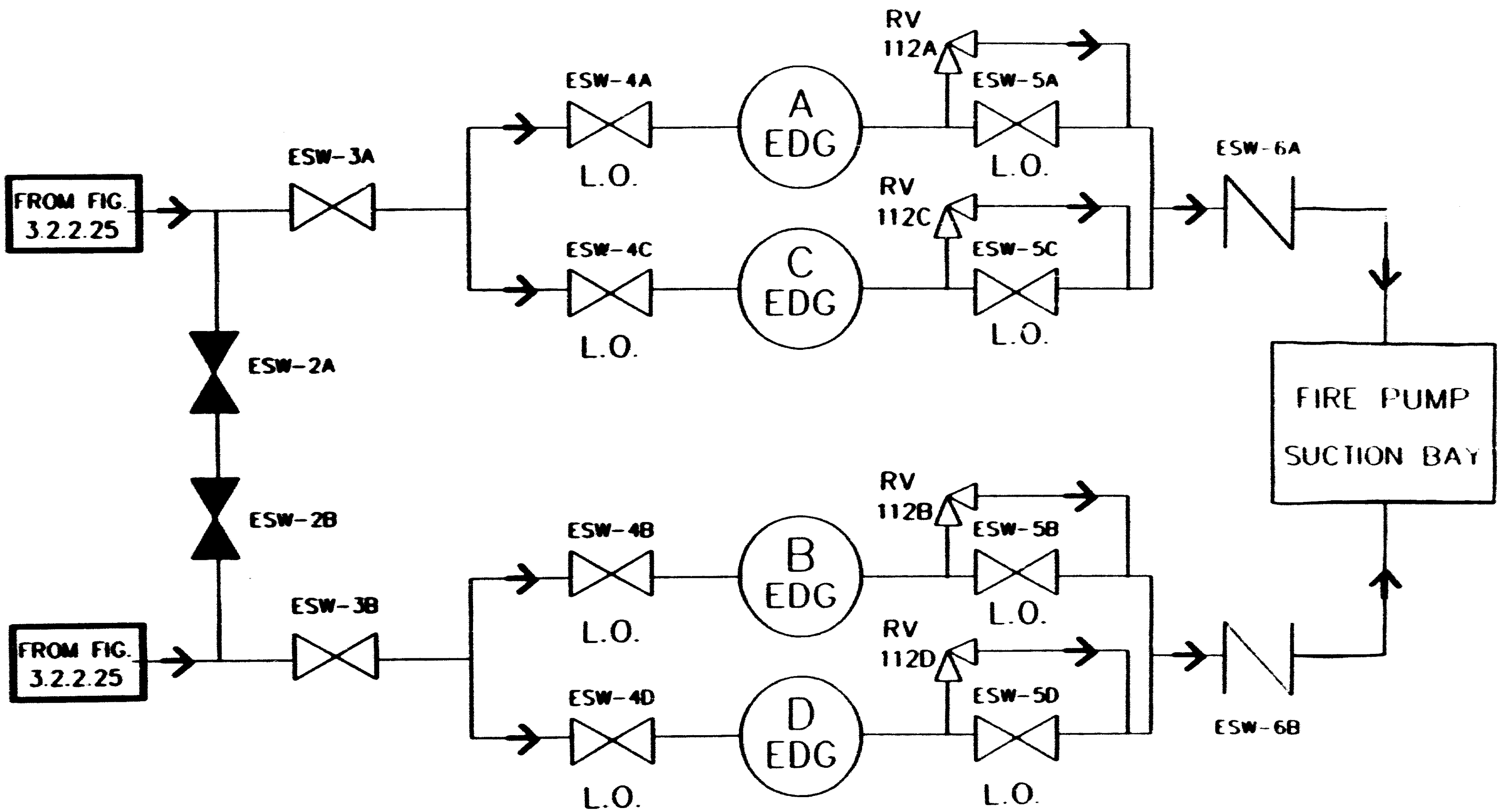


Figure 2.1.2 Emergency Service Water System Schematic Diagram (continued)[5]

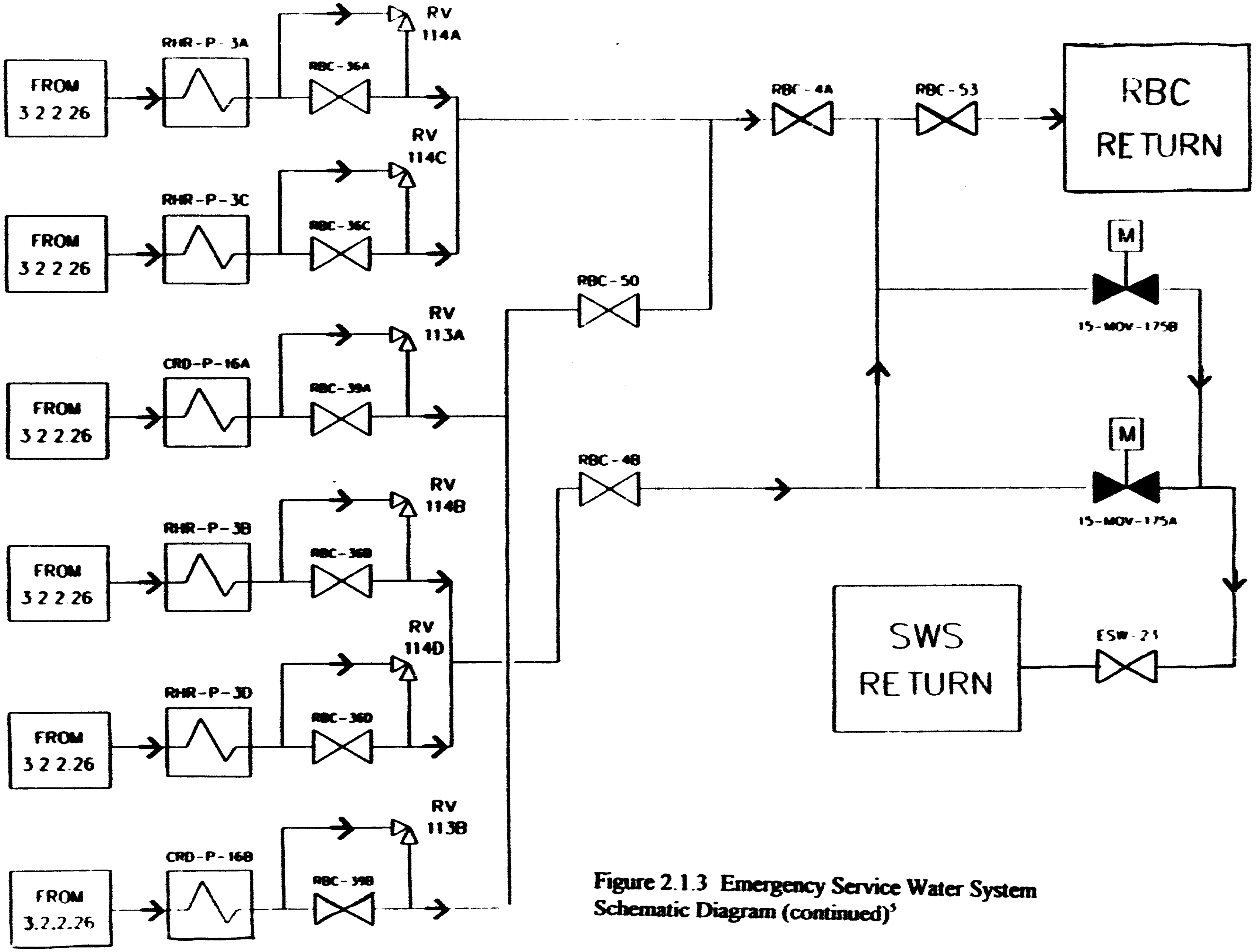


Figure 2.1.3 Emergency Service Water System Schematic Diagram (continued)[5]

FIGURE 2.1.4 SCHEMATIC LEGEND

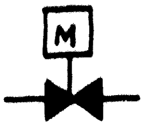
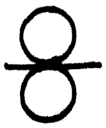
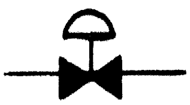
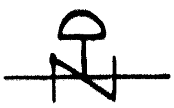
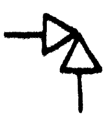
Symbol	Component
	manually operated valve (shown open)
	motor operated valve (shown closed)
	check valve
	pump
	strainer
	restricting orifice
	pressure control valve
	air operated valve
	relief valve

TABLE 2.1

RISK REDUCTION IMPORTANCE VALUES FOR ESW TOP EVENTS

Basic Event	Risk Reduction(yr^{-1})	Rank	Description
ESW-MAI-MA-LOOPB	2.42E-07	5	Loop B unavailable due to maintenance
ESW-CCF-FR-PUMPS	1.78E-07	8	CCF to run of pumps
ESW-MAI-MA-LOOPA	1.50E-07	9	Loop A unavailable due to maintenance
ESW-MDP-FR-P2A	1.48E-07	10	Failure to run of pump P2A
ESW-MDP-FR-P2B	1.41E-07	11	Failure to run of pump P2B
ESW-CCF-FS-PUMPS	9.76E-08	14	CCF to start of pumps
ESW-XHE-RE-ESW3A	9.64E-08	15.5	Human error (failure to restore to correct position) of manual valve 46ESW-3A
ESW-XHE-RE-ESW3B	8.95E-08	17.5	Human error (failure to restore to correct position) of manual valve 46ESW-3B
ESW-RCK-NO-P2A	3.36E-08	30.5	No output from control circuit 46P-2A associated with pump 2A
ESW-RCK-NO-102A	3.36E-08	30.5	No output from control circuit 46MOV-102A associated with MOV-102A
ESW-RCK-NO-102B	3.09E-08	32.5	No output from control circuit 46MOV-102B associated with MOV-102B
ESW-RCK-NO-P2B	3.09E-08	32.5	No output from control circuit 46P-2B associated with pump 2B
ESW-XHE-RE-P2A	1.73E-08	41	Human error (failure to restore to correct position) of pump P2A
ESW-CCF-OO-102AB	1.64E-08	42	CCF of normally open MOVs 102A/B to close on demand
ESW-XHE-RE-P2B	1.57E-08	44	Human error (failure to restore to correct position) of pump P2B

Basic Event	Risk Reduction(yr^{-1})	Rank	Description
ESW-RCS-OO-A63A9	8.04E-09	70.5	Failure of normally open contacts associated with HFA relay 63A to close on demand
ESW-RCS-OO-B63A9	7.13E-09	81.5	Failure of normally open contacts associated with HFA relay 63B to close on demand
ESW-MOV-OO-102A	4.39-E-09	103	Failure of normally open 46MOV-102A to close on demand
ESW-MOV-OO-102B	3.82E-09	107	Failure of normally open 46MOV-102B to close on demand
ESW-RCI-FE-A63A	3.13E-09	113	Electrical relay coil associated with HFA relay 63A-A fails to energize
ESW-RCI-FE-A42C	3.13E-09	113	Electrical relay coil associated with relay 42C-A fails to energize
ESW-MDP-FS-P2A	2.98E-09	115	Pump P2A fails to start
ESW-RCI-FE-B63A	2.74E-09	118	Electrical relay coil associated with HFA relay 63A-B fails to energize
ESW-RCI-FE-B42C	2.74E-09	118	Electrical relay coil associated with relay 42C-B fails to energize
ESW-MDP-FS-P2B	2.61E-09	122	Pump P2B fails to start
ESW-CKV-CC-ESW6A	2.18E-09	130.5	Normally closed check valve 46ESW-6A fails to open on demand
ESW-CKV-CC-ESW1A	2.18E-09	130.5	Normally closed check valve 46ESW-1A fails to open on demand
ESW-CKV-CC-ESW6B	1.86E-09	138.5	Normally closed check valve 46ESW-6B fails to open on demand
ESW-CKV-CC-ESW1B	1.86E-09	138.5	Normally closed check valve 46ESW-1B fails to open on demand
ESW-XVM-PG-ESW3A	6.92E-010	177	Manual valve 46ESW-3A plugged
ESW-XVM-PG-ESW3B	5.90E-10	178	Manual valve 46ESW-3B plugged

and C, and the ESW-3B pathway supplies EDG B and D. If one of these valves is left closed or plugged it will completely cut off the coolant flow to the affected set of EDGs.

The motor operated valves 46MOV-102A and B are also involved in several failure scenarios. These normally open MOVs are designed to close upon receipt of a low RBCLCS pressure signal which directs flow to the RBCLCS. If one or both of these valves remain open when 46MOV-101A/B and 15MOV-175A/B open to direct flow to the RBCLCS, it is assumed that there will be insufficient flow from the affected loop to the EDGs. There are several modes of 46MOV-102A/B failure: no output from the control circuit associated with the MOV, a common-cause failure of both MOVs to close, or an independent failure to close.

There are two other important ways in which an entire ESW loop can be lost. If the normally closed check valve 46ESW-1A/B, located after the intake tunnel strainer, fails to open, no water will be available from that ESW loop. If the normally closed check valve ESW-6A/B, located at the EDG discharge to the fire pump suction bay, fails to open, the EDG cooling for that loop again fails.

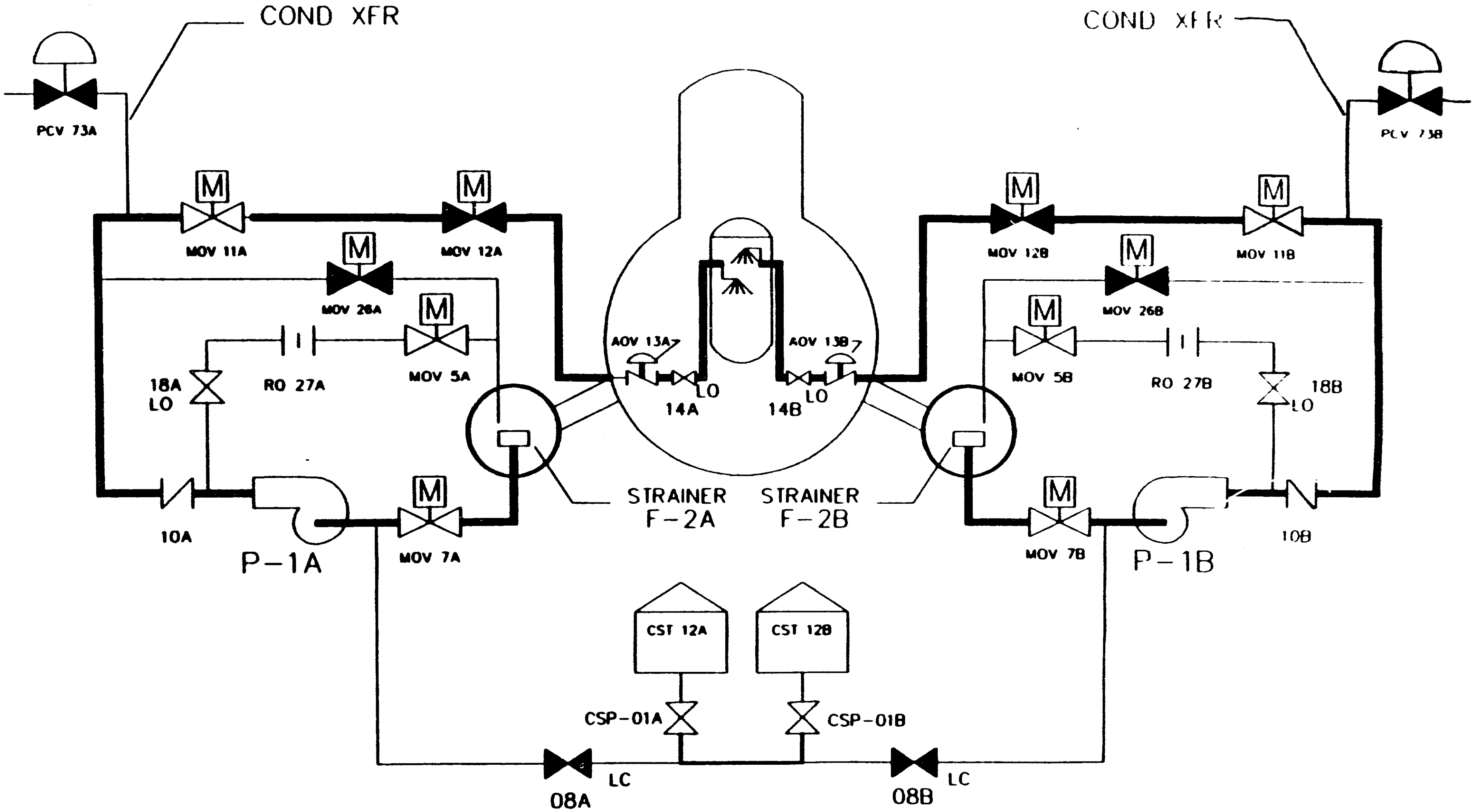
2.3 LCS System Description

The core spray system provides reactor core cooling during transients when the system pressure is low. If HPCI is unable to maintain a sufficient water level, core spray can provide protection if the automatic depressurization system (ADS) has properly reduced reactor vessel pressure. There are two independent core spray loops, each including an electric-motor-driven centrifugal pump that discharges through a spray sparger above the core. Each pump is powered through a separate electrical bus. Core spray initiates upon receipt of a high drywell pressure or low-low-low reactor water signal, with the pumps taking suction from the suppression pool. The LCS system schematic is shown in Figure 2.2.

The standby system is kept full of water to avoid a water hammer event upon initiation of the LCS system. The pump is protected from damage due to overheating during no- or low-flow operation by a minimum flow bypass line located between the pump discharge and the suppression pool. The inboard and outboard motor operated valves (14MOV-11A/B and 14MOV-12A/B) are interlocked so that both cannot be opened if the reactor pressure is above 450 psig. This prevents the LCS low-pressure piping from being damaged by exposure to high-pressure reactor water.

The risk insignificance of the LCS system arises not from its function, emergency water addition, but from the fact that other reactor systems exist which can perform the same function. Water can be supplied to the core through HPCI or the CRD system under high-pressure conditions, and through LPCI under low-pressure conditions. Thus the failure of the core spray system does not mean that water cannot be supplied to the core under transient or LOCA conditions. Other system failures would be required in addition to LCS failure for the reactor core to be without an emergency water supply.

Only four basic events involving the LCS system appear in the set of all CDF cutsets, as shown in Table 1.5.



NOTE: VALVES ARE SHOWN IN THEIR STANDBY POSITION

Figure 2.2 Core Spray System Schematic Diagram[5]

2.4 System Unavailability

System unavailability can be caused by failures in the system that must be repaired or by scheduled testing that places the system in a non-recoverable state. System unavailability due to system component failures will lead to unscheduled tests and maintenance. The failure rate of the system determines the unscheduled system unavailability. The ESW and LCS systems are comprised of similar components with similar failure probabilities; see Table 2.2 for a comparison of Fitzpatrick's plant-specific failure data for the two systems. It is important to realize that the risk significance of the ESW system does not imply that the system has a higher failure rate than the LCS system, only that its failure is more dangerous to the plant. A comparison of ESW and LCS unavailability due to unscheduled test and maintenance[5] shows their unavailabilities due to maintenance are all within the same order of magnitude:

Description	Probability
ESW Loop A Unavailable due to Maintenance	6.89E-03
ESW Loop B Unavailable due to Maintenance	9.85E-03
LCS Loop A Unavailable due to Maintenance	8.13E-03
LCS Loop B Unavailable due to Maintenance	7.21E-03

Both the ESW and the LCS systems have scheduled tests and surveillances. Because of the safety functions of each of these systems, most time-consuming intrusive preventive maintenance is performed only while ~~not~~ the reactor is not operating at full power. Maintenance performed while the reactor is not at full power was not considered in the Fitzpatrick IPE as contributing to system unavailability. However, if work

TABLE 2.2

JAMES A. FITZPATRICK PLANT-SPECIFIC FAILURE DATA[8]*

Failure Event	Event Description	ESW Mean Failure Probability	LCS Mean Failure Probability
CKV CC	Check valve, normally closed, fails to open	9.21E-05	9.90E-05
CKV OO	Check valve, fails to reclose on demand	1.00E-03	---
FLT PG	Strainer plugs	2.96E-06	---
MDP FR	Motor driven pump fails to continue running	1.88E-04	2.10E-04
MDP FS	Motor driven pump fails to start	1.24E-04	2.05E-04
MOV CC	Motor operated valve, normally closed, fails to open	2.37E-04	2.34E-04
MOV OO	Motor operated valve, normally open, fails to close	1.74E-04	1.58E-04
MOV PG	Motor operated valve plugs	1.25E-07	1.25E-07
PSW DN	Pressure switch does not open	---	1.00E-04**
RCI FE	Electrical relay coil does not energize	1.30E-04***	1.30E-04***
RCK NO	Control circuit, no output	1.11E-03	7.68E-04
RCS CO	Contacts, normally closed, fail to remain closed	---	2.70E-07****
RCS OO	Contacts, normally open, fail to close	3.00E-04****	3.00E-04****
SBR DN	Circuit breaker does not operate	2.24E-03	---

Failure	Description	ESW Mean Failure Rate	LCS Mean Failure Rate
STR PG	Strainer plugs	2.96E-06	---
XVM OC	Manual valve plugs	1.00E-07	1.00E-07

* Data taken from James A. Fitzpatrick Plant-Specific Data unless otherwise indicated.

** Data taken from: A. D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," Sandia National Laboratories, NUREG/CR-4772, SAND86-1996, February 1987.

*** Data taken from: S. E. Mays et al., "Interim Reliablility Evaluation Program: Analysis of the Browns Ferry, Unit 1, Nuclear Plant," EG&G Idaho, Inc. and Energy Inc., NUREG/CR-2802, EG&G 2199, July 1982.

**** Data taken from: U. S. Nuclear Regulatory Commission, "Risk Methods Integration and Evaluation Program (RMIEP) Methods Development: A Data-Based Methodology for Including Recovery Actions in PRA," Report NUREG/CR-4832, Vol. 1, 1990.

performed while the reactor was not at power had the potential to leave the system in a disabled state, such errors were taken into account. This takes into account, for example, the human error of leaving a system in an incorrect configuration.

The ESW system has almost no full-power system unavailability due to scheduled tests and maintenance. Most configurations existing during full-power testing will automatically self-correct if a demand is received for the system to function. One exception is the ESW Pump Flow Rate Test, which involves the closing of manual valves 46ESW-3A/B. Closing valve 3A cuts off ESW flow pathway to diesel generators A and C, while valve 3B provides a flow pathway for diesel generators B and D. The system unavailability stemming from performing this test every three months, at approximately five minutes down time per test, was considered too small to be included in the IPE. The ESW Logic System Functional Test also requires closing the manual valves 46ESW-10A/B, which isolate the CRD pump coolers from their cooling backup system once per operating cycle. The most important risk from performing these procedures lies in the possibility of human failure to reopen the valves after testing.

The LCS has scheduled surveillance that leads to the level of system unavailability represented in the Fitzpatrick IPE. The semiannual LCS Subsystem A/B Logic Functional Test makes either loop A or loop B unavailable and leads to a probability of system unavailability of 9.0E-04.

2.4.1 Scheduled Tests and Surveillances

The tests performed on the ESW system are the following:

- ESW Logic System Functional Test and Simulated Automatic Actuation Test (ST-8E),
- ESW Pump Flow Rate Test (ST-8D),
- EDG Full Load Test and ESW Pump Operability Test (ST-9B),
- Emergency Service Water Lockout Matrix Instrument Functional Test/Calibration (ISP-23),
- Reactor Building Closed Loop Cooling Containment Isolation AOV Exercise (ST-1R),
- ESW Motor Operated Valve Operability Test (ST-8C).

Maintenance on the ESW pumps, performed only while the reactor is not at full power, follows Maintenance Procedure MP-46.1, "RHR Service Water Pumps and Emergency Service Water Pumps".

The tests performed on the core spray system are the following:

- Core Spray Initiation Logic Functional Test (ST-3J),
- Core Spray Simulated Automatic Actuation (ST-3B),
- Core Spray Pump and Valve Operability Test (ST-3A),
- Reactor Level (ECCS) Transmitter Calibration and Channel Functional Test (ATTS) (ISP-276A),
- Reactor Pressure (ECCS) Transmitter Calibration and Channel Functional Test (ATTS) (ISP-275A),
- Reactor and Containment Cooling Instrument Functional Test/Calibration (ATTS) (ISP-175A).

Maintenance on the LCS pumps, performed only while the reactor is not at full power, follows Maintenance Procedure MP-014.01, "Core Spray Pump Maintenance".

2.4.2 Procedures for the ESW System

Because the ESW system is a very important standby system, invasive maintenance that would contribute to system down time while the reactor is at power is avoided. The system logic is designed to automatically realign to the proper system configuration in the event of a system demand. Thus if a motor operated valve were to be incorrectly aligned due to testing, it would automatically return to the proper configuration given a demand signal. Only automatic valves have this capability. Manually operated valves that are perturbed from their correct configuration would prevent proper operation if a demand for the system occurred while the valves were being tested. More importantly (given the short amount of time that valves are in their test configurations), there would exist for manually operated valves the human error potential to leave the valve in an incorrect position.

All ESW motor operated valves (MOVs) are inspected monthly in the ESW Motor Operated Valve Operability Test (ST-8C). This test is performed automatically from the control room. Each valve is cycled through the open and closed positions remotely. The MOV position is indicated as being either open or closed. If the valve were to fail to fully open or close, this intermediate position would be indicated by both lights being on, and proper corrective action could then be taken.

Once per quarter a test and calibration of the ESW lockout matrix system (ISP-23) is performed. This involves a test and calibration of the pressure switches that will cause the injection of ESW flow into the RBCLCS (reactor building closed loop cooling system) in the event of low RBCLCS discharge header pressure. The function of the ESW system to inject water into the RBCLCS system is no longer as risk important as it was when the Fitzpatrick IPE was written, due to system modifications. ESW now injects such a small amount of water into the RBCLCS that EDG cooling capability is not lost if there is a RBCLCS low pressure demand.

Once per quarter an ESW Pump Flow Rate Test (ST-8D) is performed. Piping downstream of the ESW pumps is vented, and the pumps are isolated. This involves the closure of the manually operated valves that supply ESW to the diesel generators, temporarily causing EDG unavailability. The pumps are then run to check their discharge pressures, and the system is returned to its normal configuration. ESW inlet tunnel water elevation is also checked. The Fitzpatrick Technical Specifications currently require this test to be performed quarterly. However, according to Mr. K. J. Vehstedt, Senior Engineer in Nuclear Generation, Fitzpatrick is currently in the process of requesting a Tech Spec change allowing them to perform this test with reduced frequency. This would reduce the amount of human error probability for leaving closed the manually operated valves supplying the EDGs.

The ESW logic is tested once per operating cycle of eighteen months, in the ESW Logic System Functional Test and Simulated Automatic Actuation Test (ST-8E). This test verifies that an ESW demand signal from either a low RBCLCS pressure or the ESW lockout matrix relays will cause the ESW pumps to start and all MOVs to reposition for ESW injection. Water is not actually injected into the RBCLCS because all of its loads are isolated. This isolation involves the closure of the manual valves supplying the CRD pump coolers, which must be reopened to inject ESW into the RBCLCS.

During the logic test the ESW system is vented to test that the system is full of water. A low pressure RBCLCS signal is simulated, causing the ESW system to align for RBCLCS injection and the ESW pumps to start. The system is then returned to the standby lineup.

The ESW system is required to operate monthly during the EDG Full Load Test and ESW Pump Operability Test (ST-9B). During this test each pair of EDGs is required to carry a full rated load. Each ESW pump associated with a pair of EDGs is tested for the ability to start upon EDG initiation and to provide sufficient ESW cooling flow. This monthly test also checks that the ESW system is properly aligned for EDG cooling

2.4.3 Procedures for the LCS System

Invasive maintenance and testing while the reactor is at full power is also avoided in the Core Spray system. The only exception is the Core Spray Initiation Logic Functional Test (ST-3J), which is performed every six months. This test demonstrates that the LCS system automatically initiates properly. During this test the injection valve inside the primary containment is de-energized, making the system unavailable. Each initiation sensor is tested for the ability to initiate core spray. LCS pumps and valves are activated to test for proper operation.

The Core Spray Pump and Valve Operability Test (ST-3A) is performed monthly. Each MOV is operated remotely and proper performance is verified by means of indicating lights. Each core spray pump is run, although water is circulated to the torus and not actually injected into the reactor.

The Reactor Pressure (ECCS) Transmitter Calibration and Channel Functional Test (ISP-275A and B) is performed once per operating cycle in order to calibrate various pressure transmitters. Sensors for the emergency core and containment cooling system (ECCS), alternate rod injection (ARI) and the recirculation pumps are tested. Only two sets of these transmitters, 10PT-101A/B/C/D and 02-3PT-52A/B/C/D, will cause a LCS initiation.

The Reactor Level (ECCS) Transmitter Calibration and Channel Functional Test (ISP-276A and B) is performed once per operating cycle in order to calibrate the reactor level transmitters for the ECCS system. A positive signal from one set of these sensors, 02-3LT-72A/B/C/D, is needed to cause an LCS initiation.

The Reactor and Containment Cooling Instrument Functional Test/Calibration (ISP-175A and B) is performed once per month to test analog trip functions and once every six months to calibrate the master and slave trip units. The procedure is generic to several different sets of instrumentation associated with the ECCS, alternate rod insertion system (ARI) and recirculation pumps. The master trip units for the two pressure sensors and the single reactor level sensor that will initiate core spray are all calibrated during this procedure.

The Core Spray Simulated Automatic Actuation Test (ST-3B) is performed once per eighteen month operating cycle, to demonstrate that the LCS system will automatically inject water into the reactor if a high drywell pressure signal is received. The prerequisites for this procedure require that it be performed only during cold shutdown, because this test actually injects core spray water into the reactor pressure vessel (RPV). Each LCS loop is drained to the torus and refilled through the condensate storage tank. A high drywell pressure signal is simulated to initiate LCS injection into the RPV. RPV water level has to be lowered after the first Core Spray loop is tested before commencing the test of the second loop.

CHAPTER 3

RISK-BASED RESOURCE ALLOCATION

3.1 Introduction

As the proceeding chapter shows, each plant system undergoes a process of continuous testing and surveillance. However, plant resources are limited. With only a finite amount of time and money to be spent inspecting and testing plant systems, some choices among inspection schedules have to be made. One method of making such choices, as previously mentioned, is through the use of PRA to prioritize system inspection importance. However, in order to understand and fully appreciate the radical change from the current methods of scheduling which this would represent for resource allocation, it is necessary to understand where the original set of system procedures originated.

The procedures required for monitoring the condition of plant systems are outlined in each plant's Technical Specifications (Tech Specs). These Tech Specs must be adhered to strictly at all times, except in certain accident scenarios. The required frequency for each system surveillance is outlined in the Tech Specs. For the various reactor safety systems, including ESW and LCS, the original Tech Spec requirements were driven by ASME inspection recommendations[4]. The other Fitzpatrick safety systems, such as HPCI and RCIC, show much similarity in their surveillance testing requirements, such as: monthly pump and MOV testing, a simulated automatic actuation test once per operating cycle, and monthly pump flow rate testing (quarterly for LCS). Although not all of the surveillance frequencies are the same, reflecting the diversity and differing degrees of complexity among these safety systems, their standard ASME basis is evident.

Although such standardization facilitates the process of developing surveillance requirements for the numerous plant systems, such across-the-board requirements for testing and surveillance do not reflect the different degrees of importance of each plant system. The NRC Maintenance Rule specifies that each licensee must develop performance goals and a method of measuring whether or not structures, systems, and components are meeting these goals. It would be reasonable to develop criteria for performance goals reflecting each system's differing degree of importance to safety. These criteria must also measure each system's importance in terms of the effort which should be expended in order to ensure the system's high reliability. Basic maintenance required to ensure a system's operability must always be performed, and is not subject to change.

In the following two sections two ratios are developed between each component's staff time burden arising from implementing plant testing and inspection procedures, and the risk that can be associated with the component. We use the staff time burden as a surrogate for the sum of the resources expended during a time interval in order to ensure high component reliability. The purpose of our analysis is to illustrate a method of allocating resources on a risk basis. Ideally, this ratio of resources to risk should be uniformly constant for all of the plant's safety-related components.

3.2 ESW and LCS Resource Allocation per Component

It is necessary to measure in a quantitative way the amount of available plant resources expended on different systems. Such a measure is hard to quantify accurately with the available plant data. This is because only routine surveillance and testing work can be easily accounted for, as it is difficult to estimate the amount of effort expended on individual components during the additional testing that corrective maintenance might require. There is very little plant data available regarding such unanticipated work. However, from a knowledge of routine plant procedures an estimate can be made as to the amount of effort expended per system, which can then be extrapolated to individual components.

It is important to differentiate between the amount of effort expended to ensure the reliability of a system, and effort that is required to keep the system operable. Certain components may be designed for a finite lifetime, after which they require either reworking or replacement. This type of work is a necessity and is not subject to change resulting from competition for resources. However, much of the time and effort expended upon a system is devoted to ensuring the reliability of the system, and to catching unexpected system failures. This is the type of time burden that is of interest here. It is reasonable to link the degree of reliability desired to the risk significance of the system.

Thus the staff time burden evaluated here deals only with testing and surveillance procedures that are performed to ensure system reliability. Routine preventive maintenance required to maintain the basic operation of system components was not included. Of course, in the two example systems selected very little preventive maintenance is required because both of the systems are of the standby type, designed for high reliability. The only exception is the annual changing of upper and lower ESW pump motor bearing reservoir oil. This preventive maintenance takes each ESW pump out of service for 4 hours annually. This time burden was not included in this study.

The routine procedures for the ESW and LCS systems have already been explained in Chapter 2. From these procedures an estimate of the amount of time expended per component can be derived. First, each procedure was reviewed to determine which components were tested or inspected during the procedure. Two different actions were each considered to constitute a test: that of forcing a required response to occur or of perturbing a component in order to produce a system alignment which would permit a test. Forcing a required action to occur involves cycling (opening and closing) a valve, or simulating a signal to turn on a pump. However, some tests require having a system in a certain configuration, usually involving isolating part of the system. Perturbing a valve setting in order to create a desired system test configuration and then returning the valve to its original state after the procedure is also considered to constitute a component test.

An estimate of the number of workerhours required is difficult to obtain. Only three of the procedures involving the ESW and LCS systems have a section requesting staff members performing the procedure to document the number of workerhours they spent performing the procedure: the EDG Full Load Test, the ESW Pump Flow Rate Test, and the ESW Logic Test. The Fitzpatrick Nuclear Power Plant staff generally does not keep data on workerhours expended per system or per procedure. Furthermore, the actual start and finish times for each procedure may not be representative of the actual amount of time spent working on the system. During outages when the system is not required to be on-line, a system may not be worked on continuously due to the increased resource demands elsewhere.

In conjunction with Mr. K. Vehstedt, estimates have been developed for the amount of effort, or burden, required by each procedure. These time estimates were then broken down by component. For most of the procedures each component involved was assigned the full procedure time. However, for procedures involving several systems only the ESW or LCS portion was included. Only ESW pump running time was accounted for from the EDG Full Load Test, as considerable time is spent during this test on diesel generator inspection which does not affect the ESW pumps. Only LCS instrument testing was considered in the Reactor Level and Reactor Pressure Transmitter Calibration and Channel Functional Tests and the Reactor and Containment Cooling Instrument Functional Test/Calibration.

The total estimated time burden per component per test is shown in Tables 3.1 and Table 3.2. The time per test is multiplied by the procedure frequency to obtain the total time expended per 18 month plant refueling cycle. It should be emphasized that the values shown are only estimates. A plant program to record the amounts of time expended in actual procedures would be required to attain more accurate numbers. However, an estimate is sufficient to illustrate the methodology presented here.

TABLE 3.1

ESW SYSTEM TIME BURDEN BY COMPONENT

Component	Test Designation	Component Function	Test Frequency (per 18 month refueling cycle)	Time Spent Per Test (hours per loop)	Total Time Spent Per 18 Month Refueling Cycle (hours per loop)
46P-2A/B pumps	ST-8E	start/stop	1	3	3
	ST-8D	start/stop	6	1	6
	ST-9B	start/stop	18	1	18
	ST-8C	start/stop	18	0.25	4.5
46MOV-102A/B motor op. valve	ST-8E	close/open	1	3	3
	ST-8D	c/o	6	1	6
	ST-8C	c/o	18	0.25	4.5
46MOV-101A/B motor op. valve	ST-8E	o/c	1	3	3
	ST-8C	o/c	18	0.25	4.5
15MOV-175A/B motor op. valve	ST-8E	o/c	1	3	3
	ST-8C	o/c	18	0.25	4.5
46ESW-3A/B manual valve	ST-8D	c/o	6	1	6
	ST-9B	flow through	18	1	18

Component	Test Designation	Component Function	Test Frequency (per 18 month refueling cycle)	Time Spent Per Test (hours per loop)	Total Time Spent Per 18 Month Refueling Cycle (hours per loop)
46ESW-10A/B manual valve	ST-8E	c/o	1	3	3
46ESW-23 manual valve	ST-8E	c/o	1	3	3
46ESW-30B manual valve	ST-8E	c/o	1	3	3
46ESW-1A/B check valve	ST-9B	flow through	18	1	18
46ESW-6A/B check valve	ST-9B	flow through	18	1	18
42C-1ESWA03 42C-1ESWB03 relays	ST-8E	test	1	3	3
63A/B-1ESWA04 63A/B-1ESWB04 HFA relays	ST-8E	test	1	3	3
15PS-122A/B/C/D pressure switch	ISP-23	test	6	1	6

TABLE 3.2

LCS SYSTEM TIME BURDEN BY COMPONENT

Component	Test Designation	Component Function	Test Frequency (per 18 month refueling cycle)	Time Spent Per Test (hours per loop)	Total Time Spent Per 18 Month Refueling Cycle (hours per loop)
14P-1A/B pump	ST-3A	start/stop	18	1	18
	ST-3B	start/stop	1	3	3
	ST-3J	start/stop	3	5.5	16.5
14P-2A/B holding pump	ST-3B	stop/start	1	3	3
14MOV-5A/B motor op. valve	ST-3A	close/open	18	1	18
	ST-3B	c/o	1	3	3
	ST-3J	c/o	3	5.5	16.5
14MOV-7A/B motor op. valve	ST-3A	c/o	18	1	18
	ST-3B	c/o	1	3	3
14MOV-11A/B motor op. valve	ST-3A	c/o	18	1	18
	ST-3J	c/o	3	5.5	16.5
14MOV-12A/B motor op. valve	ST-3A	o/c	18	1	18
	ST-3B	o/c	1	3	3

Component	Test Designation	Component Function	Test Frequency (per 18 month refueling cycle)	Time Spent Per Test (hours per loop)	Total Time Spent Per 18 Month Refueling Cycle (hours per loop)
	ST-3J	o/c	3	5.5	16.5
14MOV-26A/B motor op. valve	ST-3A	o/c	18	1	18
	ST-3B	o/c	1	3	3
	ST-3J	o/c	3	5.5	16.5
14CSP-8A/B manual valve	ST-3B	o/c	1	3	3
14CSP-18A/B manual valve	ST-3B	c/o	1	3	3
14CSP-61A/B manual valve	ST-3B	c/o	1	3	3
14CSP-69A/B manual valve	ST-3B	o/c	1	3	3
14CSP-74A/B manual valve	ST-3B	o/c	1	3	3
14A-K9A/B relay GE-HFA	ST-3J	test	3	5.5	16.5
14A-K17A/B relay GE-HFA	ST-3J	test	3	5.5	16.5
02-3LT-72A/B/C/D RX lo level txmtr	ISP-276A/B	test & calibrate	1	4	4

Component	Test Designation	Component Function	Test Frequency (per 18 month refueling cycle)	Time Spent Per Test (hours per loop)	Total Time Spent Per 18 Month Refueling Cycle (hours per loop)
02-3PT-52A/B/C/D RX lo pres txmtr 10PT-101A/B/C/D DW hi pres txmtr	ISP-275A/B	test & calibrate	1	8	8
02-3MTU-252 02-3MTU-272 10-MTU-201 A/B/C/D master trip units	ISP-175A/B	test	1	16	16

3.3 Ratio of Time Burden Versus Risk Reduction and Risk Increase Importances

In order to measure whether current testing and surveillance procedures are well balanced with regard to the risk significance of the system to which they apply, ratios of the staff time burden to the component's risk reduction and risk increase importances were calculated for each significant component in the ESW and LCS systems. As is discussed previously, the risk reduction importance (RRI) is a measure of the decrease in the value of the CDF that occurs if the basic event (component failure in this case) is eliminated by setting its probability of occurrence equal to zero. Risk increase importance (RII) is a measure of the increase in the value of the CDF that occurs if the probability of the basic event is set to unity. By comparing the ratios corresponding to different components, disparities between risk significance and the staff time expended while inspecting various components will become evident.

The RRI versus time burden ratios are identified in Tables 3.3 and 3.4. The RII versus time burden ratios are identified in Tables 3.5 and 3.6. ESW system component rankings for both risk/burden ratios are given in Table 3.7. LCS system component rankings for both risk/burden ratios are given in Table 3.8.

Several of the more important components have more than one basic event associated with them, corresponding to different failure modes. For these components the total risk reduction or risk increase importance is the sum of all the possible different failure modes. This sum, as shown in Tables 3.3 - 3.6, was used to calculate the final risk/burden ratios. In this way all possible modes of failure of a component are accounted for in the final ratios.

TABLE 3.3

ESW SYSTEM COMPONENT RISK REDUCTION IMPORTANCE VERSUS TIME BURDEN

Component	Related Basic Event	Σ Risk Reduction Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RRI) / Time Burden (E-06 yr^{-1})
46P-2A pump	ESW-CCF-FR-PUMPS	1.78E-07		
	ESW-MDP-FR-P2A	1.48E-07		
	ESW-CCF-FS-PUMPS	9.76E-08		
	ESW-RCK-NO-P2A	3.36E-08	31.5	88.5
	ESW-XHE-RE-P2A	1.73E-08	(5.39E-03)	
	ESW-MDP-FS-P2A	2.98E-09		
	All Events	4.77E-07		
46P-2B pump	ESW-CCF-FR-PUMPS	1.78E-07		
	ESW-MDP-FR-P2A	1.41E-07		
	ESW-CCF-FS-PUMPS	9.76E-08		
	ESW-RCK-NO-P2A	3.09E-08	31.5	86.46
	ESW-XHE-RE-P2A	1.57E-08	(5.39E-03)	
	ESW-MDP-FS-P2A	2.61E-09		
	All Events	4.66E-07		
46MOV-102A motor op. valve	ESW-RCK-NO-102A	3.36E-08		
	ESW-CCF-OO-102AB	1.64E-08		
	ESW-MOV-OO-102A	4.39E-09	13.5	23.55
			(2.31E-03)	
	All Events	5.44E-08		

Component	Related Basic Event	Σ Risk Reduction Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RRI) / Time Burden ($E\text{-}06\ yr^{-1}$)
46MOV-102B motor op. valve	ESW-RCK-NO-102B ESW-CCF-OO-102AB ESW-MOV-OO-102B All Events	3.09E-08 1.64E-08 3.82E-09 ---------- 5.11E-08	13.5 (2.31E-03)	22.12
46MOV-101A/B motor op. valve	minimum importance*	4.57E-11*	7.5 (1.28E-03)	0.036
15MOV-175A/B motor op. valve	minimum importance*	4.57E-11*	7.5 (1.28E-03)	0.036
46ESW-3A manual valve	ESW-XHE-RE-ESW3A ESW-XVM-PG-ESW3A All Events	9.64E-08 6.92E-10 ---------- 9.71E-08	24 (4.11E-03)	23.63
46ESW-3B manual valve	ESW-XHE-RE-ESW3B ESW-XVM-PG-ESW3B All Events	8.95E-08 5.90E-10 ---------- 9.01E-08	24 (4.11E-03)	21.92
46ESW-10A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
46ESW-23 manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
46ESW-30B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
46ESW-1A check valve	ESW-CKV-CC-ESW1A	2.18E-09	18 (3.08E-03)	0.71

Component	Related Basic Event	Σ Risk Reduction Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RRI) / Time Burden ($E\text{-}06\ yr^{-1}$)
46ESW-1B check valve	ESW-CKV-CC-ESW1B	1.86E-09	18 (3.08E-03)	0.6
46ESW-6A check valve	ESW-CKV-CC-ESW6A	2.18E-09	18 (3.08E-03)	0.71
46ESW-6B check valve	ESW-CKV-CC-ESW6B	1.86E-09	18 (3.08E-03)	0.6
42C-1ESWA03 relay	ESW-RCI-FE-A42C	3.13E-09	3 (0.51E-03)	6.1
42C-1ESWB04 relay	ESW-RCI-FE-B42C	2.74E-09	3 (0.51E-03)	5.34
63A-1ESWA04 HFA relay	ESW-RCS-OO-A63A9 ESW-RCS-FE-A63A All Events	8.04E-09 3.13E-09 ---------- 1.12E-08	3 (0.51E-03)	21.82
63A-1ESWBO4 HFA relay	ESW-RCS-OO-B63A9 ESW-RCI-FE-B63A All Events	7.13E-09 2.74E-09 ---------- 9.87E-09	3 (0.51E-03)	19.23
15PS-122A/B/C/D Pressure sensor	minimum importance*	4.57E-11*	6 (1.03E-03)	0.046

* Basic event involving the component is not important enough to show up in Fitzpatrick's sensitivity studies. The smallest risk reduction importance value that does show up in the study was used, as this would represent a maximum value for any less-important RRI.

TABLE 3.4

LCS SYSTEM COMPONENT RISK REDUCTION IMPORTANCE VERSUS TIME BURDEN

Component	Related Basic Event	Σ Risk Reduction Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	$\frac{\Sigma \text{ (RRI)}}{\text{Time Burden}}$ (E-06 yr^{-1})
14P-1A/B pump	minimum importance*	4.57E-11*	37.5 (6.42E-03)	0.0071
14P-2A/B holding pump	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
14MOV-5A/B motor op. valve	minimum importance*	4.57E-11*	37.5 (6.42E-03)	0.0071
14MOV-7A/B motor op. valve	minimum importance*	4.57E-11*	21 (3.59E-03)	0.013
14MOV-11A/B motor op. valve	minimum importance*	4.57E-11*	34.5 (5.9E-03)	0.0077
14MOV-12A/B motor op. valve	minimum importance*	4.57E-11*	37.5 (6.42E-03)	0.0071
14MOV-26A/B motor op. valve	minimum importance*	4.57E-11*	37.5 (6.42E-03)	0.0071
14CSP-8A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
14CSP-18A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089

Component	Related Basic Event	Σ Risk Reduction Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RRI) / Time Burden ($E\text{-}06\ yr^{-1}$)
14CSP-61A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
14CSP-69A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
14CSP-74A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
14A-K9A/B relay GE-HFA	LCS-RLY-NO-K9ACL/ BCL	8.01E-10	16.5 (2.82E-03)	0.28
14A-K17A/B relay GE-HFA	LCS-RLY-NO-17ACL/ BCL	8.01E-10	16.5 (2.82E-03)	0.28
02-3LT-72A/B/C/D RX lo level txmtr	minimum importance*	4.57E-11*	4 (0.68E-03)	0.067
02-3PT-52A/B/C/D RX lo pres txmtr 10PT-101A/B/C/D DW hi pres txmtr	minimum importance*	4.57E-11*	8 (1.37E-03)	0.033
02-3MTU-252 02-3MTU-272 10-MTU-201 A/B/C/D master trip units	minimum importance*	4.57E-11*	16 (2.74E-03)	0.017

* Basic event involving the component is not important enough to show up in Fitzpatrick's sensitivity studies. The smallest risk reduction importance value that does show up in the study was used, as this would represent a maximum value for any less-important RRI

TABLE 3.5

ESW SYSTEM COMPONENT RISK INCREASE IMPORTANCE VERSUS TIME BURDEN

Component	Related Basic Event	Σ Risk Increase Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RII) / Time Burden ($E\text{-}03\ yr^{-1}$)
46P-2A pump	ESW-CCF-FR-PUMPS	1.52E-03		
	ESW-MDP-FR-P2A	3.27E-05		
	ESW-CCF-FS-PUMPS	1.08E-03		
	ESW-RCK-NO-P2A	3.03E-05	31.5	504.64
	ESW-XHE-RE-P2A	2.88E-05	(5.39E-03)	
	ESW-MDP-FS-P2A	2.40E-05		

	All Events	2.72E-03		
46P-2B pump	ESW-CCF-FR-PUMPS	1.52E-03		
	ESW-MDP-FR-P2A	3.10E-05		
	ESW-CCF-FS-PUMPS	1.08E-03		
	ESW-RCK-NO-P2A	2.78E-05	31.5	502.78
	ESW-XHE-RE-P2A	2.61E-05	(5.39E-03)	
	ESW-MDP-FS-P2A	2.10E-05		

	All Events	2.71E-03		
46MOV-102A motor op. valve	ESW-RCK-NO-102A	3.03E-05		
	ESW-CCF-OO-102AB	1.07E-03		
	ESW-MOV-OO-102A	2.52E-05	13.5	489.18
		------------	(2.31E-03)	
	All Events	1.13E-03		

Component	Related Basic Event	Σ Risk Increase Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RII) / Time Burden ($E-03\ yr^{-1}$)
46MOV-102B motor op. valve	ESW-RCK-NO-102B ESW-CCF-OO-102AB ESW-MOV-OO-102B All Events	2.78E-05 1.07E-03 2.20E-05 ------------ 1.12E-03	13.5 (2.31E-03)	484.85
46MOV-101A/B motor op. valve	minimum importance*	2.19E-09*	7.5 (1.28E-03)	0.0017
15MOV-175A/B motor op. valve	minimum importance*	2.19E-09*	7.5 (1.28E-03)	0.0017
46ESW-3A manual valve	ESW-XHE-RE-ESW3A ESW-XVM-PG-ESW3A All Events	3.20E-05 1.92E-05 ------------ 5.12E-05	24 (4.11E-03)	12.46
46ESW-3B manual valve	ESW-XHE-RE-ESW3B ESW-XVM-PG-ESW3B All Events	2.97E-05 1.64E-05 ------------ 4.61E-05	24 (4.11E-03)	11.22
46ESW-10A/B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
46ESW-23 manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
46ESW-30B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
46ESW-1A check valve	ESW-CKV-CC-ESW1A	2.36E-05	18 (3.08E-03)	7.66

Component	Related Basic Event	Σ Risk Increase Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RII) / Time Burden ($E\text{-}03\ yr^{-1}$)
46ESW-1B check valve	ESW-CKV-CC-ESW1B	2.02E-05	18 (3.08E-03)	6.56
46ESW-6A check valve	ESW-CKV-CC-ESW6A	2.36E-05	18 (3.08E-03)	7.66
46ESW-6B check valve	ESW-CKV-CC-ESW6B	2.02E-05	18 (3.08E-03)	6.56
42C-1ESWA03 relay	ESW-RCI-FE-A42C	2.40E-05	3 (0.51E-03)	46.76
42C-1ESWB04 relay	ESW-RCI-FE-B42C	2.10E-05	3 (0.51E-03)	40.91
63A-1ESWA04 HFA relay	ESW-RCS-OO-A63A9 ESW-RCS-FE-A63A All Events	2.68E-05 2.40E-05 ------------ 5.08E-05	3 (0.51E-03)	98.97
63A-1ESWBO4 HFA relay	ESW-RCS-OO-B63A9 ESW-RCI-FE-B63A All Events	2.37E-05 2.10E-05 ------------ 4.47E-05	3 (0.51E-03)	87.08
15PS-122A/B/C/D Pressure sensor	minimum importance*	2.19E-09*	6 (1.03E-03)	0.0021

* Basic event involving the component is not important enough to show up in Fitzpatrick's sensitivity studies. The smallest risk increase importance value that does show up in the study was used, as this would represent a maximum value for any less-important RII.

TABLE 3.6

LCS SYSTEM COMPONENT RISK INCREASE IMPORTANCE VERSUS TIME BURDEN

Component	Related Basic Event	Σ Risk Increase Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RII) ------------ Time Burden (E-03 yr^{-1})
14P-1A/B pump	minimum importance*	2.19E-09*	37.5 (6.42E-03)	0.00034
14P-2A/B holding pump	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
14MOV-5A/B motor op. valve	minimum importance*	2.19E-09*	37.5 (6.42E-03)	0.00034
14MOV-7A/B motor op. valve	minimum importance*	2.19E-09*	21 (3.59E-03)	0.00061
14MOV-11A/B motor op. valve	minimum importance*	2.19E-09*	34.5 (5.9E-03)	0.00037
14MOV-12A/B motor op. valve	minimum importance*	2.19E-09*	37.5 (6.42E-03)	0.00034
14MCV-26A/B motor op. valve	minimum importance*	2.19E-09*	37.5 (6.42E-03)	0.00034
14CSP-8A/B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
14CSP-18A/B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
14CSP-61A/B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043

Component	Related Basic Event	Σ Risk Increase Importance (yr^{-1}) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden yr/yr)	Σ (RII) / Time Burden ($E\text{-}03\ yr^{-1}$)
14CSP-69A/B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
14CSP-74A/B manual valve	minimum importance*	2.19E-09*	3 (0.51E-03)	0.0043
14A-K9A/B relay GE-HFA	LCS-RLY-NO-K9ACL/ BCL	1.86E-06	16.5 (2.82E-03)	0.66
14A-K17A/B relay GE-HFA	LCS-RLY-NO-17ACL/ BCL	1.86E-06	16.5 (2.82E-03)	0.66
02-3LT-72A/B/C/D RX lo level txmtr	minimum importance*	2.19E-09*	4 (0.68E-03)	0.0032
02-3PT-52A/B/C/D RX lo pres txmtr 10PT-101A/B/C/D DW hi pres txmtr	minimum importance*	2.19E-09*	8 (1.37E-03)	0.0016
02-3MTU-252 02-3MTU-272 10-MTU-201 A/B/C/D master trip units	minimum importance*	2.19E-09*	16 (2.74E-03)	0.0008

* Basic event involving the component is not important enough to show up in Fitzpatrick's sensitivity studies. The smallest risk increase importance value that does show up in the study was used, as this would represent a maximum value for any less-important RII.

TABLE 3.7

ESW COMPONENT RISK/BURDEN RATIO RANKINGS

Component	Σ RRI/Burden (E-06 yr^{-1}) [Rank]	Σ RII/Burden (E-03 yr^{-1}) [Rank]
46P-2A pump	88.5 [1]	504.64 [1]
46P-2B pump	86.46 [2]	502.78 [2]
46ESW-3A manual valve	23.63 [3]	12.46 [9]
46MOV-102A motor op. valve	23.55 [4]	489.18 [3]
46MOV-102B motor op. valve	22.12 [5]	484.85 [4]
46ESW-3B manual valve	21.92 [6]	11.22 [10]
63A-1ESWA04 HFA relay	21.82 [7]	98.97 [5]
63A-1ESWB04 HFA relay	19.23 [8]	87.08 [6]
42C-1ESWA03 relay	6.1 [9]	46.76 [7]
42C-1ESWB04 relay	5.34 [10]	40.91 [8]
46ESW-1A check valve	0.71 [11]	7.66 [11]
46ESW-6A check valve	0.71 [11]	7.66 [11]
46ESW-1B check valve	0.6 [13]	6.56 [13]
46ESW-6B check valve	0.6 [13]	6.56 [13]
46ESW-10A/B manual valve	0.089 [15]	0.0043 [15]
46ESW-23 manual valve	0.089 [15]	0.0043 [15]

Component	Σ RRI/Burden (E-06 yr^{-1}) [Rank]	Σ RII/Burden (E-03 yr^{-1}) [Rank]
46ESW-30B manual valve	0.089 [15]	0.0043 [15]
15PS-122A/B/C/D Pressure sensor	0.046 [18]	0.0021 [18]
46MOV-101A/B motor op. valve	0.036 [19]	0.0017 [19]
15MOV-175A/B motor op. valve	0.036 [19]	0.0017 [19]

TABLE 3.8

LCS COMPONENT RISK/BURDEN RATIO RANKINGS

Component	Σ RRI/Burden (E-06 yr^{-1}) [Rank]	Σ RII/Burden (E-03 yr^{-1}) [Rank]
14A-K9A/B relay GE-HFA	0.28 [1]	0.66 [1]
14A-K17A/B relay GE-HFA	0.28 [1]	0.66 [1]
14P-2A/B holding pump	0.089 [3]	0.0043 [3]
14CSP-8A/B manual valve	0.089 [3]	0.0043 [3]
14CSP-18A/B manual valve	0.089 [3]	0.0043 [3]
14CSP-61A/B manual valve	0.089 [3]	0.0043 [3]
14CSP-69A/B manual valve	0.089 [3]	0.0043 [3]
14CSP-74A/B manual valve	0.089 [3]	0.0043 [3]
02-3LT-72A/B/C/D RX lo level txmtr	0.067 [9]	0.0032 [9]
02-3PT-52A/B/C/D RX lo pres txmtr 10PT-101A/B/C/D CD hi pres txmtr	0.033 [10]	0.0016 [10]
02-3MTU-252 02-3MTU-272 10-MTU-201A/B/C/D master trip units	0.017 [11]	0.0008 [11]
14MOV-7A/B motor op. valve	0.013 [12]	0.00061 [12]
14MOV-11A/B motor op. valve	0.0077 [13]	0.00037 [13]
14P-1A/B pump	0.0071 [14]	0.00034 [14]

Component	Σ RRI/Burden (E-06 yr^{-1}) [Rank]	Σ RII/Burden (E-03 yr^{-1}) [Rank]
14MOV-5A/B motor op. valve	0.0071 [14]	0.00034 [14]
14MOV-12A/B motor op. valve	0.0071 [14]	0.00034 [14]
14MOV-26A/B motor op. valve	0.0071 [14]	0.00034 [14]

The Fitzpatrick study measuring the importance values of internal core damage cutsets only covers the most important basic events. Thus risk insignificant basic events corresponding to the failure of risk insignificant components will not have a RRI or RII measure that appears significantly in the Fitzpatrick data. However, the smallest RRI or RII that does show up in the Fitzpatrick study would represent a limiting maximum value of risk importance for all less-significant components. The minimum RRI in the Fitzpatrick study was 4.57E-11 yr^{-1}, and the minimum RII was 2.19E-09 yr^{-1}.

Another measure that should also be used to calculate a risk/burden ratio is the share of the total CDF per basic event, sometimes referred to as the Fussell-Vesely index. These data were unfortunately not available from the Fitzpatrick IPE. However, the method for calculating the value of a ratio based upon each event's share of the total CDF would be the same as for RRIs and RIIs ratios. All three of these risk measures should then be used to calculate a set of ratios to ensure that nothing risk significant is missed. The use of multiple risk measures also provides reinforcement for the results obtained. A comparison between the ratio rankings obtained for the RRI and RII ratios (Tables 3.7 and 3.8) shows that although the two ratios' numerical rankings differ slightly among certain components, most notably concerning the ESW manual valve 3, both ratios point out the same components as being the most significant.

3.4 Uses of the Risk/Burden Component Ratio

A comparison of the risk/burden ratios between the ESW and LCS systems shows a great deal of difference. This is to be expected, as the two systems have very similar maintenance and surveillance procedures but quite different levels of risk significance. These ratios, however, present a quantitative way to measure the disparity between the amount of resources expended on a system and its importance to safety. There is a difference of four orders of magnitude between the ESW and LCS systems' RRI/burden ratios, and a difference of six orders of magnitude between the two systems' RII/burden ratios.

Even within the same system there is a great deal of difference in the magnitude of the ratios between components. The ESW system has a difference of three orders of magnitude between components for the RRI/burden ratios, and a difference of five orders of magnitude for the RII/burden ratios. The LCS system has a difference of two orders of magnitude between components for the RRI/burden ratios, and a difference of three orders of magnitude for the RII/burden ratios. This points out that resource allocation even within a single system is far from being optimally risk-based.

These ratios are thus directly applicable to the NRC Maintenance Rule because the Maintenance Rule is concerned with only the aspects of maintenance that relate directly to plant safety. There are numerous other reasons for performing maintenance and surveillance on systems besides their safety significance, as is discussed in Chapter 4. However, in order to satisfy the Maintenance Rule it is necessary to focus on the risk significance of the component to be maintained, and the risk/burden ratios do just that.

From a risk standpoint, the best use of plant resources should lead to a relatively uniform distribution of risk/burden ratios. In order to smooth the ratios between the different ESW system components, and between the ESW and LCS systems, a new maintenance and surveillance schedule should be developed that focuses more on those components with high values of the risk/burden ratio. This group would include the ESW pumps, ESW MOV 102, ESW manual valve 3, the ESW HFA relay 63A, the ESW relay 42C, and ESW check valves 1 and 6. The information embodied in these ratios also provide justification for decreasing surveillance on the LCS system in general, and increasing surveillance on the ESW system.

All of these actions might seem to be obviously required from inspection of the risk significance of these two systems and examination of the cutsets relating to ESW system failure. However, when dealing with other plant systems having less pronounced differences in risk significance, the risk/burden ratios may point out more subtle relationships between the systems. A full analysis of all of the plant safety systems would be necessary in order to establish reasonable values of the risk/burden ratios to use as goals in allocating resources for surveillance and maintenance procedures.

CHAPTER 4

METHODOLOGY ACCEPTABILITY AND UNCERTAINTY

4.1 Introduction

The preceding chapter introduces two ratios for use in measuring the amount of plant resources expended on a particular component versus the risk significance of the component. These ratios present a quantitative way to measure whether the current testing and surveillance requirements are consistent with the safety importance of a system. However, it is important to investigate the possible regulatory considerations affecting the use of such ratios in satisfaction of the NRC Maintenance Rule. To do so, two different elements are examined: the past and present attitude of the NRC towards the quantitative use of PRA in regulation, and the degree of uncertainty present in the ratios themselves.

4.2 Acceptability of PRA Quantitative Results

Although it is not mandatory for each operating nuclear plant to perform a PRA-type analysis to satisfy the requirement for an Individual Plant Examination (IPE), most plants find it practical to do so. There is considerable regulatory reluctance to assign numerical, quantitative goals for the safety of nuclear power plants. There is a great deal of argument over whether quantitative safety performance goals should be set at all, or if PRA results are best used to set broader, qualitative safety goals that are not specifically regulated. Current regulations still use a deterministic approach to setting regulations, although risk analyses have been used to test the reasonableness of certain deterministic criteria.

There are various reasons for the reluctance to use quantitative PRA results in the regulatory process. The purpose of a regulatory agency is not simply to believe an applicant's results but to be able to verify them. Performing a complete PRA requires considerable manpower and effort, whereas deterministic criteria are much easier to use in verifying whether a design or procedure is satisfactory. More importantly, however, there are several serious concerns that the NRC has with the current PRAs. First, the methods involved in performing the analyses are not standardized and may be different from plant to plant, or from analyst to analyst. Second, the databases used may also differ. Third, and perhaps most importantly, the treatment of uncertainty in PRA analysis has been an area of concern since the inception of the methodology.

Indeed, the NRC's initial review of the Fitzpatrick IPE points out exactly these concerns. The NRC's concerns included inaccurate or incomplete models and old, deficient databases. The NRC was also concerned that the Fitzpatrick core damage frequency was too low, although the Fitzpatrick staff has pointed out that their CDF does fall within the range of uncertainty of other BWR PRA's. Thus although the Fitzpatrick staff has refuted most of the NRC's concerns, their experience does point out the problems associated with the use of quantitative PRA results.

Through a program of quality control, the methods and databases used to perform a PRA could be standardized. By specifying a set of computer codes and standard models, the NRC could gain a great deal of certainty as to the standardization of methods and databases. The treatment of uncertainty is somewhat harder to deal with, as there are numerous areas of PRA methodology where this is a concern. Some examples are human reliability, common cause failures, and the use of expert opinion to supplement insufficient databases. All of these areas are in a constant state of updating and improvement, so to set standards in these areas might prove extremely difficult.

Even though there is considerable reluctance to base regulatory decisions upon the literal values for core damage frequency and other overall results, such as expected containment failure frequency and offsite consequences, probabilistic analyses are used extensively in several areas. This includes the classification of accident scenarios, the selection of initiating events and their combinations, and searching for particular plant or system weaknesses. PRA is also used to assess the reliability of certain (usually safety-related) systems.

The risk/burden ratios presented here do not use the CDF as a decision criterion, but instead use relative quantities based upon the CDF (risk reduction importances) to compare different plant systems. Because these quantities are used to make comparisons between similar systems, it can be argued that the uncertainties will tend to cancel out, or in this case will make the same contribution to each ratio. Thus, although there exist concerns as to the methodology and uncertainty present in the IPE used to obtain the risk/burden ratios, their use in a comparative way is still justifiable. Certainly, as more quality control over the IPE process evolves, the quantitative use of such ratios will become easier to justify.

4.3 Sources of Uncertainty

4.3.1 Plant and Procedure Modification

The process of developing an IPE is long and involved. Since the time that models were developed for the Fitzpatrick IPE, various plant modifications have been made. NYPA is attempting to update their PRA as new data become available, as part of their "living PRA" process. However, there will necessarily be a time lag between the completion of modifications and their inclusion in the IPE. Certain proposed and completed modifications to the systems discussed here will affect the ratios obtained. Since these modifications were not yet included in the IPE data, their effects do not appear in the risk/burden ratios. They are detailed here as sources of uncertainty because their exact effects upon the ratios are unknown.

For example, a modification was made to the RBCLCS/ESW crosstie line that eliminated several cutsets leading to ESW system failure. The RBCLCS (reactor building closed loop cooling system) will no longer take enough water to fail the ESW system if a demand for EDG cooling occurs. The specific failure modes that have been eliminated all involve a low pressure signal to inject water into the RBCLCS system (RBC-LOW-PRES-EDG), coupled with a failure to close of 46MOV-102 A or B and the failure of one ESW system train.

A RBCLCS low pressure signal causes 46MOV-101A/B and 15MOV-175A/B to open. This allows water to flow to several different loads: the CRD pump coolers, the crescent area coolers, the RHR pump coolers, the drywell coolers, the recirc pump and motor coolers, and the pass sample cooler. 46MOV-102 A and B provide a cross-connection between loop A and B of ESW. Thus if one ESW loop failed to operate, a low pressure RBCLCS demand occurred, and 46MOV-102 A or B failed to close, there would be insufficient water for EDG cooling.

However, recent modifications have reduced the normal flow required by a low pressure RBCLCS demand to only the CRD pump coolers, the crescent area coolers, and the pass sample cooler. With these loads the system still has enough water for EDG cooling if the aforementioned failures occur. This invalidates the following cutsets:

- T1 * RBC-LOW-PRES-EDG * ESW-CCF-OO-102AB
- T1 * RBC-LOW-PRES-EDG * ESW-MAI-MA-LOOPA * ESW-MOV-OO-102B
- T1 * RBC-LOW-PRES-EDG * ESW-RCS-OO-A63A9 * ESW-MAI-MA-LOOPB
- T1 * RBC-LOW-PRES-EDG * ESW-RCK-NO-102B * ESW-MDP-FR-P2A
- T1 * RBC-LOW-PRES-EDG * ESW-RCK-NO-102B * AC4-XHE-MC-UVRLA
- T1 * RBC-LOW-PRES-EDG * ESW-RCK-NO-102B * ESW-XHE-RE-ESW3A.

Various combinations of these cutsets with the A and B train events reversed would also be eliminated.

The main effect of these cutsets being eliminated would be to reduce the risk significance of the ESW MOVs 102 A and B. These MOVs currently have the forth highest RRI/burden ratio in the ESW system, after the pumps and manual valve 46ESW-3A. Thus this modification will probably have a significant effect upon the risk/burden ratio of an important component in the ESW system. This modification will also reduce the overall risk significance of the ESW system. It is not possible to assess these effects quantitatively until the IPE is updated.

A procedural modification may be approved in the near future that will also affect the Fitzpatrick IPE, involving the closing of the manual valves 46ESW-3A and B during the testing of ESW pump discharge pressure. The current test method is to "deadhead" each pump, or run it at its highest head zero flow condition, in order to measure the discharge pressure. The normally open valves to each EDG, 3A and B, must be closed in order to produce the shutoff head / zero flow condition to measure a point on the pump curve.

The test was done this way because the ESW system did not have a flow-measuring device to measure pump flow. However, recent modifications have added flow monitoring equipment downstream of the ESW pumps. Fitzpatrick has submitted a Tech Spec change request to eliminate the need to perform the test in its current form. This would eliminate the need to close 46ESW-3A/B during ST-8D, the ESW Pump Flow Rate Test.

Such a Tech Spec change will have two effects. Since procedure ST-8D was performed on a monthly basis, the time burden on 46ESW-3A/B will be reduced. However, most of the risk significance of these manual valves was due to the human error probability of leaving these valves closed after performing this test. Thus the risk significance of this component will also be greatly reduced. The end result will almost certainly lower the risk/burden ratios considerably, although again this is impossible to measure quantitatively until the IPE is updated.

4.3.2 Data Estimation

The main area of data uncertainty is the plant staff time burden numbers for each testing and surveillance procedure. These estimates were obtained in conjunction with Mr. K. Vehstedt, who conferred with Instrumentation and Control technicians from the Fitzpatrick plant who were familiar with the two systems. Although the use of expert judgment is common in PRA analysis, it is difficult to quantify the amount of uncertainty present in such data. A very informal approach was used where the engineer was asked to estimate the amount of workerhours required to perform each procedure.

Another consideration in the time burden estimate is the time spent on activities related to initiating, approving, and closing out procedures. This time cannot be estimated from analyzing the procedure itself, as it relates to management and quality control practices at each individual plant. At Fitzpatrick this has been estimated to actually comprise the majority of the total staff time spent on the procedure. A Fitzpatrick study calculated that actually performing a procedure comprises only 12-15 percent of the total staff time. The time burden used here represents only the actual performance time for each procedure. However, as the ratios are used only in a comparative sense, the managerial time burden would be expected to be approximately constant for each procedure.

Another area of uncertainty is introduced by the use of a minimum risk reduction importance and minimum risk increase importance for those components not risk significant enough to be included in the Fitzpatrick sensitivity study. This represents an area of conservatism, because the RRI and RII of these components will fall below the lowest importances given in the study which were used to calculate the risk/burden ratios. Thus the components for which a minimum RRI and RII were used will tend to have inflated risk/burden ratios.

4.3.3 Considerations Other Than Risk Reduction and Risk Increase Importances

It is important to remember that there are considerations other than risk reduction and increase importances which will make it important to inspect plant systems. As previously mentioned, core damage frequency is not the only measure of risk significance; PRA rankings for containment failure frequency and source terms should also be considered. There is also the additional consideration of SSCs that have been effectively regulated to the point where they no longer show up as being risk significant.

Besides risk significance, which is the main focus of the NRC's regulatory concerns, the utility will have numerous other reasons to inspect plant systems. These concerns include balance of plant, loss of capacity, efficiency, and radiological ALARA issues. The risk/burden ratios do not take these concerns into account, and thus from an operations viewpoint would not be sufficient to assess the inspection needs of all plant systems.

CHAPTER 5

SUMMARY AND CONCLUSIONS

5.1 Summary

The necessity to implement the NRC Maintenance Rule by 1996 provides an impetus to investigate the scheduling of maintenance and inspection procedures at nuclear power plants. Maintenance and surveillance represents a significant portion of the work performed at a nuclear plant, and proper resource allocation in this area is essential. The purpose of this study was to demonstrate a method for selecting the structures, systems, and components (SSCs) important to safety as required by the Maintenance Rule, and then to develop criteria that can be used to schedule a testing program based on the safety significance of these SSCs.

The New York Power Authority's Fitzpatrick plant was used as an example for this study. The Fitzpatrick IPE was used to select a risk significant and risk insignificant system to illustrate the methodology presented here. Safety significance can be ranked by minimum cutset frequencies, risk reduction importances, or risk increase importances. The emergency service water (ESW) system was selected as the risk significant system, and the core spray (LCS) system was selected as the risk insignificant system.

Each system was analyzed for important component failures as indicated by risk significant basic events in the set of all minimum cutsets. Surveillances performed on each system were broken down on a component basis. The staff time burden allocated to each component was estimated from the surveillance procedures in conjunction with members of the Fitzpatrick plant staff. Only the time spent inspecting the system to ensure its reliability was included. Basic preventive maintenance required to make a component function was not taken into account, as this work is a necessity not subject to change.

The time burden and risk significance were used to develop two risk/burden ratios. These ratios represent a measure of the risk significance of a component compared to the amount of effort currently expended to ensure the reliability of the system. Ideally, these ratios should be reasonably constant from component to component and from system to system. However, as can be seen from the disparity between the ratios for the ESW system and the LCS system, and even between components within each system, this is currently not the case. These ratios present a quantitative way to measure whether surveillance practices are reasonable with respect to the risk significance of the system, and could be used to reorganize surveillance schedules on a risk importance basis.

5.2 Conclusions

Previous inspection scheduling was mainly based upon a system's function, and not necessarily its importance in terms of the risk associated with system failure. This becomes evident when two standby safety systems like the ESW and LCS systems are compared. These two systems have very similar inspection schedules but widely different risk significance with respect to CDF.

The risk/burden ratios introduced here for each component represent an attempt to quantify the relationship between the time spent ensuring a component's reliability (burden) and the importance of a component's reliability, as represented by risk reduction and risk increase importances. The benefit of using such ratios to schedule inspection and testing is that systems whose reliability is vital from a safety standpoint would be allocated a proportionally higher share of available plant resources. Additionally, the most risk significant components in a system will receive more attention than those whose failure is unlikely or unimportant.

It is hoped that these ratios could play a part in developing a maintenance and inspection program designed to satisfy the NRC Maintenance Rule. However, there are numerous uncertainties present in these ratios that must be taken into account. The PRA techniques used to rank systems and components from a safety standpoint are associated with numerous uncertainties, and there has been considerable regulatory reluctance in the past to use PRA data in a quantitative way. In addition, accurate data regarding the staff time expended on individual procedures is not available. Studies should be done in this area in order to gain a more accurate picture of where plant resources are being spent.

When developing a plant-wide inspection schedule, considerations other that risk must be taken into account. Plant operating criteria must also be considered, as steady, consistent operations are also a vital part of proper resource allocation. However, the risk/burden ratios do represent both a departure from past inspection scheduling practices and an important criteria to consider when developing more efficient schedules.

REFERENCES

1. Specter, Herschel. "PSA, Calculus, and Nuclear Regulation", NYPA, White Plains, NY. (1992).

2. Specter, Herschel. NYPA, Fax communication, Nov. 12, 1992.

3. Vesely, W.E. and P.K. Samanta. "PRA-Based Prioritization Procedures with a Focus on Maintenance Prioritization Applications", Presentation to NRC and NUMARC Personnel. Nov. 16, 1992.

4. NUMARC. "Industry Guidelines for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants (Draft Document)", Nuclear Management and Resources Council, Inc. Washington, D.C. July, 1992.

5. New York Power Authority. "James A. Fitzpatrick Nuclear Power Plant Individual Plant Examination. Vol. 1 & 2", White Plains, NY. August, 1991.

6. Tanguy, P. (CEA). "French Practice of Limited Application of Quantitative Safety Goals", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

7. Dunster, H. J. (HSE-UK). "The Value and Limitation of Quantitative Safety Goals", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

8. Sege, G. (USNRC). "Issues in Development of an NRC Safety Goal", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

9. O'Donnell, E. P. (Ebasco). "A Proposed Approach to the Establishment and Use of Quantitative Safety Goals in the Nuclear Regulatory Process", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

10. Temme, M. I. (GE). "Development of a Quantitative Risk Standard", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

11. Okrent, D. (UCLA). "Some Recent Developments on Safety Goals for LWRs", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

12. Cave, L. (PPL-UK), J. R. Harrison (CEGB-UK), A. Marchese (USNRC), J. N. Tweedy (SSEB-UK). "The Practical Application of Quantitative Safety Criteria for Nuclear Power Plant", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Risk Assessment. Port Chester, NY. September, 1981.

13. New York Power Authority James A. Fitzpatrick Nuclear Power Plant. Operations Surveillance Test Procedure:
    - ST-3A Core Spray Pump and Valve Operability Test
    - ST-3B Core Spray Simulated Automatic Actuation
    - ST-9B EDG Full Load Test and ESW Pump Operability Test
    - ST-8D ESW Pump Flow Rate Test
    - ST-8E ESW Logic System Functional Test and Simulated Automatic Actuation Test
    - ST-3J Core Spray Initiation Logic Functional Test
    - ST-1R Reactor Building Closed Loop Cooling Containment Isolation AOV Exercise

14. New York Power Authority James A. Fitzpatrick Nuclear Power Plant Instrument Surveillance Procedure:
    - ISP-23 Emergency Service Water Lockout Matrix Instrument Functional Test/Calibration
    - ISP-175A Reactor and Containment Cooling Instrument Functional Test/Calibration
    - ISP-275A Reactor Pressure (ECCS) Transmitter Calibration and Channel Functional Test
    - ISP-276A Reactor Level (ECCS) Transmitter Calibration and Channel Functional Test

15. New York Power Authority James A. Fitzpatrick Nuclear Power Plant Maintenance Procedure:
    - MP-014.01 Core Spray Pump Maintenance
    - MP-46.1 RHR Service water Pumps and Emergency Service Water Pumps

APPENDIX A

THE MAINTENANCE RULE

50.65 Requirements for monitoring the effectiveness of maintenance at nuclear power plants.

(a)(1) Each holder of an operating license under 50.21(b) or 50.22 shall monitor the performance or condition of structures, systems, or components, against licensee-established goals, in a manner sufficient to provide reasonable assurance that such structures, systems, and components, as defined in paragraph (b), are capable of fulfilling their intended functions. Such goals shall be established commensurate with safety and, where practical, take into account industry-wide operating experience. When the performance or condition of a structure, system or component does not meet established goals, appropriate corrective action shall be taken.

(2) Monitoring as specified in paragraph (a)(1) of this section is not required where it has been demonstrated that the performance or condition of a structure, system, or component is being effectively controlled through the performance of appropriate preventive maintenance, such that the structure, system, or component remains capable of performing its intended function.

(3) Performance and condition monitoring activities and associated goals and preventive maintenance activities shall be evaluated at least annually, taking into account, where practical, industry-wide operating experience. Adjustments shall be made where necessary to ensure that the objective of preventing failures of structures, systems, and components through maintenance is appropriately balanced against the objective of minimizing unavailability of structures, systems, and components due to monitoring or preventive maintenance. In performing monitoring and preventive maintenance activities, and assessment of the total plant equipment that is out of service should be taken into account to determine the overall effect on performance of safety functions.

(b) The scope of the monitoring program specified in paragraph (a) (1) of this section shall include safety-related and nonsafety related structures, systems and components, as follows:

(1) Safety-related structures, systems, or components that are relied upon to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, and the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the 10 CFR part 100 guidelines.

(2) Nonsafety related structures, systems, or components:

(i) That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs); or

(ii) Whose failure could prevent safety-related structures, systems, and components from fulfilling their safety-related function: or

(iii) Whose failure could cause a reactor scram or actuation of a safety-related system.

(c) The requirements of this section shall be implemented by each licensee no later than July 10, 1996.

APPENDIX B

DESCRIPTIONS OF THE 9 DOMINANT CORE DAMAGE ACCIDENT SEQUENCES[6]

The 9 risk-dominant core damage accident sequences are summarized in the following descriptions.

T1-35-T3C-84:

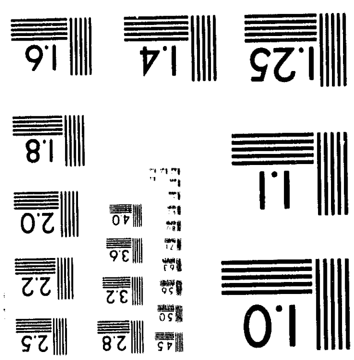
T1-35 [T1*/C*/B2*P1]. A loss of offsite power transient occurs (T1), leading to a turbine trip. The reactor scrams (/C) and at least one division of emergency onsite ac power supplies a safeguard bus (10500 or 10600) (/B2). The SRVs open to relieve reactor pressure; but one SRV fails to reclose (P1), creating a loss of coolant accident. This sequence transfers to the inadvertent opening of a relief valve (T3C) transient tree for further development.

T3C-84 [T3C*/C*B1*/B2*Q*/U1*V1*/W1]. A relief valve is inadvertently stuck open (TC3). The reactor scrams (/C). Offsite power is lost (B1). Onsite emergency power is, however, established (/B2). The power conversion system fails (Q). HPCI starts to inject water (/U1) to provide core water level control; however, HPCI eventually fails because of low reactor vessel steam supply - a relief valve is open. Condensate injection (V1) is unavailable because of the loss of offsite power.

T1-38-TB-1:

T1-38 [T1*/C*B2]. A loss of offsite power transient occurs (T1) and the reactor scrams (/C), but emergency onsite ac power is unavailable (B2). This sequence transfers to the station blackout tree for further development.

TB-1 [TB*/P*/U1/U1X]. A transient event occurs (T). Subsequently both offsite and onsite ac power are lost (B). The reactor is shutdown. The SRVs open and reclose (/P) to relieve the pressure from the power imbalance caused when the turbine trips. The SBO renders all core cooling systems, except HPCI, RCIC and the fire protection system, inoperable. Since the feedwater system cannot provide reactor make-up, reactor water level falls. At a reactor water level of 126.5 in. above TAF, HPCI and RCIC are automatically initiated. HPCI injects water (/U1) to control core water level. Automatic switchover of HPCI suction from the CST to the torus on high torus water level is bypassed (/U1X). After the initial reflooding with water provided by HPCI, the operator may use HPCI or RCIC to provide reactor level control. After 6 hours, however, HPCI will fail because of battery depletion. This sequence results in core damage and a vulnerable containment.


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0

2 of 2

T1-38-TB-2:

TB-2 [TB*/P*U1*U1X/U2]. Same as sequence TB-1, except that HPCI high torus water level transfer is not bypassed (U1X). This leads to HPCI failure when the suppression pool temperature exceeds 200°F. The operator uses RCIC for reactor water level control but RCIC will fail after 6 hours because of battery depletion. This sequence results in core damage and a vulnerable containment.

T1-38-TB-4:

TB-4 [TB*/P*U1*/U2]. Same as sequence TB-1, except that random mechanical faults fail HPCI (U1). The operator uses RCIC to provide reactor water level control (/U2), but RCIC fails after 8 hours because of battery depletion. This sequence results in core damage and a vulnerable containment.

T1-38-TB-5:

TB-5 [TB*/P*U1*U2]. Same as sequence TB-1, except that both HPCI and RCIC fail to operate (U1*U2). This sequence results in early core damage and a vulnerable containment.

T1-38-TB-6:

TB-6 [TB*P1*/U1]. A transient event occurs (T). Subsequently both offsite and onsite ac power are lost (B). The reactor is scrammed. The SRVs open to relieve pressure but one SRV fails to reclose. Since the feedwater system cannot provide reactor make-up, reactor water level falls. At a reactor water level of 126.5 in. above TAF, HPCI and RCIC are automatically initiated. HPCI injects water (/U1) to control core water level but fails because of low reactor steam pressure. This sequence results in core damage and a vulnerable containment.

T1-38-TB-8:

TB-8 [TB*P1*U1*U2]. Same as sequence TB-6 except that both HPCI and RCIC fail to operate (U1*U2). This sequence results in early core damage and a vulnerable containment.

T1-38-TB-9:

TB-9 [TB*P2]. A transient event occurs (T). Subsequently both offsite and onsite ac power are lost (B). The reactor is scrammed. The SRVs open to relieve reactor pressure but two SRVs fail to reclose (P2). HPCI and RCIC both will fail in less than 1 hour because of low reactor steam pressure. This sequence results in early core damage and a vulnerable containment.

T3A-4-TB-1:

T3A-4 [T3A*/C*B1*B2]. A transient occurs that causes a turbine trip (T3A). The control rods are inserted into the core (/C). Subsequently, offsite and onsite ac power are lost (B1*B2). This sequence transfers to the station blackout tree for further development.

DATE

FILMED

11/13/94

END