

UNIFIED FACILITIES CRITERIA (UFC)

FACILITY ENERGY SYSTEM RESILIENCE AND RELIABILITY



APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

This Page Intentionally Left Blank

CANCELLED

UNIFIED FACILITIES CRITERIA (UFC)

FACILITY ENERGY SYSTEM RESILIENCE AND RELIABILITY

Any copyrighted material included in this UFC is identified at its point of use. Use of the copyrighted material apart from this UFC must have the permission of the copyright holder.

U.S. ARMY CORPS OF ENGINEERS (Preparing Activity)

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND

AIR FORCE CIVIL ENGINEER CENTER

Record of Changes (changes are indicated by \1\ ... /1/)

Change No.	Date	Location

CANCELLED



This Page Intentionally Left Blank

CANCELLED

FOREWORD

The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with [USD \(AT&L\) Memorandum](#) dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate. All construction outside of the United States, its territories, and possessions is also governed by Status of Forces Agreements (SOFA), Host Nation Funded Construction Agreements (HNFA), and in some instances, Bilateral Infrastructure Agreements (BIA). Therefore, the acquisition team must ensure compliance with the most stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.

UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Military Department's responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Systems Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC) are responsible for administration of the UFC system. Technical content of UFC is the responsibility of the cognizant DoD working group. Defense Agencies should contact the respective DoD Working Group for document interpretation and improvements. Recommended changes with supporting rationale may be sent to the respective DoD working group by submitting a Criteria Change Request (CCR) via the Internet site listed below.

UFC are effective upon issuance and are distributed only in electronic media from the following source:

- Whole Building Design Guide website <https://www.wbdg.org/ffc/dod>.

Refer to UFC 1-200-01, *DoD Building Code*, for implementation of new issuances on projects.

AUTHORIZED BY:



PETE G. PEREZ, P.E., SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers



R. DAVID CURFMAN, P.E., SES
Chief Engineer
Naval Facilities Engineering Systems Command



DAVID H. DENTINO, SES
Deputy Director of Civil Engineers
DCS/Logistics, Engineering &
Force Protection (HAF/A4C)
HQ United States Air Force



MICHAEL McANDREW, SES
Deputy Assistant Secretary of Defense
(Construction)
Office of the Secretary of Defense

This Page Intentionally Left Blank

CANCELLED

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1-1 BACKGROUND	1
1-2 PURPOSE AND SCOPE	1
1-3 APPLICABILITY	1
1-4 GENERAL BUILDING REQUIREMENTS	1
1-5 CYBERSECURITY	1
1-6 GLOSSARY	2
1-7 REFERENCES	2
CHAPTER 2 RESILIENCE	3
2-1 RESILIENCE	3
2-1.1 Prepare, Absorb, Recover and Adapt.....	3
2-1.2 Considerations.....	3
2-1.3 Absorption and Recovery.....	3
2-1.4 Prioritizing Robustness or Recovery.....	5
2-1.5 Availability Definitions.....	6
2-1.6 Reliability.....	7
2-1.7 Maintainability.....	7
2-1.8 Relationship Among Reliability, Maintainability, and Availability.....	8
2-1.9 Factors Influencing Availability.....	8
2-1.10 Improving Availability of C5ISR Facilities.....	9
2-2 PROGRAM ELEMENTS	12
2-2.1 RAM Requirements Implementation.....	13
2-2.2 Human Factors Engineering (HFE).....	13
2-2.3 Power System Safety Program.....	13
2-2.4 Consolidation Systems Test Program.....	14
2-2.5 Standardization Program.....	14
2-2.6 Configuration Management (CM) Program.....	14
2-2.7 Operations and Maintenance Planning.....	14
CHAPTER 3 DESIGN CONSIDERATIONS	17
3-1 RELIABILITY/AVAILABILITY DESIGN REQUIREMENTS	17
3-1.1 Availability Requirements.....	17

3-1.2	Responsibilities for Determining Availability Requirements.	17
3-1.3	Availability Requirements for Specific Facility Types.	17
3-2	GENERAL DESIGN REQUIREMENTS.....	17
3-2.1	Historical Records.....	18
3-2.2	Control Systems.	18
3-2.3	Maintenance Concepts.	19
3-2.4	Evaluations.	19
3-2.5	Operations and Maintenance Documentation.....	20
3-2.6	Verification.....	20
CHAPTER 4	ACCEPTABLE METHOD FOR EVALUATING SYSTEM RESILIENCE .	23
4-1	ROBUSTNESS.....	23
4-1.1	Evaluating Robustness.	23
4-2	RECOVERY.....	28
4-2.1	Recovery Time.....	28
4-2.2	Stepped Recovery of Power System Assets.....	28
4-3	DETERMINING OPERATIONAL REQUIREMENTS FOR RESILIENCE	
	METRICS. 30	
4-3.1	Evaluate the Needs of the System.....	30
4-3.2	Availability Requirements.....	30
4-3.3	Minimum Acceptable Level of Degraded State Availability.	31
CHAPTER 5	RELIABILITY/AVAILABILITY	35
5-1	BASIC RELIABILITY AND AVAILABILITY CONCEPTS.	35
5-1.1	Probability and Statistics.....	35
5-1.2	Calculating Reliability.....	39
5-1.3	Calculating Availability.	42
5-1.4	Predictions and Assessments.....	47
5-2	IMPROVING AVAILABILITY.....	49
5-2.1	Overview of the Process.....	49
5-2.2	New Facilities.....	49
5-2.3	Existing Facilities.	52
5-2.4	Improving Availability Through Addition of Redundancy.....	54
5-3	ASSESSING RELIABILITY AND AVAILABILITY.....	63
5-3.1	Purpose of the Assessment.	63

5-3.2	Prediction.....	63
5-3.3	Analytical Methodologies.....	64
5-3.4	Analysis Considerations.....	69
5-3.5	Modeling Examples.....	71
5-3.6	Modeling Complexities.....	77
5-3.7	Conclusion.....	80
CHAPTER 6 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS.....		81
6-1	BACKGROUND ON FMECA.....	81
6-1.1	Define FMECA.....	81
6-1.2	FMECA Benefits.....	81
6-1.3	Team Effort.....	82
6-1.4	FMECA Characteristics.....	83
6-1.5	Requirements.....	83
6-1.6	Goals.....	84
6-2	FAILURE MODES AND EFFECTS ANALYSIS (FMEA) METHODOLOGY.....	84
6-2.1	Methodology – Foundation.....	84
6-2.2	Define the System to be Analyzed (Functional/Hardware Approach) ..	85
6-2.3	Failure Mode Identification.....	97
6-2.4	Failure Effects Analysis.....	98
6-2.5	Failure Detection Methods.....	101
6-2.6	Compensating Provisions.....	102
6-2.7	Severity Rankings.....	102
6-2.8	Results of FMEA.....	105
6-3	CRITICALITY ANALYSIS (CA) METHODOLOGY.....	109
6-3.1	Methodology – Moving into Criticality Analysis.....	109
6-3.2	Criticality Analysis.....	109
6-3.3	Transfer Select Data from FMEA.....	113
6-3.4	Quantitative Criticality Analysis.....	114
6-3.5	Effects of Redundancy – Quantitative.....	119
6-3.6	Qualitative Criticality Analysis.....	122
6-3.7	Effects of Redundancy – Qualitative.....	130
6-4	RANKINGS.....	137

6-4.1	Criticality Rankings.....	137
6-4.2	Criticality Matrix.....	143
6-5	RESULTS.....	145
6-5.1	Overview.....	145
6-5.2	Recommendations – from the Criticality Matrix Example.....	145
6-5.3	Incentives.....	147
6-5.4	Results.....	147
CHAPTER 7 RELIABILITY CENTERED MAINTENANCE (RCM)		149
7-1	RCM.....	149
7-1.1	The RCM Concept.....	149
7-1.2	Benefits of RCM.....	150
7-1.3	Origins of RCM.....	151
7-1.4	Relationship of RCM to Other Disciplines.....	152
7-2	MAINTENANCE.....	153
7-2.1	Categories of Maintenance.....	154
7-2.2	Categorization by when Maintenance is Performed.....	155
7-2.3	Maintenance Concepts.....	158
7-2.4	Packaging a Maintenance Program.....	159
7-3	ELEMENTS OF RCM PROGRAM.....	160
7-3.1	RCM Implementation Plan.....	160
7-3.2	Data Collection Requirements.....	163
7-3.3	Commitment to Life Cycle Support of the Program.....	164
7-3.4	RCM as a Part of Design.....	165
7-3.5	Focus on the Four Ws.....	165
7-4	FUNDAMENTALS OF RCM.....	169
7-4.1	Objectives of RCM.....	169
7-4.2	Applicability of Preventive Maintenance.....	169
7-4.3	Failure.....	170
7-5	RCM PROCESS.....	172
7-5.1	C5ISR Candidates for RCM Analysis.....	172
7-5.2	RCM Data Sources.....	175
7-5.3	PM Tasks Under RCM.....	177

7-5.4	The RCM Process.	180
7-5.5	Specific Considerations for Implementing RCM for C5ISR Facilities.	199
7-5.6	Evaluation of Alternatives.	202
APPENDIX A FACTORS INFLUENCING FIELD MEASURES OF RELIABILITY		207
A-1	INHERENT RELIABILITY VERSUS OPERATIONAL RELIABILITY....	207
A-1.1	Inherent Reliability.	207
A-1.2	Operational Reliability.	207
A-2	ACCOUNTING FOR THE DIFFERENCES.....	207
A-2.1	Design of Procedure.	207
A-2.2	Design Requirements.	208
APPENDIX B STATISTICAL DISTRIBUTION USED IN RELIABILITY AND MAINTAINABILITY.....		209
B-1	INTRODUCTION TO STATISTICAL DISTRIBUTION.....	209
B-1.1	Exponential and Weibull.	209
B-1.2	Normal and Lognormal.	209
B-2	THE EXPONENTIAL DISTRIBUTION.....	209
B-3	THE WEIBULL DISTRIBUTION.....	210
B-4	THE NORMAL DISTRIBUTION.	212
B-5	THE LOGNORMAL DISTRIBUTION.....	213
APPENDIX C AVAILABILITY AND OPERATIONAL READINESS		215
C-1	AVAILABILITY.....	215
C-1.1	Nature of the Equations.	215
C-1.2	Derivation of Steady State Equation for Availability.	215
C-2	OPERATIONAL READINESS.....	218
C-2.1	Readiness in the Commercial World.....	218
C-2.2	Relationship of Availability and Operational Readiness.....	218
APPENDIX D PREP DATABASE IEEE DOT STANDARD 3006.8		219
APPENDIX E GLOSSARY		237
E-1	ACRONYMS.....	237
E-2	DEFINITION OF TERMS.....	240
APPENDIX F REFERENCES		251

FIGURES

Figure 2-1	System Response to a Disruptive Event	4
Figure 2-2	Two System with Different Robustness.....	5
Figure 2-3	Two Systems with Different Recovery Time.....	6
Figure 2-4	A Sound Reliability Strategy addresses All Phases of a System's Life Cycle	11
Figure 2-5	Factors Selecting Tasks for a Specific Program.....	12
Figure 4-1	RBD for a Typical Distribution System	24
Figure 4-2	Fragility Curves vs Event Probability.....	25
Figure 4-3	Distribution System Model in Degraded State	27
Figure 4-4	Stepped Recovery of Power System Assets	29
Figure 4-5	Sample Recovery Timeline	30
Figure 4-6	N+2 vs N+1 System Resilience	32
Figure 5-1	Typical Normal Distribution Curve	37
Figure 5-2	Exponential Curve Relating Reliability and Time.....	40
Figure 5-3	Example RBD	40
Figure 5-4	RBD of a System with Redundant Components	41
Figure 5-5	Different Combinations of MTBF and MTTR Yield Same Availability	44
Figure 5-6	Example Availability Block Diagram	46
Figure 5-7	Availability Block Diagram of a System with Redundant Components	46
Figure 5-8	Types of Redundancy.....	54
Figure 5-9	Effect of Maintenance Concept on Level of Fault Tolerance	58
Figure 5-10	Analyzing the Contribution to System Reliability Helps Determine Where Redundancy is Needed.....	59
Figure 5-11	Simple Markov Model	66
Figure 5-12	Less Simple Markov Model	67
Figure 5-13	Timeline of a Monte Carlo Simulation	69
Figure 5-14	Simple Series Model.....	71
Figure 5-15	Simple Parallel Model	73
Figure 5-16	Simple Parallel Model, First Reduction.....	73
Figure 5-17	Simple Parallel Model, Second Reduction.....	74
Figure 5-18	Parallel Model with Controls Contingency	75

Figure 5-19	Double Ended Bus	75
Figure 5-20	Model of Double Ended Bus	76
Figure 5-21	Model of Double Ended Bus, Case 1.....	77
Figure 5-22	Model of Double Ended Bus, Case 2.....	77
Figure 5-23	Downstream Fault.....	79
Figure 6-1	Facility Development Process	83
Figure 6-2	Typical FMEA Flow	85
Figure 6-3	Functional Method.....	86
Figure 6-4	Hardware Method.....	87
Figure 6-5	Functional Block Diagram of System.....	91
Figure 6-6	Functional Block Diagram of the Sub-Systems	92
Figure 6-7	Reliability Block Diagram.....	93
Figure 6-8	FMECA Flow.....	110
Figure 6-9	Data Triangle	113
Figure 6-10	Single Point System vs Redundant System	130
Figure 6-11	Criticality Matrix.....	144
Figure 7-1	Major Categories of Maintenance by when Performed.....	154
Figure 7-2	Typical Approach to Categorizing Maintenance by where it is Performed.	155
Figure 7-3	An Example of Packaging PM Tasks.....	159
Figure 7-4	Example of how PM Cards can be used to Document Required PM Tasks	160
Figure 7-5	The RCM Process Starts in the Design Phase and Continues for the Life of the System	161
Figure 7-6	Applicability of Age Limit Depending on Failure Pattern	167
Figure 7-7	Block Diagram of A simple Redundant System	171
Figure 7-8	The RCM Process	181
Figure 7-9	RCM Decision Logic Tree (Adapted from MSG-3).....	187
Figure 7-10	Evident Failure – Hazardous Effects	190
Figure 7-11	Evident Failure – Operational Effects	191
Figure 7-12	Evident Failure – Economic Effects	192
Figure 7-13	Hidden Failure – Hazardous Effects.....	194
Figure 7-14	Hidden Failure – Non-Hazardous Effects.....	195

Figure B-1 The Exponential PDF for Varying Values of λ 210

Figure B-2 The Two-Parameter Weibull PDF for Different Values of β and a Given Value of η 212

Figure B-3 The Normal PDF for Varying Values of σ and Fixed μ 213

Figure B-4 The Lognormal PDF for Different Values of μ and a Fixed σ 214

Figure C-1 Simple Markov Model..... 216

TABLES

Table 2-1 Typical Reliability-Related Measures 12

Table 4-1 Average Weekly Downtime Based on Availability 30

Table 4-2 Determine Resilience Requirements..... 34

Table 5-1 Commonly Used Continuous Distributions..... 37

Table 5-2 Effect of Measurement Interval on Observed Availability 45

Table 5-3 Methods for Assessing Reliability..... 48

Table 5-4 The Process for Improving Facility Availability 49

Table 5-5 Analyses Helpful in Designing for Reliability..... 51

Table 5-6 Diagnostic Implications of Fault Tolerant Design Approaches 56

Table 5-7 Availability of System Depicted in Figure 5-10 59

Table 5-8 Relative Unreliability of Subsystems (Repairs Ignored)..... 60

Table 6-1 Example of DA Form 7610, FMEA Worksheet Flow (One Column at a Time) 95

Table 6-2 Example of DA Form 7610, Functional FMEA System Level..... 96

Table 6-3 Example of DA Form 7610, FMEA Progression..... 100

Table 6-4 Severity Ranking Table 103

Table 6-5 Severity Classification for Qualitative CA 104

Table 6-6 Example of DA Form 7610, Completed FMEA (functional) for Industrial Water Supply 106

Table 6-7 Example of DA Form 7610, Completed FMEA (hardware) for HVAC System 107

Table 6-8 Example of DA Form 7611, FMECA Worksheet – Quantitative 111

Table 6-9 Example of DA Form 7611, FMECA Worksheet – Qualitative 112

Table 6-10 Failure Mode Ratio (α) 115

Table 6-11	Example of DA Form 7611, Quantitative FMECA with Redundant Components	124
Table 6-12	Occurrence Rankings	127
Table 6-13	Severity Rankings.....	127
Table 6-14	Detection Rankings	129
Table 6-15	Example of DA Form 7612, FMECA Worksheet Using Qualitative Rankings	134
Table 6-16	Example of DA Form 7613, Failure Mode Criticality Rankings	138
Table 6-17	Example of DA Form 7614, Item Criticality Rankings	141
Table 7-1	Cost Benefits of using RCM for Developing PM Program.....	150
Table 7-2	Examples of Tasks under Two Categories of Preventive Maintenance	156
Table 7-3	Data Sources for the RAM Analysis	164
Table 7-4	Non-Destructive Inspection (NDI) Techniques, Briefly	166
Table 7-5	Examples of Failure Mechanisms and Modes.....	166
Table 7-6	Examples of Failure Effect Categorization	168
Table 7-7	Examples of Effects of Operational Failures.....	172
Table 7-8	Criteria for Applying RCM to Products	173
Table 7-9	General Data Sources for the RCM Analysis.....	175
Table 7-10	NDI Techniques.....	178
Table 7-11	Data Elements from FMEA that are Applicable to RCM Analysis....	184
Table 7-12	Example of Failure Modes and Effects Analysis Worksheet; DA Form 7610	185
Table B-1	Summary of the Exponential Distribution.....	210
Table B-2	Summary of the Weibull Distribution	211
Table B-3	Summary of the Normal Distribution.....	213
Table B-4	Summary of the Lognormal Distribution.....	214
Table C-1	Quantitative Measures of Availability.....	215
Table D-1	Reliability and Maintainability Calculations.....	219
Table D-2	USACE-PREP Equipment Reliability Database	220

This Page Intentionally Left Blank

CANCELLED

CHAPTER 1 INTRODUCTION

1-1 BACKGROUND.

Unified Facilities Criteria (UFC) documents provide planning, design, construction, sustainment, restoration, and modernization criteria. They also apply to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with USD (AT&L) Memorandum dated 29 May 2002. The United States Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Systems Command (NAVFAC) and the Office of the Air Force Civil Engineer are responsible for administration of the UFC system. This is one of those documents.

Resilience is “the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions.” When applying resilience principles to the design and operation of critical facilities, it is useful to incorporate tools for evaluating the effectiveness of existing and proposed system designs or upgrades. The purpose of this document is to describe quantitative methods for evaluating the resilience of an existing or proposed designs for the electrical, Mechanical and Controls for Critical Facilities.

1-2 PURPOSE AND SCOPE.

This document summarizes current knowledge, research related to backup power system reliability, and identified best cost options in areas for R&D investment. The scope of this document is electrical systems, cooling systems (chilled water systems, condenser water systems, and all other aspects for facility cooling) and control systems.

1-3 APPLICABILITY.

This document’s concepts are applicable to mission critical systems. The design requirements in this document apply to mission critical facility design and construction and within-scope design and construction of exterior utility systems that are in direct support of mission critical facility functions.

1-4 GENERAL BUILDING REQUIREMENTS.

Comply with UFC 1-200-01, *DoD Building Code*. UFC 1-200-01 provides applicability of model building codes and government unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, high performance and sustainability requirements, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

1-5 CYBERSECURITY.

All facility-related control systems (including systems separate from a utility monitoring and control system) must be planned, designed, acquired, executed, and maintained in accordance with UFC 4-010-06, and as required by individual Service Implementation Policy.

1-6 GLOSSARY.

APPENDIX E contains acronyms, abbreviations, and terms.

1-7 REFERENCES.

APPENDIX F contains a list of references used in this document. The publication date of the code or standard is not included in this document. Unless otherwise specified, the most recent edition of the referenced publication applies.

CANCELLED

CHAPTER 2 RESILIENCE

2-1 RESILIENCE.

2-1.1 Prepare, Absorb, Recover and Adapt.

RESILIENCE is the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions. When applying resilience principles to the design and operation of critical facilities, it is useful to incorporate tools for evaluating the effectiveness of existing and proposed system designs or upgrades. The purpose of this chapter is to describe quantitative methods for evaluating the resilience of an existing or proposed design.

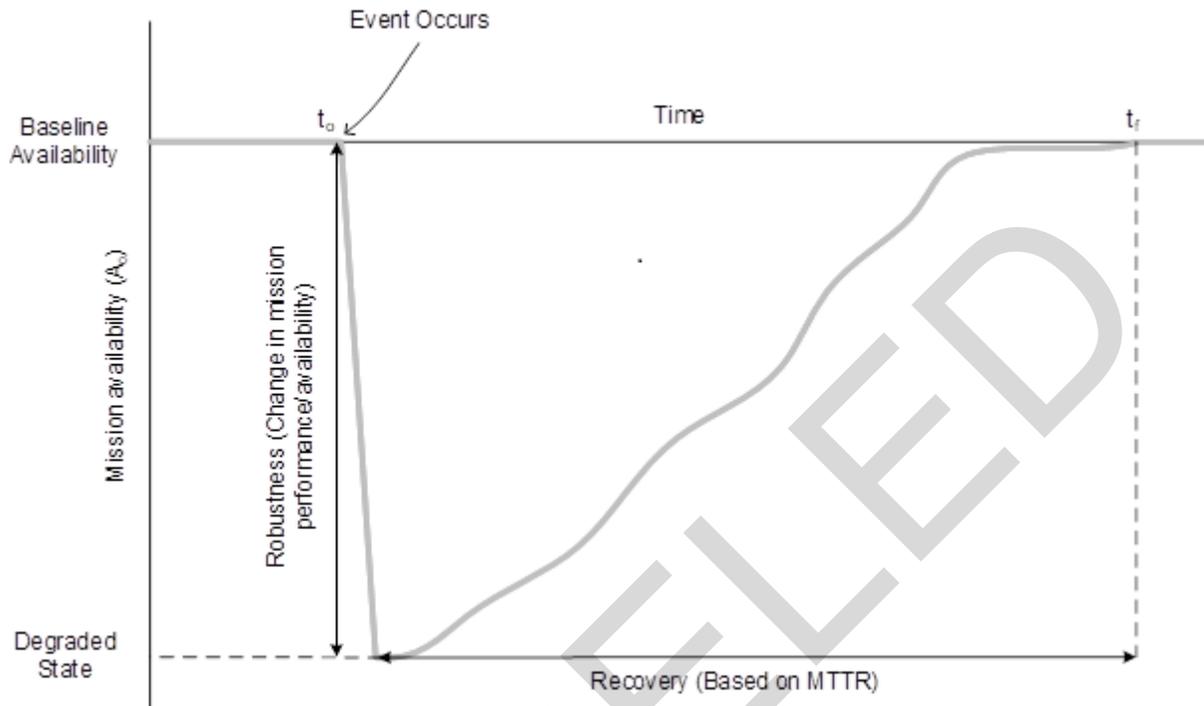
2-1.2 Considerations.

System operational considerations and the nature of events to be considered may dictate the preferred measure of availability for evaluating a given event. For example, hurricanes are often closely tracked and forecasted, allowing for several days or even weeks of advance notice prior to arrival. This can provide time for workers to delay or back out of planned maintenance tasks. In this situation, the availability of the system is more representative of its inherent availability. For disturbances which occur without warning such as seismic events, it may be more useful to consider operational availability as this is more representative of normal day-to-day operations. For the purposes of this discussion, the following examples will refer to operational availability.

2-1.3 Absorption and Recovery.

Using availability concepts, the overall resilience of a system can be quantified in two phases: absorption of the event, and recovery. Consider an event occurring as shown in Figure 2-1.

Figure 2-1 System Response to a Disruptive Event



Immediately following the event, there is a sharp drop in mission availability. The change in mission availability from the baseline to the degraded state represents the robustness of the system to that particular event. The lower the change in mission availability, the more robust the system. The time required to restore the system to its baseline state is referred to as recovery. This is based on the mean-time-to-repair (MTTR) of any assets affected by the event and may be affected by several factors including site remoteness, event severity, and environmental conditions. The overall resilience, $R(t)$ of the system to any particular event can be quantified according to the area under the curve as shown in Equation 2-1. By this model, a perfectly resilient system would have resilience index value of zero.

Equation 2-1. Resilience

$$R(t) = \int_{t_o}^{t_f} A_o(t) dt$$

Where:

$R(t)$ = resilience

t_f = time required to restore (hours)

t_o = time event occurs (hours)

A_o = mission availability

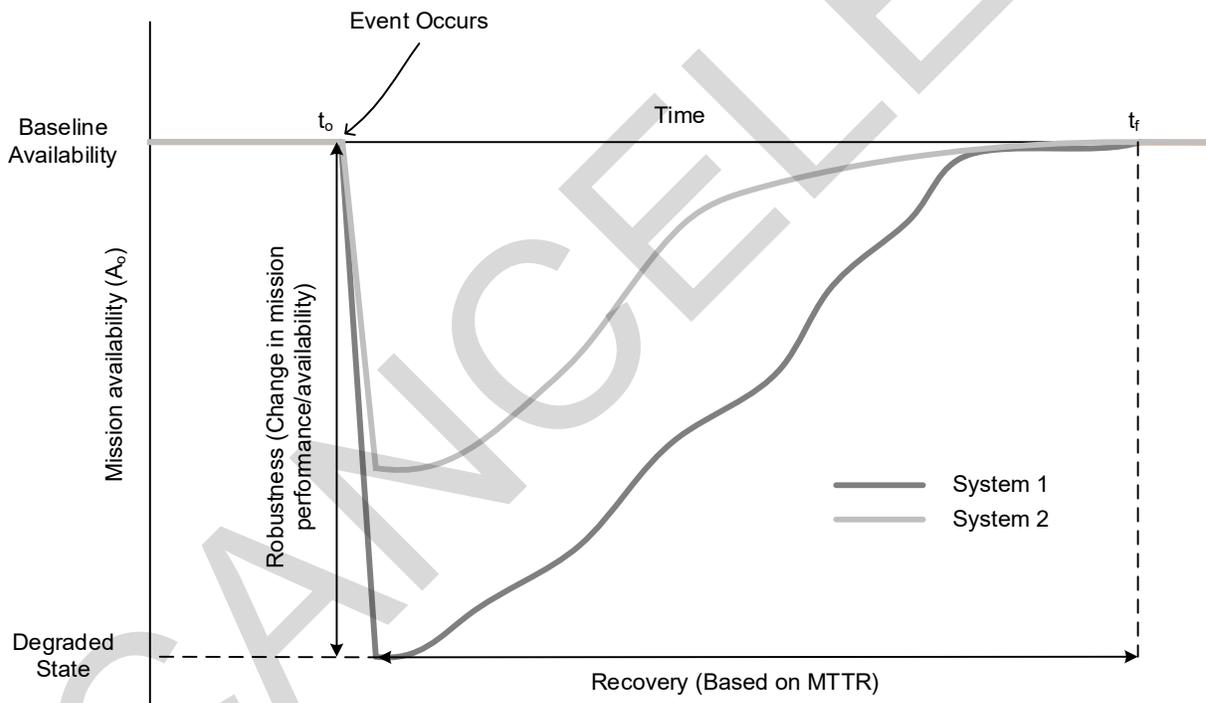
(t) = time (hours)

dt = downtime (hours)

2-1.4 Prioritizing Robustness or Recovery.

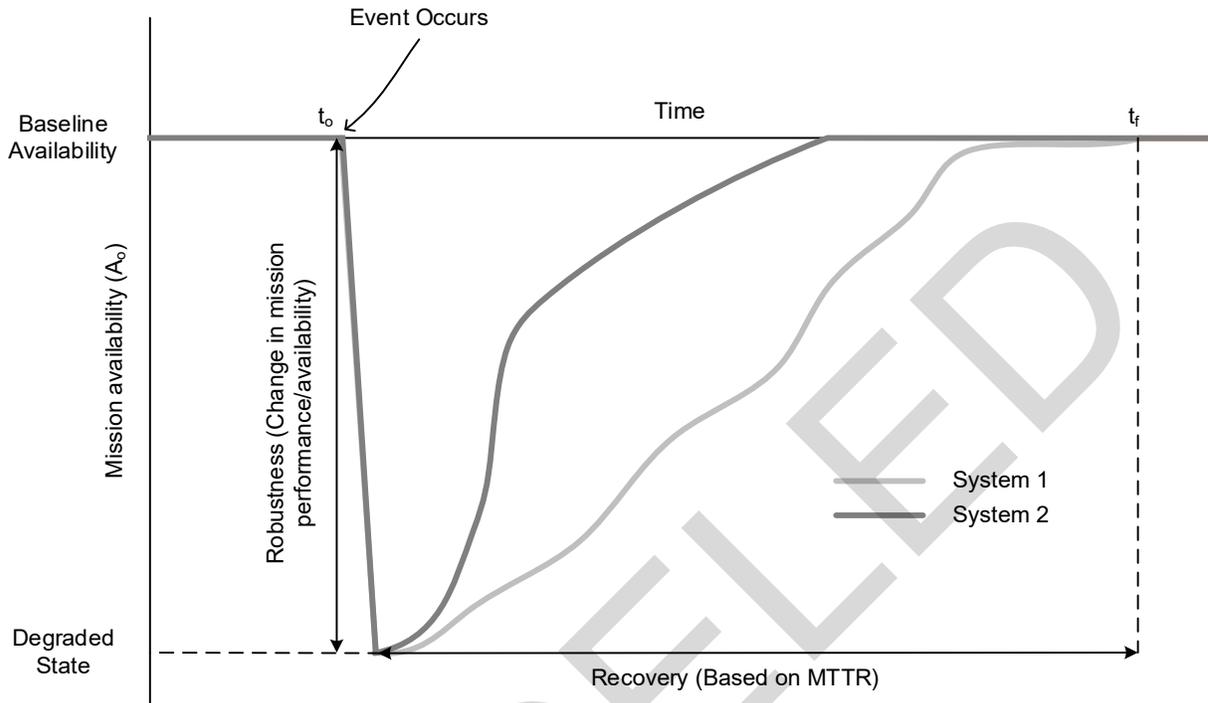
Depending on mission needs, it may be more important to prioritize either robustness or recovery. For those installations with limited availability of repair parts and personnel, consider prioritizing robustness. Where resources are more readily available, consider prioritizing recovery, provided that the minimum requirements for mission functions are satisfied. Figure 2-2 shows two systems with different levels of resilience. The two systems have the same recovery time, but System 2 has a lower initial decrease in mission availability. System 2 is more resistant to the postulated event and is more resilient than system 1 despite having the same recovery time. This may be beneficial for improving overall resilience at remote sites where recovery time is limited by the physical demand of getting replacement parts to the site.

Figure 2-2 Two System with Different Robustness



In other cases, it may be more important to prioritize recovery from an event as opposed to robustness. Figure 2-3 shows two systems with similar robustness to an event, but different recovery times. Though both systems have the same ability to absorb the shock from the event, the shorter recovery time for System 2 yields less area under the curve. Accordingly, System 2 can be said to be more resilient than System 1. The difference between the system responses shown in Figure 2-2 and Figure 2-3 demonstrate that similar improvements in overall resilience can be achieved by improving either robustness or recovery. Consider site-specific factors such as duration of backup power supplies and minimum equipment requirements when determining an optimal resilience improvement strategy.

Figure 2-3 Two Systems with Different Recovery Time



2-1.5 Availability Definitions.

Availability is defined as the percentage of time that a system is available to perform its required function(s). It is measured in a variety of ways, but it is principally a function of downtime. Availability can be used to describe a component or system, but it is most useful when describing the nature of a system of components working together. Because it is a fraction of time spent in the “available” state, the value can never exceed the bounds of $0 < A < 1$. Thus, availability will most often be written as a decimal, as in 0.99999, as a percentage, as in 99.999%, or equivalently spoken, “five nines of availability.” Chapter 5 contains a detailed discussion of availability.

2-1.5.1 Operational Availability (A_0).

Another equation for availability directly uses parameters related to the reliability and maintainability characteristics of the item as well as the support system. Equation 2-2 reflects this measure.

Equation 2-2. Operational Availability

$$A_o = \frac{MTBM}{MDT + MTBM}$$

Where:

A_o = operational availability

MTBM = mean time between maintenance (hours)

MDT = mean downtime (hours)

2-1.5.2 Inherent Availability (A_i).

In Equation 2-2, MTBM includes all maintenance required for any reason, including repairs of actual design failures, repairs of induced failures, cases where a failure cannot be confirmed, and preventive maintenance. When only maintenance required to correct design failures are counted and the effects of the support system are ignored, the result is inherent availability, which is given by Equation 2-3.

Equation 2-3. Inherent Availability

$$A_i = \frac{MTBF}{MTTR + MTBF}$$

Where:

A_i = inherent availability

MTBF = mean time between failure

MTTR = mean time to repair

2-1.6 Reliability.

Reliability is concerned with the probability and frequency of failures (or more correctly, the lack of failures). A commonly used measure of reliability for repairable systems is the mean time between failures (MTBF). The equivalent measure for non-repairable items is mean time to failure (MTTF). Reliability is more accurately expressed as a probability of success over a given duration of time, cycles, etc. For example, the reliability of a power plant might be stated as 95% probability of no failure over a 1000-hour operating period while generating a certain level of power. (Note that the electrical power industry has historically not used the definitions given here for reliability. The industry defines reliability as the percentage of time that a system is available to perform its function, such as, availability. The relationship between reliability and availability is discussed in paragraph 2-1.8.)

2-1.7 Maintainability.

Maintainability is defined as the measure of the ability of an item to be restored or retained in a specified condition. Maintenance should be performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. Simply stated, maintainability is a measure of how effectively and economically failures can be prevented through preventive maintenance

and how quickly system operation can be restored following a failure through corrective action. Note that maintainability is not the same as maintenance. Maintainability is a design parameter, while maintenance consists of actions to correct or prevent a failure event.

2-1.8 Relationship Among Reliability, Maintainability, and Availability.

Perfect reliability (such as, no failures, ever, during the life of the system) is difficult to achieve. Even when a "good" level of reliability is achieved, some failures are expected. The effects of failures on the availability and support costs of repairable systems can be minimized with a "good" level of maintainability. A system that is highly maintainable can be restored to full operation in a minimum of time with a minimum expenditure of resources.

2-1.8.1 Inherent Availability.

Inherent availability is when only reliability and corrective maintenance or repair (such as, design) effects are considered. This level of availability is solely a function of the inherent design characteristics of the system.

2-1.8.2 Operational Availability.

Availability is determined not only by reliability and repair, but also by other factors related to preventative maintenance and logistics. Operational availability is when the effects of preventative maintenance and logistics are included. Operational availability is a "real-world" measure of availability and accounts for delays such as those incurred when spares or maintenance personnel are not immediately at hand to support maintenance.

2-1.9 Factors Influencing Availability.

Availability of a system in actual field operations is determined by the following.

2-1.9.1 The Frequency of Occurrence of Failures.

These failures may prevent the system from performing its function (mission failures) or cause a degraded system effect. This frequency is determined by the system's level of reliability.

2-1.9.2 Restoration and Maintenance Time.

The time required restoring operations following a system failure or the time required to perform maintenance to prevent a failure. These times are determined in part by the system's level of maintainability.

2-1.9.3 Logistics Delays.

The logistics provided to support maintenance of the system. The number and availability of spares, maintenance personnel, and other logistics resources combined

with the system's level of maintainability determine the total downtime following a system failure.

2-1.9.4 Reliability Impact.

Reliability is a measure of a system's performance that affects availability, mission accomplishment, and operating and support (O&S) costs. Too often performance is only thought of in terms of voltage, capacity, power, and other "normal" measures. However, high frequency of system failures can be overshadowing the importance of more typical system metrics.

2-1.9.5 Impact of Failures and Costs.

Reliability also affects the costs to own and operate a system. Using an example of a critical DoD facility, Reliability determines how often repairs are needed. The less often the facility has a failure, the less it will cost to operate over its life. The reliability of any repairable system is a significant factor in determining the long-term costs to operate and support the system. For non-repairable systems, the cost of failure is the loss of the function (for example, the missile misses its target, the fuse fails to protect a circuit, etc.). In addition, the mission plays a part in the overall operation of the facility. The objective is to run as efficient as possible while still maintaining mission requirements.

2-1.9.6 Improving Availability of Failures.

Regardless of how reliable a system may be, failures will occur. An effective maintenance program applied to a system that has been designed to be maintainable is necessary to deal with the certainty of failure. Even when several redundant items are installed to decrease the chance of a mission failure, when any one item fails, it must be repaired or replaced to retain the intended level of redundancy.

2-1.10 Improving Availability of C5ISR Facilities.

The decision on which methods to use for improving availability depends on whether the facility is being designed and developed or is already in use.

2-1.10.1 Existing C5ISR Facilities.

For a facility that is being operated, three basic methods are available for improving availability when the current level of availability is unacceptable:

- Selectively adding redundant units, such as: (e.g., generators, chillers, fuel supply, etc.) to eliminate sources of single-point-failure
- Optimizing maintenance using a reliability-centered maintenance (RCM) approach to minimize downtime
- Redesign subsystems to replace components and subsystems with higher reliability items.

2-1.10.2 New C5ISR Facilities.

The opportunity for designing high availability and reliability systems is greatest when designing a new facility. A highly available facility will result from the following: applying an effective RAM strategy, modeling, and evaluating the systems, designing for maintainability, and ensuring that manufacturing and commissioning do not negatively affect the inherent levels of reliability, availability, and maintainability. Further, upon completion, an RCM program should be employed to cultivate the opportunities for high RAM success. Although the primary focus of this UFC is on improving the availability of current facilities, a brief discussion of the approach used when designing a new facility is provided in the next paragraphs to give the reader an appreciation of an effective design and development program.

2-1.10.2.1 RAM Strategy.

A RAM strategy describes how an organization approaches reliability for all systems and services it develops and provides to its customers. The strategy can be considered as the basic formula for success, applicable across all types of systems and services. A reliability strategy that has proved successful in a variety of industries and in government is shown in Figure 2-4.

2-1.10.2.2 RAM Program.

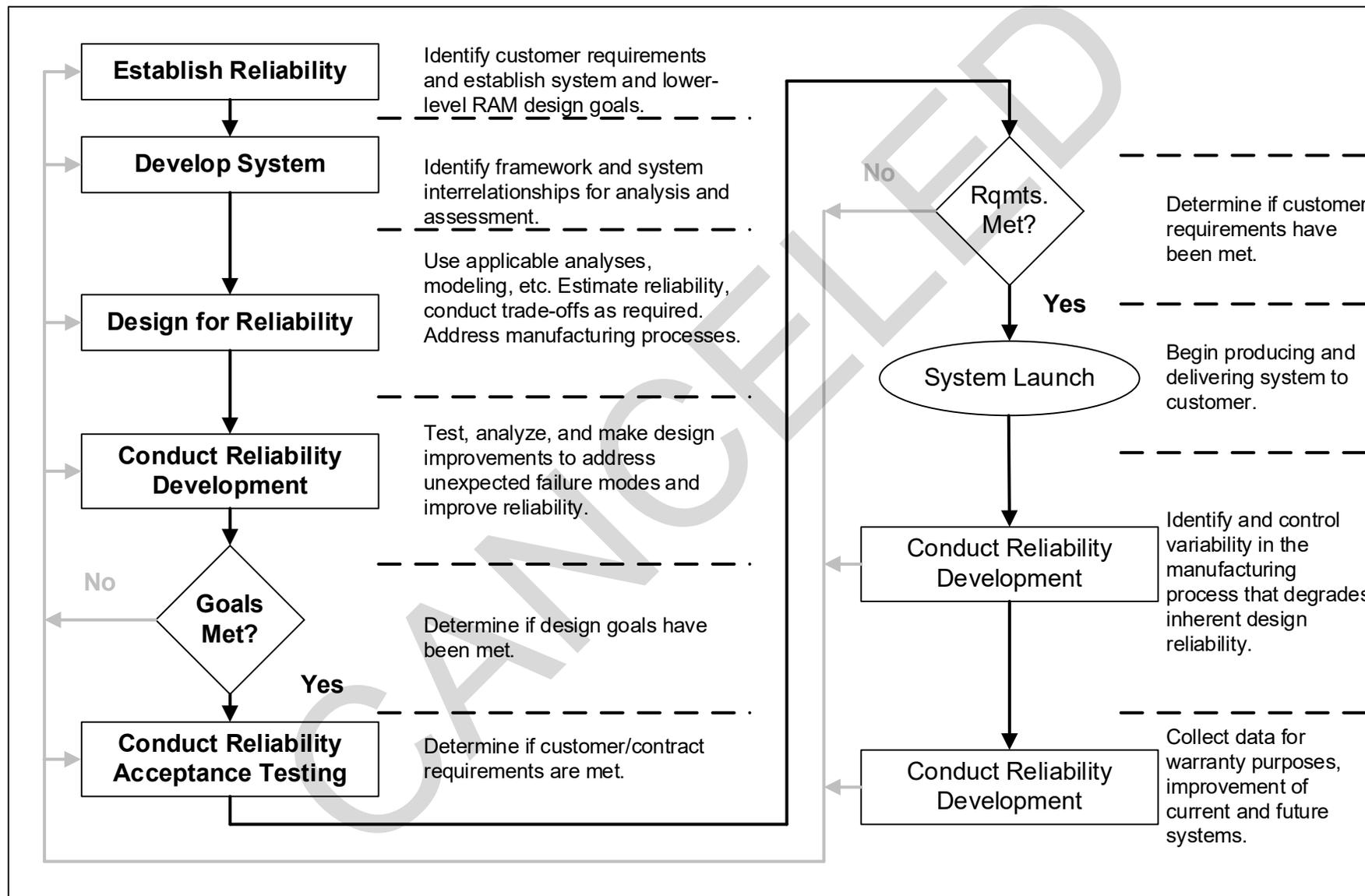
A RAM program is the application of the RAM strategy to a specific system or process. As can be inferred from Figure 2-4, each step in the strategy requires the selection and use of specific methods and tools. For example, various methods can be used to develop requirements or evaluating potential failures.

(a) Developing Requirements. Translations and analytical models can be used to derive requirements. Quality Function Deployment (QFD) is a technique for deriving more detailed, lower-level requirements from one level of indenture to another, beginning with customer needs. It was developed originally as part of the Total Quality Management movement. Translations are parametric models intended to derive design RAM criteria from operational values and vice versa. Analytical methods include:

- thermal analysis
- durability analysis
- predictions, etc.

They are used to make accommodations for special considerations to system design, such as environmental concerns.

Figure 2-4 A Sound Reliability Strategy addresses All Phases of a System's Life Cycle



(b) Evaluate possible failures. Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are two different methods for evaluating possible failures. The reliability engineer must determine which one to use, or whether to use both. Chapters 5, 6 and 7 will address these and other methods and how to determine which are applicable to a specific situation. Selecting the specific tasks to accomplish each step of the strategy results in a tailored system program. Figure 2-5 shows some of the factors that must be considered in selecting tasks to implement the reliability strategy.

Figure 2-5 Factors Selecting Tasks for a Specific Program

<p>Effectiveness and applicability of tasks vary depending on:</p> <ul style="list-style-type: none"> • Production runs (total population) – limits use of system-level statistical analysis • Critical functions/cost of failure – may require exhaustive analysis • Technology being used – may require new models • Nature of development (such as evolutionary vs. revolutionary) experience of much less value when breaking new ground <p>Selection of tasks is also a function of past experience, budget, schedule, and the amount of risk commanders and facility managers are willing to accept</p>

2-1.10.2.3 Reliability Requirements.

The entire effort of designing for reliability begins with identifying the customer's reliability requirements. These requirements are stated in a variety of ways, depending on the customer and the specific system. Table 2-1 lists some of the ways in which a variety of industries measure reliability. Note that in the case of the oil & gas and communications industries, availability is the real requirement. The reliability and maintainability requirements must then be derived based on the availability requirement.

Table 2-1 Typical Reliability-Related Measures

Customer	System	Measure of Reliability
Airline	Aircraft	On-time departure
Consumer	Automobile	Frequency of Repair
Hospital	Medical	Availability & Accuracy
Military	Weapon	Mission Success Probability
Highway Department	Bridge	Service Life
Oil & Gas	Sub-sea	Availability
Communications Organization	Utilities	Availability

2-2 PROGRAM ELEMENTS.

The essential elements of a system's engineering program are described below. They must be considered in light of the organization's mission and function, the availability of

existing natural and manmade resources and the security necessary for a new or existing facility.

2-2.1 RAM Requirements Implementation.

The designer must implement reliability, availability, and maintainability (RAM) to achieve the required availability of the C5ISR utility systems.

2-2.2 Human Factors Engineering (HFE).

Human factors engineering (HFE) activities will ensure that reliability, availability, and safety of the C5ISR power system are not degraded through human activities during operation or maintenance. The design agency must accomplish the HFE program requirements using established standard HFE design criteria and practices based on MIL-STD-1472, Human Engineering.

2-2.3 Power System Safety Program.

The C5ISR power system safety program must ensure that the design incorporates, within program restraints, the highest attainable level of inherent safety. It must eliminate or reduce the probability of events that can cause injury or death to personnel, or damage to or loss of equipment or property. For example, pipes, lines, and tanks must be placed away from high-traffic areas. Safety documentation must be provided for safety items that require designation or may cause action during subsequent program phases. The design agency system safety program must be based on a philosophy that the most effective actions to control potential hazards are those taken early in the design process.

2-2.3.1 Special Operating Procedures.

When hazards cannot be controlled by design measures, including safety and warning devices, special operating procedures must be developed and documented. The safety program must provide support to the systems engineering (SE) program and must ensure that the applicable requirements of MIL-STD-882, System Safety, are met.

2-2.3.2 System Safety Analyses.

The systems safety program must define and address the system safety analyses that must be performed during development of design. During the early design phase, an analysis that identifies conditions that may cause injury or death to personnel and damage or loss to equipment and property must be performed. Prior to the final safety design review, the design agency must perform a second systems safety analysis to determine adherence of the design to all required safety standards and criteria, and to ensure avoidance or reduction of identified hazards. Operating and maintenance procedures must also be reviewed for compliance with all required safety standards and criteria.

2-2.3.3 Safety Hazards Identified.

The systems safety program must include procedures to ensure that safety hazards identified by the systems safety analyses are eliminated or reduced to acceptable levels of risk, and that those actions taken are fully documented.

2-2.3.4 Safety Program Documentation.

The design agency must prepare specific safety program documentation. This documentation must include, but not be limited to, safety analysis reports and the final systems safety report.

2-2.4 Consolidation Systems Test Program.

The design agency must develop a consolidated systems test program that covers all phases of testing, develops confidence in the system, and provides means for interim and final acceptance of equipment and systems. The design agency must minimize cost through elimination of testing duplication and by maximizing the collection of data for each test. Successful completion of these tests must be accomplished prior to final acceptance.

2-2.5 Standardization Program.

The design agency must develop and implement a standardization program to minimize equipment and component stockage. Redundant systems must be of the same design.

2-2.6 Configuration Management (CM) Program.

The configuration management (CM) program must maintain effective control over design from criteria development through design, construction, and installation of the equipment. The design agency should work with maintenance staff supervisor to determine maintenance capabilities and any training or funding requirements. A government configuration control procedure must be developed by the design agency for use in the C5ISR utility systems configuration control program.

2-2.7 Operations and Maintenance Planning.

Operations and maintenance (O&M) planning will be done by the design agency and must identify and recommend essential items of the program during the design phase. The design agency should work with maintenance staff supervisors to determine maintenance capabilities and any training or funding requirements. An RCM program should be implemented to identify single point failures and identify the critical systems. Basic elements of the program are as follows.

2-2.7.1 Data Requirements.

As part of the SE database, data requirements must be identified for preparation of O&M manuals. Systems functional descriptions must be developed. Requirements must be developed for data collection, including spare parts list, calibration requirements,

special tools and test equipment, spare parts stockage level, and shelf-life data. Spare parts list, spare parts stockage level, test equipment, and test frequency must be provided for the using government agency. For a resilient C5ISR facility, spare parts for critical equipment are necessary to make the facility complete and usable, because they impact the required resilience of the facility design.

2-2.7.2 Complex Systems and Equipment.

Systems and equipment of high complexity or peculiarity must be identified, and special training for personnel who operate and maintain such systems and equipment must be identified.

2-2.7.3 Identify Critical Items.

The design agency must identify those items critical to accuracy and repeatability and must recommend calibration requirements. Unique calibration requirements and procedures must be provided whenever necessary.

2-2.7.4 Systems Test and Checkout.

Systems test and checkout requirements to be performed following major maintenance activities must be developed during design to ensure safe and normal operation of the system.

CANCELLED

This Page Intentionally Left Blank

CANCELLED

CHAPTER 3 DESIGN CONSIDERATIONS

3-1 RELIABILITY/AVAILABILITY DESIGN REQUIREMENTS.

3-1.1 Availability Requirements.

The availability will initially be set to at least 0.999 (99.9%, approximately 8 hours and 45 minutes of downtime a year). The criticality of the mission will determine if a higher availability is required but must not be required to exceed 0.999999 (99.9999%, approximately 31 seconds of downtime a year). The utility systems must be evaluated using the standard R/A analysis techniques to determine if goals are met.

3-1.2 Responsibilities for Determining Availability Requirements.

The mission and facility owners and operators should be the parties responsible for determining the availability requirements for their mission and facility. In the absence of the mission and facility owners and operators providing the availability requirements the facility should be designed and constructed to a minimum of at least 0.999 (99.9%, approximately 8 hours and 45 minutes of downtime a year).

3-1.3 Availability Requirements for Specific Facility Types.

There are some missions and facilities that are critical enough to require a higher availability requirement. Even if the mission and facility owners and operators do not provide availability requirements the following missions and facilities should be designed and constructed to the minimum availability level listed.

The criticality of the following missions and facilities is sufficiently high they should be designed and constructed to have a minimum availability of at least 0.99999 (99.999%, approximately five minutes of downtime a year). This availability requirement applies to any operational headquarters facility, airfield and supporting infrastructure, harbor facility supporting naval vessels, munitions production and storage facility, radar, space launch facility, or operational communications facility that is determined to be a critical mission.

The criticality of the following missions and facilities is sufficiently high they should be designed and constructed to have a minimum availability of at least 0.999999 (99.9999%, approximately 31 seconds of downtime a year). This availability requirement applies to any missile field, ballistic missile early warning radar, satellite control facility, cyber operations facility, or biological defense facility that is determined to be a critical mission.

3-2 GENERAL DESIGN REQUIREMENTS.

The design agency's role in the O&M concept is to establish the foundation for stable C5ISR utility systems that must provide continuous operation incorporating redundancy (dual systems), readiness (standby systems), flexibility (multiple modes of operations), and standardization (parts and equipment). Power plant facilities, systems, and O&M

documentation must be designed to permit rapid startup and repair of equipment under emergency conditions. O&M functions must be enhanced through the application of these guidelines by the C5ISR utility systems designer.

3-2.1 Historical Records.

A recording device must be included in the design to provide a log of facility performance. This recorder must accept either analog or digital signals (such as input and output parameters for generators, main switchgear feeders, uninterruptible power supply (UPS) systems, power distribution units, chillers, etc.), convert them to numerical data, scale them to useful values and store them in electronic storage. The signals should be stored at intervals of 15 minutes or other specified preset time intervals. The recorder must have the capability to record critical signal values more frequently than the preset recording rate (for example, every five seconds) when prompted by a signal from the operator or operating equipment. The recorder must automatically return to its primary recording when system operation returns to normal. Records must be maintained on-site for a minimum of five years. A supervisory control and data acquisition (SCADA) system should be incorporated into the design of the systems.

3-2.2 Control Systems.

Control systems are the third major component making a C5ISR facility as reliable as possible with electrical systems being the first major component and mechanical systems being the second major component. Control systems are the brains behind the operational characteristics during normal and abnormal conditions. Control systems are commonly identified as SCADA systems and are designed to monitor conditions and react in a manner to maintain a set point. Typical SCADA systems are comprised of a series of sensors sending signals to a central command center where the signals are interpreted. A data communication protocol will be required for the signals between the central command center and the sensors to be interpreted and acted upon. Some examples of common data communication protocols include Lonworks and BACNet. There are other data communication protocols available and the protocol providing the most robust solution should be used. Signals are sent from the command center to actuators to throttle input conditions and provide the necessary environmental condition required for the mission operations. Typical components for a SCADA system are:

- Computer access panel
- Digital drivers
- Power supplies
- Programmable Logic Controller (PLC)
- Interface devices such as control panels or circuit breakers

3-2.3 Maintenance Concepts.

The design outputs prepared by the design agency must reflect the following maintenance concepts.

3-2.3.1 Equipment Standardization Program.

The design agency must develop and implement an equipment standardization program to simplify equipment maintenance.

3-2.3.2 Modular Designed Subassemblies.

The design agency must specify modular designed subassemblies which will permit rapid repair.

3-2.3.3 Built-in Test Modules/Fault Sensors.

The design agency must specify that manufacturers provide built-in test modules/fault sensors. Selector switches that allow personnel to access and sequentially monitor operating variables within an assembly must be provided.

3-2.3.4 Equipment Tag.

The design agency must specify that a plate with an equipment tag number be attached to the equipment by the construction contractor. The design agency must specify a method for identifying and numbering wires and cables, for marking cable termination strips, and for uniformly interconnecting equipment of different manufacturers. Corresponding identity codes must be used for termination strips and wiring. The design agency must specify that if a manufacturer changes the characteristics of a purchased component for use in a composite item, the true source identity of the originally purchased part will remain intact.

3-2.4 Evaluations.

The following evaluations must be an integral part of the design process.

3-2.4.1 Operations Evaluations.

Operations evaluations must consider both user and system requirements.

(1) The design agency must evaluate user requirements to determine operating parameters and the effect that these parameters will have on system operation, output efficiency, and personnel safety. The design agency must determine if limits need to be placed on manual control and, if so, must specify those limits.

(2) The design agency must evaluate the system requirements as to the operational effects produced by changing power by switching the source of electrical power and maintenance or repair activities within the facility. System designers must identify critical mission variables subject to O&M schedules and incorporate equipment and/or

operational redundancies to perform maintenance without disruption to critical operations. The design agency must specify areas in the control system that should allow automatic adjustments to system equipment to aid the operator when events occur that demand immediate operator intervention.

3-2.4.2 Evaluate User Constraints and Parameters.

The design agency must evaluate user constraints and parameters to ensure maintainability of the C5ISR utility systems.

3-2.4.3 Perform a Hazard Evaluation.

The design agency must perform a hazard evaluation to ensure adherence to Occupational Safety and Health Administration (OSHA), National Electrical Code (NEC), and other locally binding safety standards.

3-2.5 Operations and Maintenance Documentation.

The design agency must perform an O&M analysis to identify the equipment in the C5ISR utility systems that contributes significantly to the maintenance burden of the system and the O&M data required to support maintenance of this equipment by the using government agency. This analysis must be coordinated with the using government agency to determine maintenance parameters and O&M data that are available to the using government agency.

3-2.5.1 Identify O&M Data Requirements.

The design agency must identify O&M data requirements on an individual basis for all maintenance-significant equipment. Typical data requirements include the following items.

- Minimum spare parts list.
- Recommended spare parts list.
- Recommended onsite test equipment.
- Recommended O&M training.

3-2.5.2 Specify Functional Areas of Operating System.

The design agency must specify functional areas of the operating system and/or equipment where a technical representative will be furnished by the manufacturer for training, test, checkout, validation, or pre-operational exercises.

3-2.6 Verification.

A verification of O&M procedures and data manual content must be performed by the using government agency to demonstrate technical accuracy, fulfillment of intent, and

applicability to the performance of O&M within the facility. A review of the verification process may necessitate that additional information be obtained from the equipment manufacturer.

3-2.6.1 Verification Process.

Verification should begin during the equipment acceptance process and continue as the using government agency applies the instructions, data, and technical manuals to the continuous routines of equipment operation and repair.

3-2.6.2 Verification Support.

The design agency must support the user's verification process by:

- (1) Specifying acceptance test procedures which the contractor must be expected to fulfill during facility acceptance. The format should contain adequate sign-off routines to verify the performance of equipment in accordance with design specifications.
- (2) Requiring that, for specially designed equipment that does not fit well into a standard acceptance format, the contractor must submit an acceptance plan in lieu of the designer-specified acceptance test procedures.

CANCELLED

This Page Intentionally Left Blank

CHAPTER 4 ACCEPTABLE METHOD FOR EVALUATING SYSTEM RESILIENCE

4-1 ROBUSTNESS.

Robustness is defined as “the ability to absorb shocks and continue operating.” (North American Electric Reliability Corporation - NERC) For many critical facilities, there may be many mission assets which are considered uninterruptible. Since it is imperative to the mission that these assets remain on-line, any downtime or outage for such assets would be considered mission failure; the shock has not been absorbed. When evaluating missions for which any interruption is unacceptable, component failure or degradation should be considered as reducing the probability of mission success. Component failures or degradations should be considered as eliminating equipment redundancies or reducing individual component reliability. In these cases, it is appropriate to evaluate the performance of the system as the resulting operational availability for the mission. For example, if an event occurs which reduces the mission availability to 0.999, then the average expected weekly downtime of the mission is about 10 minutes. If a more resistant system is only reduced to an availability of 0.9999, the expected weekly downtime for the mission is approximately one minute. This essentially represents a 10-fold difference in system performance during the recovery period.

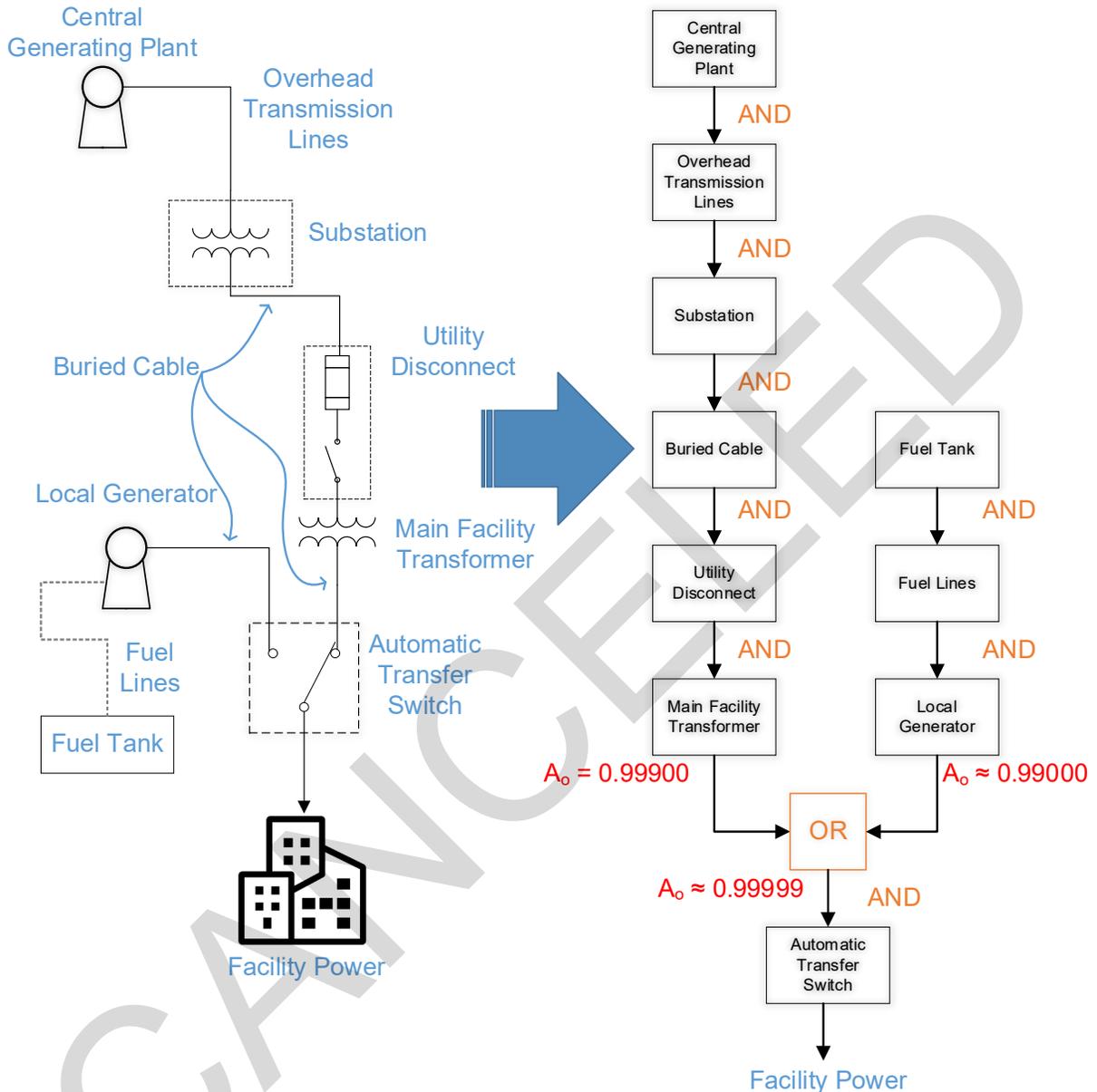
4-1.1 Evaluating Robustness.

As discussed, robustness may be quantified as a change in mission availability caused by the occurrence of a postulated event. Traditional reliability and availability analysis methods such as reliability block diagrams (RBDs), state-space modeling, or Monte Carlo simulations, may be used to evaluate mission availability during base-case and contingency operations. For the purposes of evaluating resilience, the following paragraphs will focus on the reliability RBD/Boolean algebra methodology.

4-1.1.1 Constructing an RBD.

Constructing a RBD requires translating the system topology into a set of discrete elements and logic gates. Items connected in series are typically combined with AND operators; parallel objects and strings are typically combined with OR operators. Depending on system configuration and redundancy parallel objects and strings may be combined using AND or OR operators. Each element in the block diagram has an associated availability statistic, which is derived from statistical data collected from similar components. Figure 4-1 shows an example of a typical utility system translated into an RBD. Note that combining redundant paths with an OR operator significantly increases the mission availability.

Figure 4-1 RBD for a Typical Distribution System



4-1.1.2 Contingency Event Data.

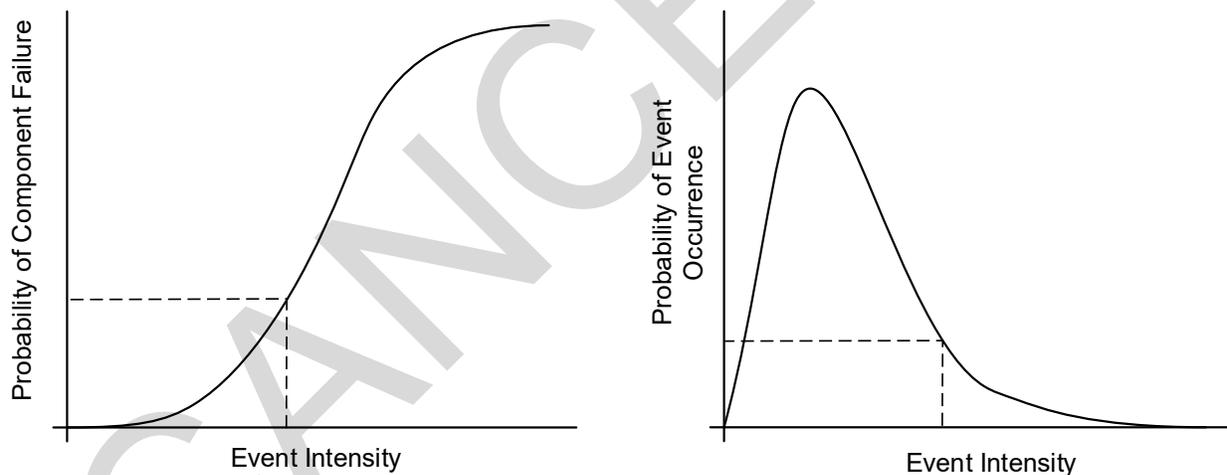
Incorporating contingency event data into availability modeling allows for a quantifiable difference in performance between base-case and contingency operations. There are two primary ways through which this is accomplished. The first, and most intuitive method, involves a deterministic approach, and is similar to traditional Failure Modes, Effects and Criticality Analysis (FMECA) analysis. This method assumes that an event of a certain magnitude has occurred and evaluates the effect that the event has on overall system availability. The following steps outline the deterministic method for Robustness evaluation:

4-1.1.2.1 Determine Events for which the Robustness of the System should be Assessed.

When applying the deterministic method, only a particular event or set of related events should be evaluated at a time. When selecting scenarios for evaluation, the probability and severity of the event should be considered. As a starting point, consider key components in the system where, as determined by baseline availability studies, failure is likely to significantly impact the performance of the system. Chapter 5 will discuss how to perform/create the baseline availability analysis.

In cases where reliable statistics exist to determine the probability that a particular event may occur, it is possible to select events based on the conditional probability of component failure given the occurrence of the event. In general, higher intensity events have a greater chance of causing component failure, but also occur less frequently. This can be seen in the two graphs in Figure 4-2. The graph on the left shows the fragility curve for a particular component; this shows the probability of component failure according to the intensity of an event. The graph on the right shows the probability density function (PDF) for a particular event based on event intensity.

Figure 4-2 Fragility Curves vs Event Probability



From these graphs, it can be seen that an event of a given intensity has a corresponding probability of causing component failure ($P(\text{failure})$), and an independent probability that it will occur ($P(\text{event})$). Combining these two probabilities in Equation 4-1 yields the conditional probability of failure given the occurrence of the event.

Equation 4-1. Conditional Probability of Failure Given Occurrence of the Event

$$P(\text{failure given event}) = \frac{P(\text{failure}) \cap P(\text{event})}{P(\text{event})}$$

Where:

P = probability

\cap = the probability that Events A and B both occur is the probability of the intersection of A and B. The probability of the intersection of Events A and B is denoted by $P(A \cap B)$. If Events A and B are mutually exclusive, $P(A \cap B) = 0$.

4-1.1.2.2 Conditional Probability of Failure.

The conditional probability of failure given event occurrence can be used to evaluate the relative risk associated with an event and determine whether further evaluation of that event is justified. For example, a site in Utah may not need to evaluate its response to a hurricane. If fragility data and event data indicate that event occurrence does not significantly increase the risk of component failure (such as the conditional probability of failure is within one order of magnitude of inherent failure rate), that scenario does not necessarily require further evaluation.

For other events, the severity of risk may be more subjective. For contingencies such as HEMP events, wildlife damage, cyber-attacks, or terrorist attacks, the probability of occurrence may be unknown or is subject to change. Consequently, a threshold value for conditional probability of failure may not exist, and a different means of event selection is warranted.

4-1.1.2.3 Determine what Components are likely to Fail as a Result of the Event.

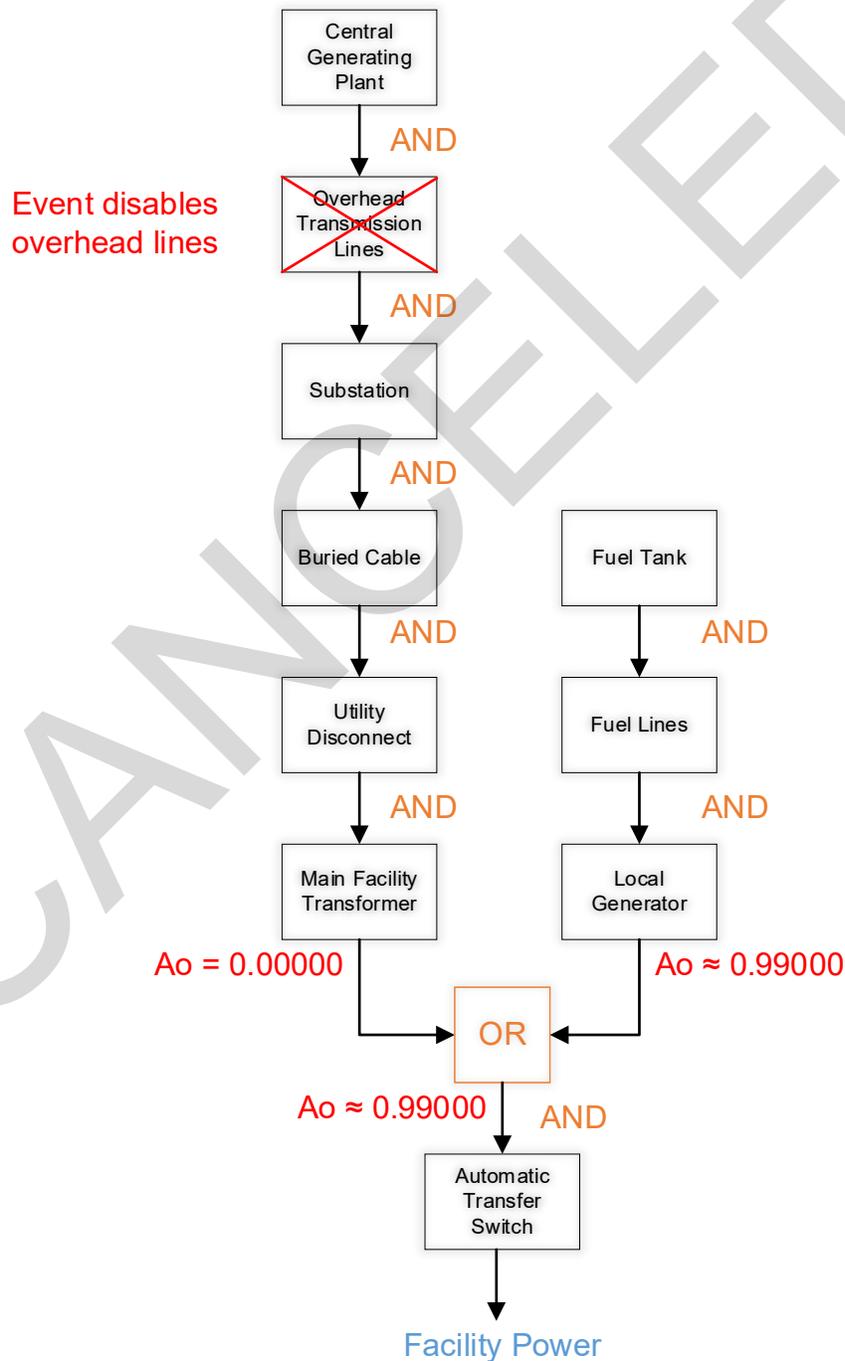
All components in a system are uniquely vulnerable to a set of events. For example, exterior generators may be vulnerable to flooding, whereas SCADA controlled switchgear may be more vulnerable to cyber-attacks. If fragility curves for individual components are available, then the probability of component failure associated with an event can be incorporated into the system availability model. Consider using an analysis tool such as HAZUS, as developed by the Federal Emergency Management Agency (FEMA), to assess the overall risk of component failure due to specific events. HAZUS is an example of a risk assessment tool that utilizes both fragility and event data in its analysis. Where event and fragility data are unavailable, it may be more practical to assume certain key components as having failed due to a postulated event. This deterministic approach clearly identifies single points of failure or areas that require additional hardening measures.

4-1.1.2.4 Analyze the Degraded System State.

As previously mentioned, functionality for critical missions that are considered uninterruptible must be maintained. In these cases, the change in system performance can be measured by the change in mission availability from the baseline state. In other words, a contingency event is considered to affect mission availability, not overall mission success. For example, in the postulated power system in Figure 4-3, a wind event disables only overhead transmission lines. Since backup power can be immediately supplied by emergency generators, mission loads can continue to operate. However, until the transmission lines are restored, the likelihood of failure is significantly increased.

Similar methods can be used to evaluate the degraded mission availability as for the baseline case (for example RBDs, Monte Carlo, state space). More information on each of these methods is provided in Chapter 5. To evaluate the degraded state, the input data used for the analysis must be modified to reflect the impact of the event being considered. The simplest method is to consider failed components as having an availability of zero. If equipment fragility curves are available, the resulting equipment reliability can be incorporated into the existing availability model.

Figure 4-3 Distribution System Model in Degraded State



4-2 RECOVERY.

Operations in the recovery phase have stabilized, and no further damage or degradation is expected. The system may be operating in alternate or emergency modes with a reduced availability. Power may be provided to critical systems via stand-by generators, alternate utility feeds, or distributed energy resources. In this phase, the emphasis is on restoring the system to its baseline operation.

4-2.1 Recovery Time.

As previously discussed, the shorter the recovery time, the more resilient the system. Recovery time is determined by the average length of time required to return damaged components to service. In general, the availability of the system increases as assets are recovered. For large or complex systems, availability during the recovery phase may change continuously. For smaller systems, or where fewer redundant paths exist, it can be more useful to consider the change in availability during the recovery phase as a step function. That is, there are discrete step changes in availability as components or success paths are returned to service.

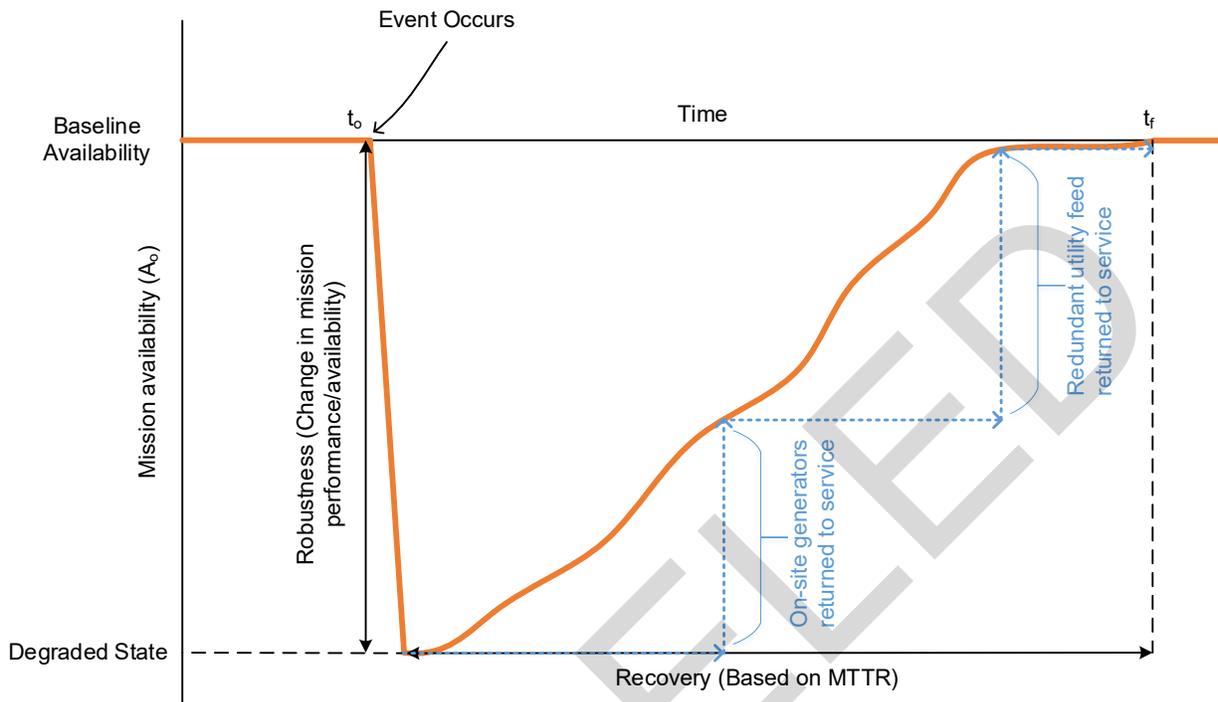
4-2.2 Stepped Recovery of Power System Assets.

Figure 4-4 provides an example of this concept. In this example, an event has disabled both the on-site generation as well as one of two redundant utility feeders. The on-site generators are quickly returned to service, resulting in a large step increase in availability. After some time, the redundant utility feed is returned to service, resulting in a second step increase in availability. It is important to note that for a single success path to be restored, all series components must be fully restored before improvements in availability are realized. For example, if an event disables a backup generator, its associated fuel tank and fuel lines, all these assets must be repaired before that feed is considered back on-line.

The step-change model in Figure 4-4 indicates the recovery time for the system can be approximated using the mean-time-to-repair (MTTR) for the various affected components. However, designers, planners, and facility managers must use caution when using MTTR to anticipate recovery time following a contingency event. MTTR data is typically based on failure modes that occur during normal operation. Contingency events may cause different failures to occur, and additional logistics delays must be considered based on the nature of the event and the location of the site. To determine the recovery time for a system, MTTR data should be used as an input to evaluate a disaster recovery plan.

Following a contingency event, the facility or site should have a plan in place to adapt to and recover quickly from its affects. Due to limitations of personnel, resources, and logistics, repairs for all components cannot occur simultaneously. It may also be required that some assets be restored in sequence. The following steps provide an outline for considerations when developing a recovery plan:

Figure 4-4 Stepped Recovery of Power System Assets



4-2.2.1 Identify the Components that are likely to have Failed.

This step may already have been completed as part of evaluating system robustness. Fragility curves and unique factors such as site geography are used to identify those components and success paths which may be inoperable following the event.

4-2.2.2 Evaluate Repair Priorities.

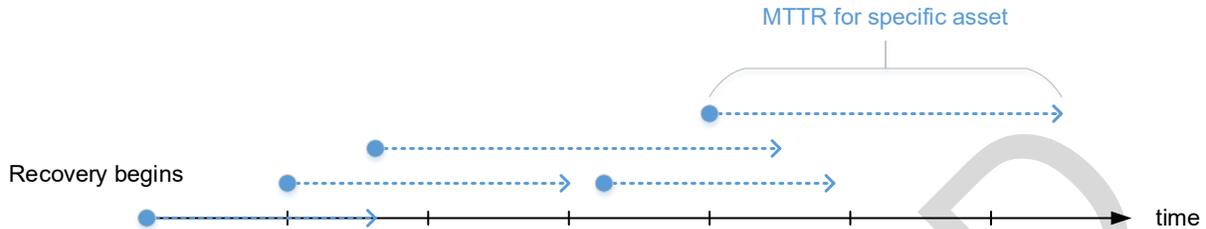
The RBD can be used to evaluate the effectiveness of individual repair activities based on what effect they have on mission availability and the time it takes to execute the repair. For example, when comparing two repair activities which have similar execution times, the activity which results in a larger improvement in mission availability should be prioritized. Typical MTTR values can be used as an input to evaluate the time requirements for each activity, but event-specific failure modes, and additional logistical delays should also be evaluated. In this step it is important to consider any repairs that, due to operational or resource limitations, may need to be executed in sequence.

4-2.2.3 Determine the Overall Time to Return to Baseline Operations.

Once the overall structure of the recovery plan is in place, the timeline for recovery should be evaluated. The result should be a site-specific, and event-specific number representing the required execution time for the planned series of repair activities. The result should be evaluated against operational limitations such as fuel reserves to determine whether the recovery time is adequate. Figure 4-5 shows an example of how the timeline for a typical recovery plan may look. Each arrow represents the repair time

for a specific asset. Note that individual repair events are staggered to optimize personnel and equipment resources throughout the recovery phase.

Figure 4-5 Sample Recovery Timeline



4-3 DETERMINING OPERATIONAL REQUIREMENTS FOR RESILIENCE METRICS.

Requirements for resilience metrics can vary from site to site and depend on a multitude of factors. As previously discussed, certain sites may want to prioritize either robustness or recovery depending on their specific needs.

4-3.1 Evaluate the Needs of the System.

To evaluate the needs of the system, it is important to apply a realistic time scale to the baseline and degraded availability states. Typically, availability is related to equipment downtime on a yearly scale; a “six-nines” system relates to about 30 seconds of downtime per year. However, contingency scenarios are more likely measured in weeks. Table 4-1 shows the corresponding weekly downtime for various levels of availability.

Table 4-1 Average Weekly Downtime Based on Availability

Availability	Average Weekly Downtime (Minutes)
0.9	1008
0.99	100.8
0.999	10.08
0.9999	1.008
0.99999	0.1008
0.999999	0.01008

4-3.2 Availability Requirements.

There are certain mission types with specific availability requirements. These requirements come from a memorandum from the Office of the Under Secretary of Defense dated 20 May 2021. The subject of the memorandum is Metrics and Standards for Energy Resilience at Military Installations. The availability requirement for the following mission types must be 99.999% or five-9’s:

- Operational Headquarters Facility
- Airfield and Supporting Infrastructure
- Harbor Facility Supporting Naval Vessels
- Munitions Production and Storage Facility
- Radar
- Space Launch Facility
- Operational Communications Facility that is determined to be a critical mission

The availability requirement for the following mission types must be 99.9999% or six-9's:

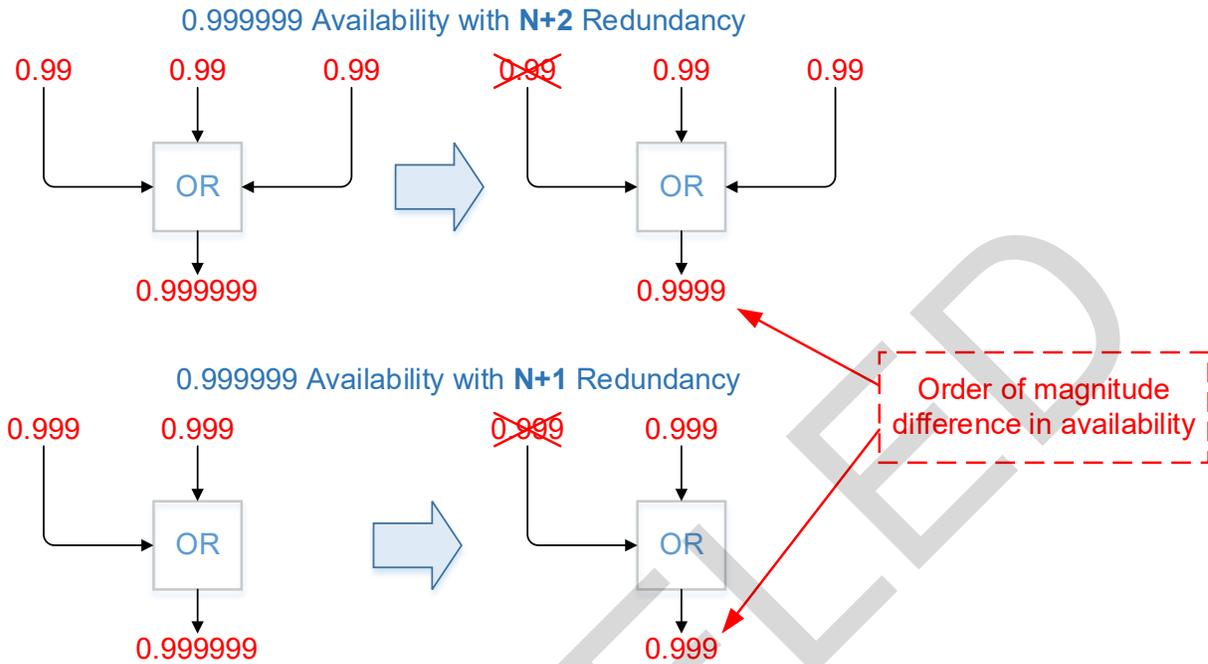
- Missile Field
- Ballistic Early Warning Radar
- Satellite Control Facility
- Cyber Operations Facility
- Biological Defense Facility that is determined to be a critical mission

A critical mission that does not fit these mission types is allowed to have an availability range from 99.9% (three-9's) to 99.9999% (six-9's) depending on the criticality of the mission.

4-3.3 Minimum Acceptable Level of Degraded State Availability.

When assessing the minimum acceptable level of degraded state availability, it is also important to consider the site-specific requirements for availability, as well as requirements for system topology. For example, a baseline availability requirement of six nines (0.999999) can be achieved using an N+2 redundant arrangement of three elements each with an availability of 0.99, or an N+1 redundant arrangement of two elements each with an availability of 0.999. If an event occurs which incapacitates only one feed, the N+2 system will have a degraded state availability a full order of magnitude higher than the N+1 system. Naturally, systems with a higher level of required redundancy should have more stringent requirements for resilience than those with less design redundancy. This is shown in Figure 4-6.

Figure 4-6 N+2 vs N+1 System Resilience



Site-specific requirements for resilience should also be decided by weighing several major factors. Ultimately, the required level of resilience is based on the level of mission criticality, the remoteness of the site, and whether the mission is duplicated and can be executed at any other sites.

4-3.3.1 Criticality.

Many DoD installations serve a range of critical missions. In a perfect world, designers would be able to protect all levels of critical missions from the effects of any possible event. However, due to funding and design constraints, some assets must be prioritized over others. Ultimately, the assets should be prioritized according to the DoD Mission-Based Critical Asset Identification Process (CAIP, DoD Inst 3020.45). To simplify the decision process for resilience planning, missions and supporting assets can also be categorized as having low, medium, or high criticality. Criticality in this context refers to the impact that incapacity or destruction of a mission would have on the physical or economic security or public health or safety.

This criticality level can be assigned based on national priorities, or within the scope of a local project. For example, when considering resilience improvements for only a single installation or facility, it may be useful to consider the low-medium-high scale as spanning the range of criticality present at that installation. In many cases, specific details related to the level of criticality of a mission may be classified.

4-3.3.2 Remoteness.

Critical facilities and other critical assets exist in a variety of locations. This can have a significant effect on recovery of a mission following an extreme event. Remoteness is

primarily related to the geographical location of a facility or installation but can be further influenced by other accessibility factors. Topographic features such as bodies of water or mountainous terrain, as well as the number and condition of access roads can also impact the remoteness of a site. For example, if a site can only be accessed via a single bridge, it would be considered as more remote than a similar site with several access points.

Like the level of criticality, the remoteness of a site can be categorized in relative terms. For the purposes of resilience planning, sites should be considered to have low, medium, or high remoteness. Typically, more remote sites should prioritize the robustness phase of resilience as recovery may be limited by physical constraints. This maximizes overall resilience by prioritizing the ride-through ability for these missions.

4-3.3.3 Duplicated Missions.

Some missions can be carried out at geographically diverse sites such that a contingency event at one is unlikely to affect mission success at any of the other sites. This creates additional mission redundancy and can reduce resilience requirements at an individual site. It is important to evaluate the practical considerations in mission duplication; several questions must be answered. Will the mission be transferred to an alternate site automatically? Will personnel be available at the alternate site to process the mission? Can the mission be transferred in anticipation of a foreseen event? In the interest of simplicity, the ability of a mission to be carried out at alternate sites should be considered as a simple yes or no.

Once these three factors have been evaluated, the results can be used to determine the requirement categories for both Robustness and Recovery. As previously discussed, these two aspects of resilience should be considered independently due to the unique needs of individual sites. Using Table 4-2 below, the three factors can be applied to place a mission or asset in prioritized categories for both Robustness and Recovery. The result is a low-medium-high index for each resilience phase. For example, a mission with medium criticality, high remoteness, and no mission duplication would have a High Robustness requirement and a Medium recovery requirement.

Table 4-2 is designed to provide a simple framework to assign independent requirements for both robustness and recovery. This should be used as a tool to determine the relative need for prioritizing either phase of the system response to a given event. In some cases, a single facility may have different required levels of robustness and recovery.

Table 4-2 Determine Resilience Requirements

		Resilience Phase	
		Robustness	Recovery
Resilience Metric Requirement	Low	Criticality: Low-Med Remoteness: Low Duplicated Missions: Yes	Criticality: Low Remoteness: Low-Med Duplicated Missions: Yes
	Medium	Criticality: Low-Med-High Remoteness: Med Duplicated Missions: Yes	Criticality: Low-Med Remoteness: Low-Med-High Duplicated Missions: No
	High	Criticality: Med-High Remoteness: Med-High Duplicated Missions: No	Criticality: High Remoteness: Low-Med-High Duplicated Missions: No

CANCELLED

CHAPTER 5 RELIABILITY/AVAILABILITY

5-1 BASIC RELIABILITY AND AVAILABILITY CONCEPTS.

5-1.1 Probability and Statistics

This chapter provides the reader with an overview of the mathematics of reliability theory. It is not presented as a complete (or mathematically rigorous) discussion of probability theory and statistics but should give the reader a reasonable understanding of how reliability is calculated. Before beginning the discussion, a key point must be made. Reliability is a design characteristic that indicates a system's ability to perform its mission over time without failure or without logistics support. In the first case, a failure can be defined as any incident that prevents the mission from being accomplished; in the second case, a failure is any incident requiring unscheduled maintenance. Reliability is achieved through sound design, the proper application of parts, and an understanding of failure mechanisms. Estimation and calculation techniques are necessary to help determine feasibility, assess progress, and provide failure probabilities and frequencies to determine spare part requirements and other analyses.

5-1.1.1 Uncertainty.

Uncertainty - at the heart of probability. The mathematics of reliability is based on probability theory. Probability theory, in turn, deals with uncertainty. The theory of probability had its origins in gambling.

(1) Simple examples of probability in gambling are the odds against rolling a six on a die, of drawing a deuce from a deck of 52 cards, or of having a tossed coin come up heads. In each case, probability can be thought of as the relative frequency with which an event will occur in the long run.

(a) Tossing an honest coin will result in heads (or tails) 50% of the time, this does not mean it will necessarily toss five heads in ten trials. It only means that in the long run, it is expected to be 50% heads and 50% tails. Another way to look at this example is to imagine a very large number of coins being tossed simultaneously; again, it is expected to be 50% heads and 50% tails.

(b) Rolling an honest die, it is expected the chance of rolling any possible outcome (one, two, three, four, five, or six) is one in six. It is possible to roll a given number, say a six, several times in a row. However, in a large number of rolls, it is expected to roll a six (or a one, or a two, or a three, or a four, or a five) only $1/6$ or 16.7% of the time.

(c) Drawing from an honest deck of 52 cards, the chance of drawing a specific card (an ace, for example) is not as easily calculated as rolling a six with a die or tossing a heads with a coin. First it must be recognized that there are four suits, each with a deuce through ace (ace being high). Therefore, there are four deuces, four tens, four kings, etc. So the chance of drawing any ace is four in 52 since there are only four aces. It is instinctively known that the chance of drawing the ace of spades, for example, is less than four in 52. Indeed, it is one in 52 (only one ace of spades in a deck of 52 cards).

(2) Why is there a 50% chance of tossing a head on a given toss of a coin? It is because there are two results, or events, which can occur (assume that it is very unlikely for the coin to land on its edge) and for a balanced, honest coin, there is no reason for either event to be favored. Thus, the outcome is random, and each event is equally likely to occur. Hence, the probability of tossing a head (or tail) is one of two equally probable events occurring = $1/2 = 0.5 = 50\%$ of the time. On the other hand, one of six equally probable events can result from rolling a die: it can be a one, two, three, four, five, or six. The result of any roll of a die (or of a toss of a coin) is called a discrete random variable. The probability that on any roll this random variable will assume a certain value, call it x , can be written as a function, $f(x)$. The probabilities of $f(x)$, specified for all values of x , are referred to as the values of probability function of x . For the die and coin, the function is constant. For the coin, the function is $f(x) = 0.5$, where x is either a head or tail. For the die, $f(x) = 1/6$, where x can be any of the six values on a die.

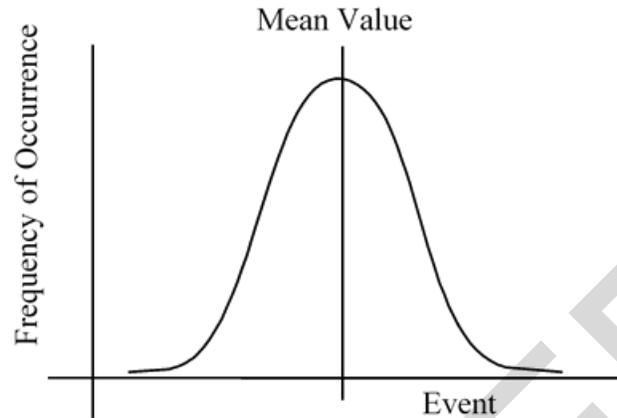
5-1.1.2 Probability Functions.

All random events have either an underlying probability function (for discrete random variables) or an underlying PDF (for a continuous random variable).

(1) The results of a toss of a coin or roll of a die are discrete random variables because only a finite number of outcomes are possible; hence these events have an underlying probability function. When the probability of each event is equal, underlying probability function is said to be uniform.

(2) The number of possible heights for American males is infinite (between 5 feet – 8 inches (1.72 meters) and 6 feet (1.83 meters), for example, there are an infinite number of possible heights) and is an example of a continuous random variable. The familiar bell-shaped curve describes most natural events, such as the height of a person, intelligence quotient of a person, errors of measurement, etc. The underlying PDF represented by the bell-shaped curve is called normal or Gaussian. Figure 5-1 shows a typical normal distribution. Note that the event corresponding to the midpoint of the curve is called the mean value. The mean value, also called the expected value, is an important property of a distribution. It is like an average and can be compared with the center of mass of an object. For the normal distribution, half the events lie below the mean value and half above. Thus, if the mean height of a sample of 100 Americans is 5 feet -9 inches (1.75 meters), it is expected that half the sample would be less than 69 inches (1.75 meters) tall, and half would be taller. It is also expected that most people would be close to the average with only a few at the extremes (very short or very tall). In other words, the probability of a certain height decreases at each extreme and is “weighted” toward the center, hence, the shape of the curve for the normal distribution is bell-shaped.

Figure 5-1 Typical Normal Distribution Curve



(3) The probability of an event can be absolutely certain (the probability of tossing either a head or a tail with an honest coin), absolutely impossible (the probability of throwing a seven with one die), or somewhere in between. Thus, a probability always can be described with Equation 5-1.

Equation 5-1. Probability of an Event

$$0 \leq P \leq 1$$

Where:

P = probability of an event

(4) Determining which distribution best describes the pattern of failures for an item is extremely important, since the choice of distributions greatly affects the calculated value of reliability. Two of the continuous distributions commonly used in reliability are shown in Table 5-1. Note that $f(t)$ is called the probability density function (PDF). Reliability is usually concerned with the probability of an unwelcome event (failure) occurring.

Table 5-1 Commonly Used Continuous Distributions

Distribution	Probability Density Function	Most Applicable to
Exponential	$f(t) = \lambda e^{-\lambda t}$	Electronic parts and complex systems
Weibull (2-parameter)	$f(t) = \frac{\beta}{\eta} \left(\frac{t}{\eta}\right)^{\beta-1} e^{-\left(\frac{t}{\eta}\right)^\beta}$	Mechanical Parts

Where:

$f(t)$ = probability density function

η = scale

e = the base of natural logarithms

λ = the failure rate (inverse of MTBF)

t = time (hours)

Where:

$f(t)$ = probability density function

β = shape parameter/Weibull slope

η = scale

t = time (hours)

e = the base of natural logarithms

(a) The underlying statistical distribution of the time to failure for parts is often assumed to be exponential. A glance at the equation of the PDF explains why. It is easy to work with and has a constant mean, λ . Rather than assuming a distribution, one should determine the most appropriate one using various techniques for analyzing time-to-failure data.

(b) When the exponential distribution is applicable, the rate at which failures occur is constant and equal to λ . For other distributions, the rate at which failures occur varies with time. For these distributions, a Hazard Function is used, which is a function that describes how the rate of failures varies over time.

(c) Note that different types of parts (such as, items that fail once and then are discarded and replaced with a new item) may have different underlying statistical distributions of the time to failure. The times to failure of electronic parts, for example, often follow the exponential distribution. The times to failure for mechanical parts, such as gears and bearings, often follow the Weibull distribution. Of course, the parameters for the Weibull for a gear will most likely be different from the parameters for a ball bearing. The applicability of a given distribution to a given part type and the parameters of that distribution are determined, in part, by the modes of failure for the part.

(d) By their very nature, systems consist of many, sometimes thousands, of parts. Since systems, unlike parts, are repairable, they may have some parts that are very old, some that are new, and many with ages in between these extremes. In addition, each part type will have a specific distribution of times to failure associated with it. The consequence of these part characteristics together within a system is that systems tend to exhibit a constant failure rate. That is, the underlying statistical distribution of the time to failure for most systems is exponential. This consequence is extremely significant because many reliability prediction models, statistical demonstration tests, and other system analysis are predicated on the exponential distribution.

5-1.1.3 Determining Failure Rate or Hazard Function.

How is the failure rate (or Hazard Function) of a specific system or component determined? Two methods are used.

(1) In the first method, use failure data for a comparable system or component already in use. This method assumes that the system in use is comparable to the new system and that the principle of transferability applies - this principle states that failure data from one system can be used to predict the reliability of a comparable system.

(2) The other method of determining failure rate or the Hazard Function is through testing of the system or its components. Although, theoretically, this method should be the "best" one, it has two disadvantages. First, predictions are needed long before prototypes or pre-production versions of the system are available for testing. Second, the reliability of some components is so high that the cost of testing to measure the reliability in a statistically valid manner would be prohibitive. Usually, failure data from comparable systems are used in the early development phases of a new system and supplemented with test data when available.

5-1.2 Calculating Reliability.

If the time (t) over which a system must operate and the underlying distributions of failures for its constituent elements are known, then the system reliability can be calculated by taking the integral (essentially the area under the curve defined by the PDF) of the PDF from t to infinity, as shown in Equation 5-2.

Equation 5-2. Reliability

$$R(t) = \int_t^{\infty} f(t) dt$$

Where:

$R(t)$ = reliability over time t

t = time (hours)

$f(t)$ = probability density function

dt = downtime (hours)

5-1.2.1 Exponential Distribution.

If the underlying failure distribution is exponential, Equation 5-2 becomes Equation 5-3.

Equation 5-3. Exponential Distribution

$$R(t) = e^{-\lambda t}$$

Where:

λ = the failure rate (inverse of MTBF)

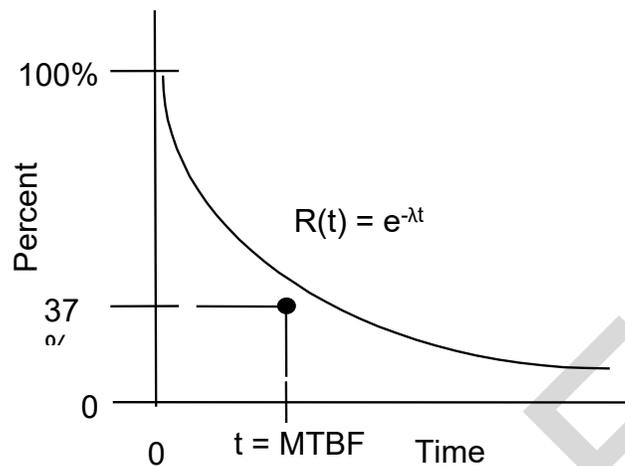
t = the length of time the system must function

e = the base of natural logarithms

$R(t)$ = reliability over time t

(1) Figure 5-2 shows the curve of Equation 5-3. The mean is not the "50-50" point, as was true for the normal distribution. Instead, it is approximately the 37-63 point. In other words, if the mean time between failures of a type of equipment is 100 hours, it is expected that only 37% (if $t = \text{MTBF} = 1/\lambda$, then $e^{-\lambda t} = e^{-1} = 0.367879$) of the population of equipment to still be operating after 100 hours of operation. Put another way, when the time of operation equals the MTBF, the reliability is 37%.

Figure 5-2 Exponential Curve Relating Reliability and Time

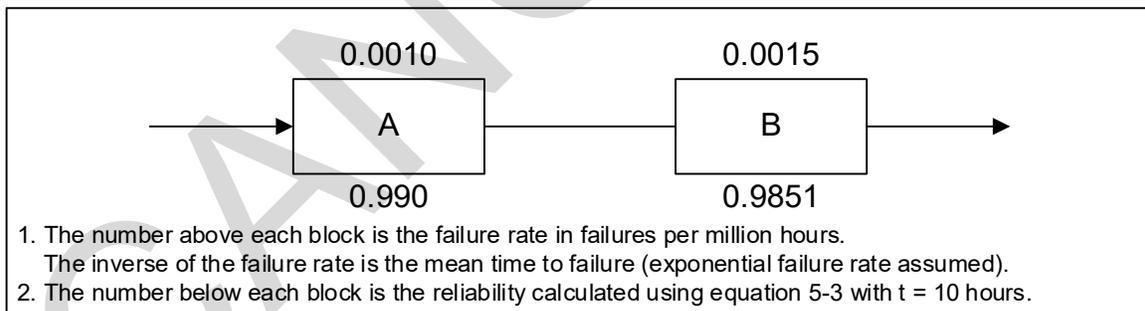


(2) If the underlying distribution for each element is exponential and the failure rates (λ_i) for each element are known, then the reliability of the system can be calculated using Equation 5-3.

5-1.2.2 Series Reliability.

Consider the system represented by the RBD in Figure 5-3.

Figure 5-3 Example RBD



(1) Components A and B in Figure 5-3 are said to be in series, which means all must operate for the system to operate. Since the system can be no more reliable than the least reliable component, this configuration is often referred to as the weakest link configuration.

(2) Since the components are in series, the system reliability can be found by adding together the failure rates of the components and substituting the result as seen in Equation 5-4. Furthermore, if the individual reliabilities are calculated (the bottom values,) the system reliability can be found by multiplying the reliabilities of the two components as shown in Equation 5-5.

Equation 5-4. System Reliability

$$R(t) = e^{-(\lambda_A + \lambda_B)t} = e^{-0.0025 \times 10} = 0.9753$$

Where:

$R(t)$ = system reliability

λ = the failure rate (inverse of MTBF)

t = the length of time the system must function

e = the base of natural logarithms

Equation 5-5. System Reliability

$$R(t) = R_A(t) \times R_B(t) = 0.99000 \times 0.98510 = 0.9753$$

Where:

$R(t)$ = system reliability

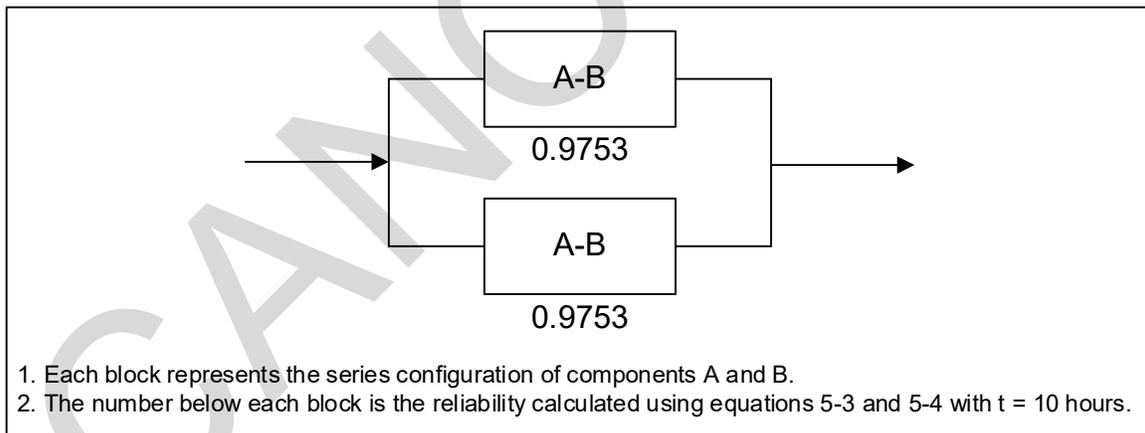
$R_A(t)$ = system A reliability

$R_B(t)$ = system B reliability

5-1.2.3 Reliability with Redundancy.

Now consider the RBD shown in Figure 5-4.

Figure 5-4 RBD of a System with Redundant Components



(1) The system represented by the RBD in Figure 5-4 has the same components (A and B in series denoted by one block labeled: A-B) used in Figure 5-3, but two of each component are used in a configuration referred to as redundant or parallel. Two paths of operation are possible. The paths are top A-B and bottom A-B. If either of two paths is intact, the system can operate. The reliability of the system is most easily calculated by (Equation 5-6) finding the probability of failure ($1 - R(t)$) for each path, multiplying the probabilities of failure (which gives the probability of both paths failing), and then subtracting the result from 1. The reliability of each path was found in the previous example. Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is $1 - 0.9753 = 0.0247$. The probability that

both paths will fail is $0.0247 \times 0.0247 = 0.0006$. Finally, the reliability of the system is $1 - 0.0006 = 0.9994$, about a 2.5% improvement over the series configured system.

Equation 5-6. System Reliability of Figure 5-4

$$R(t) = 1 - (1 - R_T(t)) \times (1 - R_B(t)) = 1 - (0.0274 \times 0.0274) = 0.9994$$

Where:

$R(t)$ = system reliability

R_T = the reliability of the top path

R_B = the reliability of the bottom path

(2) Two components in parallel may always be on and in operation (active redundancy) or one may be off (standby redundancy). In the latter case, failure of the primary component must be sensed to indicate that the standby module should be activated. Standby redundancy may be necessary to avoid interference between the redundant components. If the redundant component is normally off, reduces the time over which the redundant component will be used (it's only used from the time when the primary component fails). Of course, more than two components can be in parallel. Paragraph 5-2.4.1 discusses the various types of redundancy and how they can be used to improve the availability of current C5ISR facilities.

(3) Adding a component in parallel, such as, redundancy, improves the system's ability to perform its function. This aspect of reliability is called functional or mission reliability. Note, however, that in Figure 5-4 another set of components with its own failure rate has been added. To calculate the total failure rate for all components, they are added together. The result is 5000 failures per million operating hours (0.005000). The failure rate for the series-configured system in Figure 5-3 was 2500 failures per million operating hours. Although the functional reliability of the system improved, the total failure rate for all components increased. This perspective of reliability is called basic or logistics reliability. When standby redundancy is used, the sensing and switching components add to the total failure rate.

5-1.2.4 Logistics Reliability.

Whereas functional reliability only considers failures of the function(s), logistics reliability considers all failures because some maintenance action will be required. Logistics reliability can be considered as either the lack of demand placed on the logistics system by failures or the ability to operate without logistics. If standby redundancy is used with the redundant component not on, the apparent failure rate of the standby component will be less than that of its counterpart (it will likely operate less than ten hours), but the failure rate of the switching circuits must now be considered.

5-1.3 Calculating Availability.

For a system such as an electrical power system, availability is a key measure of performance. An electrical power facility must operate for very long periods of time, providing power to systems that perform critical functions, such as C5ISR. Even with the

best technology and most robust design, it is economically impractical, if not technically impossible, to design power facilities that never fail over weeks or months of operation. Although forced outages are never welcome and power facilities are designed to minimize the number of forced outages, they still occur. When they do, restoring the system to operation as quickly and economically as possible is paramount. The maintainability characteristics of the system predict how quickly and economically system operation can be restored.

5-1.3.1 Reliability, Availability, and Maintenance.

Reliability and maintainability (R&M) are considered complementary characteristics. Looking at a graph of constant curves of inherent availability (A_i), one can see this complementary relationship. A_i is defined by Equation 5-7 and reflects the percent of time a system would be available if delays due to maintenance, supply, etc. are ignored.

Equation 5-7. Inherent Availability

$$A_i = \frac{MTBF}{MTBF + MTTR} \times 100\%$$

Where:

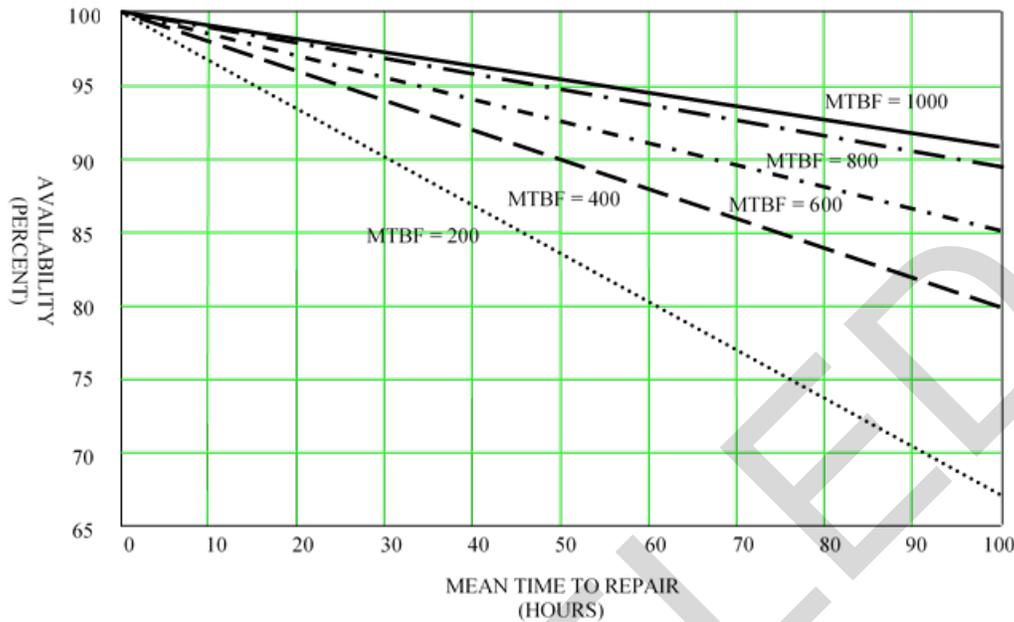
A_i = *inherent availability*

$MTBF$ = *mean time between failure*

$MTTR$ = *mean time to repair*

As seen in Equation 5-7, if the system never failed, the $MTBF$ would be infinite, and A_i would be 100%. Or, if it took no time at all to repair the system, $MTTR$ would be zero and again the availability would be 100%. Figure 5-5 is a graph showing availability as a function of reliability and maintainability (reliability is calculated using Equation 5-6). Note that the same availability with different values of R&M can be achieved. With higher reliability ($MTBF$), lower levels of maintainability are needed to achieve the same availability and vice versa. It is very common to limit $MTBF$, $MTTR$, or both. For example, the availability requirement might be 95% with an $MTBF$ of at least 600 hours and a $MTTR$ of no more than 3.5 hours.

Figure 5-5 Different Combinations of MTBF and MTTR Yield Same Availability



5-1.3.2 Other Measures of Availability

Availability is calculated through data collection by two primary methods:

(1) Operational availability includes maintenance and logistics delays and is defined using Equation 5-8:

Equation 5-8. Operational Availability

$$A_o = \frac{MTBM}{MTBM + MDT}$$

Where:

A_o = operational availability

MTBM = mean time between all maintenance

MDT = mean downtime for each maintenance action

(2) Availability is also a function of raw uptime and downtime as seen in Equation 5-9:

Equation 5-9. Availability

$$A = \frac{Uptime}{Uptime + Downtime}$$

Where:

A = availability

where uptime is the time during which the system is available for use and downtime is the time during which the system is not available for use. Given that the sum of uptime

and downtime is equal to the total system run time, this calculation is simply a ratio, indicating the percentage of the time that the system is up (or available).

(3) Note that A_o and A_i are probabilistic measures, while A is a deterministic measure. MTBF, MTBM, MTTR, and MDT are measures of reliability and maintainability (R&M). By designing for appropriate levels of R&M and ensuring statistically appropriate calculations, a high confidence in the availability can be obtained. However, that confidence can never be 100%. Measuring A is done by measuring the amount of uptime in a given total time and then calculating the observed availability using Equation 5-9. For this measure of availability, the time interval for the measurement is extremely important. Its importance can be understood by considering an availability requirement of 95% with a maximum downtime of ten hours. Table 5-2 shows the effect of varying intervals of time for measuring A .

Table 5-2 Effect of Measurement Interval on Observed Availability

Total Time	Actual Downtime	Actual Uptime	Measured Availability	Maximum Downtime to Meet Requirement (Using Equation 5-9)
1 hours	0.5 hours	0.5 hour	50%	0.05 hours (3 minutes)
8 hours	1 hour	7 hours	87.5%	0.4 (24 minutes)
24 hours	2 hours	22 hours	91.67%	1.2 hours
240 hours	10 hours	230 hours	95.83%	10 hours
7200 hours	10 hours	7190 hours	99.86%	10 hours

(a) Very short intervals make it increasingly difficult, if not impossible, to meet an availability requirement. It is very possible that a failure could occur in the first hour of operation. If that were the case, the system would pass the 95% availability test only if the repair could be made in 3 minutes or less. For many systems, it may be impossible to correct any failure in three minutes or less. So even if it is unlikely that a failure will occur in the first hour of operation (such as, the system is highly reliable), the probability of such a failure is not zero. If a failure occurs in the first hour and requires more than three minutes to repair, the system will have failed to meet an availability requirement of 95%. Yet, if the system is truly reliable, it may experience no more failures (and no more downtime) in the next 24 hours of operation, in which case the measured availability will be greater than the requirement.

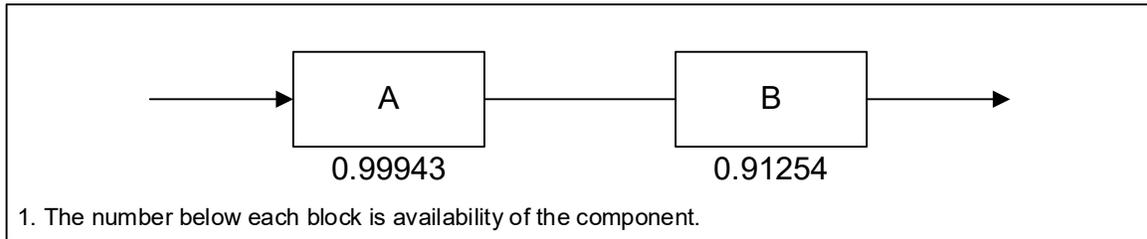
(b) Since A_o , A_i , and A are not measured in the same way, it is extremely important in contractual form to state clearly (for example, in a step-by-step, deductive manner) how availability will be measured during acceptance or qualification testing.

5-1.3.3 Calculating Simple System Availabilities.

Calculating simple system availability measures is similar to the reliability calculations in paragraphs 5.1-2.2 and 5.1-2.3.

(1) For series availability, consider the system represented by the block diagram in Figure 5-6.

Figure 5-6 Example Availability Block Diagram



(a) Since the components are in series, the system availability can be found by multiplying the availabilities of the two components as shown in Equation 5-10.

Equation 5-10. Series Availability

$$\text{Series Availability} = A_A \times A_B = 0.99943 \times 0.91254 = 0.91202$$

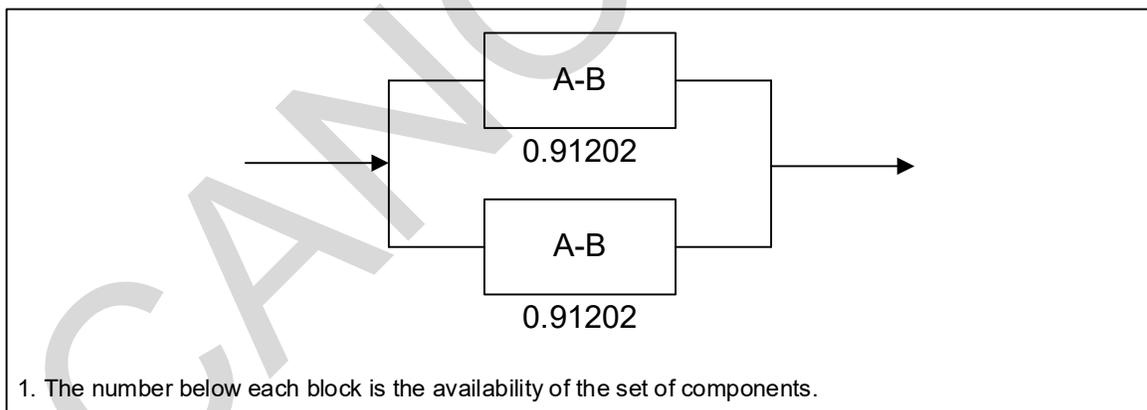
Where:

A_A = component A availability

A_B = component B availability

(2) For parallel availability, consider the system represented by the block diagram in Figure 5-7.

Figure 5-7 Availability Block Diagram of a System with Redundant Components



(a) Since the components are parallel, the system availability can be found as shown in Equation 5-11.

Equation 5-11. Parallel Availability

$$\text{Parallel Availability} = 1 - (1 - A_T) \times (1 - A_B)$$

$$\text{Parallel Availability} = 1 - (0.08798) \times (0.08798)$$

$$\text{Parallel Availability} = 0.99226$$

Where:

A_T = the availability of the top path

A_B = the availability of the bottom path

5-1.4 Predictions and Assessments.

Predictions and assessments refer to the process of evaluating the RAM calculations, system weaknesses, and areas offering opportunities for improvement. Quantitative numbers are a usual byproduct of a prediction or assessment. Such numbers are necessary for calculating spares requirements, probability of success, and other purposes.

5-1.4.1 Reliability Predictions.

In a new development program, reliability predictions are a means of determining the feasibility of requirements, assessing progress toward achieving those requirements, and comparing the reliability impact of design alternatives. Predictions can be made through any appropriate combination of reliability models, historical data, test data, and engineering judgment. The choice of which prediction method to use depends on the availability of information. That choice can also be a function of the point of the system life cycle at which the prediction is performed. Considerations in performing predictions include that correct environmental stresses are used, the reliability model is correct, the correct part qualities are assumed, and that all operational and dormancy modes are reflected.

5-1.4.2 Reliability Assessments.

Predictions are one method of assessing the reliability of an item. At the onset of a new development program, the prediction is usually purely analytical. As the program progresses, other methods become available to improve or augment the analytical prediction. These methods include testing, design reviews, and others. For existing systems, reliability assessments include analyzing field data to determine the level of reliability being achieved and identify weaknesses in the design and opportunities for improvement.

5-1.4.2.1 Common Techniques.

Table 5-3 lists some common techniques that can be used for assessing reliability and guidance for their use. Some of these methods provide a numerical value that is representative of the system reliability at a point in time; all provide a valuable means of better understanding the design's strengths and weaknesses so that it can be changed accordingly.

5-1.4.2.2 Assessment Methods.

The assessment methods chosen should be appropriate for the system and require only a reasonable level of investment given the value of the results. The failure of some components, for example, may have little impact on either system function, or on its operating and repair costs. A relatively costly analysis may not be justified. For other

systems, a thermal analysis may not be needed, given the nature of the system and its operating environment. When the consequences of failure are catastrophic, every possible effort should be made to make the system fail-safe or fault tolerant.

Table 5-3 Methods for Assessing Reliability

Method	Application
Accelerated Life Testing	Effective on parts, components, or assemblies to identify failure mechanisms and life limiting critical components.
Critical Item Control	Apply when safety margins, process procedures and new technology present risk to the production of the system.
Design of Experiments (DOE)	Use when process physical properties are known, and parameter interactions are understood. Usually done in early design phases, it can assess the progress made in improving system or process reliability.
Design Reviews	Continuing evaluation process to ensure details are not overlooked. Should include hardware and software.
Dormancy Analysis	Use for products that have "extended" periods of non-operating time or unusual non-operating environmental conditions or high cycle on and off periods.
Durability Analysis	Use to determine cycles to failure or determine wear out characteristics. Especially important for mechanical products.
Failure Modes, Effects and Criticality Analysis (FMECA)	Applicable to equipment performing critical functions (for example control systems) when the need-to-know consequences of lower-level failures is important
Failure Reporting Analysis and Corrective Action (FRACAS)	Use when iterative tests or demonstrations are conducted on breadboard, or prototype products to identify mechanisms and trends for corrective action. Use for existing systems to monitor performance.
Failure Tree Analysis (FTA)	Use for complex systems evaluations of safety and system reliability. Apply when the need to know what caused a hypothesized catastrophic event is important.
Finite Element Analysis (FEA)	Use for designs that are unproven with little prior experience/test data, use advanced/unique packaging/design concepts, or will encounter severe environmental loads.
Life Cycle Planning	Use if life limiting materials, parts or components are identified and not controlled.
Parts Obsolescence	Use to determine need for and risks of application of specific parts and lifetime buys.
Prediction	Use as a general means to develop goals, choose design approaches, select components, and evaluate stresses. Equally useful when redesigning or adding redundancy to an existing system.
Reliability Growth Test (RGT)/Test Analyze and Fix (TAAF)	Use when technology or risk of failure is critical to the success of the system. These tests are costly in comparison to alternative analytical techniques.
Sneak Circuit Analysis (SCA)	Apply to operating and safety critical functions. Important for space systems and others of extreme complexity. May be costly to apply.
Supplier Control	Apply when high volume or new technologies for parts, materials or components are expected.
Test Strategy	Use when critical technologies result in high risk of failure
Thermal Analysis (TA)	Use for products with high power dissipation, or thermally sensitive aspects of design. Typical for modern electronics, especially of densely packages products.
Worst Case Circuit Analysis (WCCA)	Use when the need exists to determine critical component parameters variation and environmental effects on circuit performance.

5-2 IMPROVING AVAILABILITY.

5-2.1 Overview of the Process.

Facility managers are faced with the responsibility of providing the proper utilities (electrical, chilled water, steam, etc.) at the needed levels (power levels, voltage, pressure, etc.) to their customers when needed to support an end mission. The steps for improving the availability of new facilities in design and facilities already in use are shown in Table 5-4. The steps for each situation will be discussed in this chapter.

Table 5-4 The Process for Improving Facility Availability

New Facilities Being Designed	Facilities Already in Use
<ol style="list-style-type: none"> 1. Determine system availability requirements 2. Derive reliability and maintainability requirements from availability requirement 3. Develop one-line diagrams 4. Conduct analyses to predict availability, reliability, and maintainability and to determine weaknesses in design based on failure criteria and cost/benefit analysis 5. Conduct testing to validate analytical results 6. Update assessment of availability, reliability, and maintainability based on test results 7. Revise design as necessary based on test results 8. Construct facility and continuously assess performance and identify opportunities for improvement 9. Continuously assess performance and identify opportunities for improvement 	<ol style="list-style-type: none"> 1. Determine system availability requirements 2. Derive reliability and maintainability requirements from availability requirement 3. Develop one-line diagrams 4. Collect data for availability assessment 5. Assess availability, reliability, maintainability, and logistics performance being achieved for each system (this establishes the baseline performance) 6. Identify shortfalls (differences between required level of performance and baseline performance) 7. Perform cost-benefit analysis to prioritize improvement efforts 8. Design and develop system changes 9. Assess improvement in availability, reliability, and maintainability based on analyses and test 10. Implement design changes 11. Continuously assess performance and identify opportunities for improvement

5-2.2 New Facilities

Since reliability and maintainability, and hence availability, are predominantly affected by design, it is essential that these system characteristics be addressed in the design of a new system. It is during design, that these characteristics can be most effectively and positively influenced at the least cost.

5-2.2.1 Determine System Availability Requirements.

Establishing clear, comprehensive, and measurable requirements is the first and most important step in designing and developing systems. The design requirements must allow the user needs to be met. User needs are often stated in non-design terms. For facilities, these might include operational availability, readiness, mean time between maintenance (where maintenance includes all maintenance actions, including those to

repair operator-induced failures), and total downtime (including the time to order and ship parts if necessary). Designers must have requirements that they can control. For a facility, these may include inherent availability, mean time between design failures, and mean time to repair (includes only the actual "hands on" time to make a repair). The facility availability requirement should be included in the specifications for a new facility.

5-2.2.2 Derive Reliability and Maintainability Requirements from Availability Requirement.

Based on the user need (for example, operational availability), the reliability and maintainability design requirements (for example, mean time between failure and mean time to repair) must be derived. This derivation of lower-level requirements is usually done by the design organization and continues throughout the development effort until design requirements are available at the lowest level of indenture (subsystem, assembly, subassembly, part) that makes sense.

5-2.2.3 Develop One-line Diagrams.

One-line diagrams will be instrumental in the creation of all models concerning RAM criteria and analysis. It is critical that diagrams are accurate and up to date. Paragraph 5.3-5 of this UFC demonstrates how one-line diagrams are used in modeling and calculation.

5-2.2.4 Conduct Analyses.

Conduct analyses to predict availability, reliability, and maintainability and to determine weaknesses in design and redesign based on failure criteria and cost/benefit analysis. Some of the pertinent analyses are summarized in Table 5-5.

5-2.2.5 Conduct Testing to Validate Analytical Results.

No matter how diligently the models are developed, and the analytical tools are used, all variations and factors cannot be accounted for. By testing a given design, unexpected problems will be uncovered. These problems can include new types of failures, more frequent than expected failures, different effects of failures, and so forth. Problems discovered during test provide opportunities for improving the design and models and tools.

5-2.2.6 Update Assessment of Availability, Reliability, and Maintainability Based on Results.

Based on the results of testing, the analytical assessments of reliability made earlier should be updated. Adding the results of testing provides higher confidence in the assessment than is possible using analytical results alone.

Table 5-5 Analyses Helpful in Designing for Reliability

Analysis	Purpose	Applications	When to Perform
FEA	<ul style="list-style-type: none"> • Computer simulation technique for predicting material response or behavior of modeled device • Determine material stresses and temperature • Determine thermal and dynamic loading 	<ul style="list-style-type: none"> • Use for devices that: <ul style="list-style-type: none"> - Are unproven with little prior experience/data - Use advanced/unique packaging/design concepts - Will encounter severe environmental loads - Have critical thermal/mechanical constraints 	<ul style="list-style-type: none"> • In design phase when candidate devices can be selected using selection criteria
TA	<ul style="list-style-type: none"> • Calculate junction temperatures • Calculate thermal gradients • Calculate operating temperatures 	<ul style="list-style-type: none"> • For integrated circuits • For electronics and electrical devices 	<ul style="list-style-type: none"> • During circuit design • Prior to design of cooling systems
Dormancy Analysis	<ul style="list-style-type: none"> • Calculate failure rates of devices in dormancy or storage 	<ul style="list-style-type: none"> • Use for devices identified to have periods of dormancy 	<ul style="list-style-type: none"> • During design
FTA	<ul style="list-style-type: none"> • Top-down approach to identify effects of faults on system safety or reliability • Address multiple failure 	<ul style="list-style-type: none"> • Can be applied when FMECA too expensive • To address effects of multiple failures 	<ul style="list-style-type: none"> • Early in design phase, in lieu of FMECA
FMECA	<ul style="list-style-type: none"> • Bottom-up approach to identify single failure points and their effects • To assist in the efficient design of BIT and FIT • To establish and rank critical failures • To identify interface problems 	<ul style="list-style-type: none"> • More beneficial if performed on newly designed equipment • More applicable to equipment performing critical functions (for example, control systems) 	<ul style="list-style-type: none"> • Early in design phase
SCA	<ul style="list-style-type: none"> • To identify failures not caused by part failures • To reveal unexpected logic flows that can produce undesired results • To expose design oversights that create conditions of undesired operation 	<ul style="list-style-type: none"> • Mission and safety critical functions • Hardware with numerous interfaces • Systems with high testing complexities • Use selectively due to high testing complexities 	<ul style="list-style-type: none"> • Later in design stage but prior to CDR
WCCA	<ul style="list-style-type: none"> • To evaluate circuits for tolerance to “drift” • When time dependency is involved • To evaluate the simultaneous existence of all unfavorable tolerances • Single failures 	<ul style="list-style-type: none"> • Assesses combined effect of parts parameters variation and environmental effects on circuit performance <ul style="list-style-type: none"> • Not often applied • Use selectively 	<ul style="list-style-type: none"> • Later design stage as required

LEGEND: Finite Element Analysis (FEA); Thermal Analysis; Fault Tree Analysis (FTA); Failure Modes, Effects and Criticality Analysis (FMECA); Sneak Circuit Analysis (SCA); Worst Case Circuit Analysis (WCCA); Build-in-Test (BIT); Framework for Integrated Test (FIT); Critical Design Review (CDR)

5-2.2.7 Revise Design as Necessary Based on Test Results.

If the updated assessment indicates the design is falling short of the RAM requirements, the design must be revised to improve the reliability. Even when the updated assessment indicates the design is close to meeting the requirements, design changes should be considered referencing cost-benefit considerations.

5-2.2.8 Construct Facility and Continuously Assess Performance and Identify Opportunities for Improvement.

Once the RAM requirements are satisfied by the facility design, the facility is constructed. The inherent levels of reliability must be sustained over time. To that end, data needs to be collected continuously to assess the availability performance of the facility. This operational, field data should be archived for use in designing new facilities.

5-2.3 Existing Facilities.

For facilities in use, the process for improving availability is somewhat different than that discussed for new systems. It is different for two major reasons. First, improvements must be made by modifying an existing design, which is usually more difficult than creating the original design. Second, the improvements must be made with as little disruption to the facility as possible since it is supporting an ongoing mission. Although design changes are usually the primary focus of improvement efforts, changes in procedures or policy should also be considered. Not only are such changes usually much easier and economical to make, but they may also be more effective in increasing availability.

5-2.3.1 Determine System Availability Requirements.

As was the case for a new system, the requirements must be known. For existing facilities, it may be difficult to find the original user needs or design requirements. Even when the original requirements can be determined, the current requirements may have changed due to mission changes, budget constraints, or other factors.

5-2.3.2 Derive Reliability and Maintainability Requirements from the Availability Requirement.

After the system availability requirements are determined, it is necessary to translate them into reliability and maintainability requirements.

5-2.3.3 Develop One-line Diagrams.

This step can be bypassed if original one-lines are still current.

5-2.3.4 Collect Data for Availability Assessment.

Ideally, a data collection system was implemented when the facility was first put into operation. If that is not the case, one should be developed and implemented. The data to be collected includes the category of failures, causes of failures, date and time when failures occur, mechanisms affected, and so on. A substantial byproduct of an RCM program is the generation of such unique, facility data.

5-2.3.5 Assess Performance.

Assess the availability, reliability, maintainability, and logistics performance being achieved for each system. Performing this step establishes the baseline performance for the facility.

5-2.3.6 Identify Shortfalls.

Shortfalls are the differences between the required level of performance and baseline performance.

5-2.3.7 Performance Cost-Benefit Analysis to Prioritize Improvement Efforts.

Many potential improvements will be identified throughout the life of a facility. Those that are safety-related or are essential for mission success will always be given the highest priority. Others will be prioritized based on the costs to implement compared with the projected benefits. Those that have only a small return for the investment will be given the lowest priority.

5-2.3.8 Design and Develop System Changes.

The process for improving the availability, reliability, and maintainability performance of an existing facility is essentially the same as for designing new facility.

5-2.3.9 Assess Improvement.

Assess improvement in reliability, availability, and maintainability based on analyses and tests. Before implementing any potential improvements, some effort must be made to ensure that the design changes must be validated. All too often, a change that was intended to improve the situation makes it worse. Through careful analyses and appropriate testing, one can determine that the proposed change results in some level of improvement.

5-2.3.10 Implement Design Changes.

Those design changes that are validated as improving availability must be implemented in a way that minimizes the downtime of the facility. Perhaps they can be made during scheduled maintenance periods. Or perhaps there are times of the day, month, or year when downtime is less critical to the mission than at other times. Careful planning can minimize the impact on the mission. Also, the procedures, tools, training, and materials

needed for the design change must be in place and validated prior to starting the facility modification.

5-2.3.11 Monitor Performance.

Continuously assess performance and identify opportunities for improvement. Continuous improvement should be the goal of every facility manager. As the facility ages, the cost-benefits of what were low-priority improvements may change, new problems may be introduced, and new mission requirements may arise. By collecting data and maintaining a baseline of the facility availability performance, the facility manager will be able to make future improvements as they become necessary or economical.

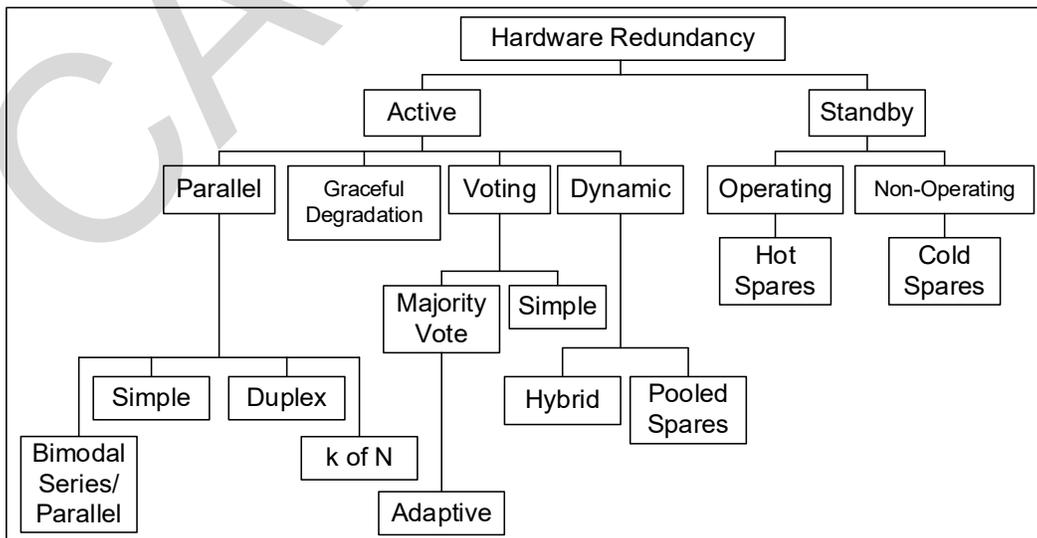
5-2.4 Improving Availability Through Addition of Redundancy.

Redundancy is a technique for increasing system reliability and availability by making the system immune to the failure of a single component. It is a form of fault tolerance – the system can tolerate one or more component failures and still perform its function(s).

5-2.4.1 Types of Redundancy.

There are essentially two kinds of redundancy techniques employed in fault tolerant designs, space redundancy and time redundancy. Space redundancy provides separate physical copies of a resource, function, or data item. Time redundancy, used primarily in digital systems, involves the process of storing information to handle transients, or encoding information that is shifted in time to check for unwanted changes. Space, or hardware, redundancy is the approach most commonly associated with fault tolerant design. Figure 5-8 provides a simplified tree-structure showing the various types of hardware redundancy that have been used or considered in the past.

Figure 5-8 Types of Redundancy



5-2.4.2 Impact on Testability.

Many of today's more sophisticated systems not only require an ability to detect faults but also to diagnose or isolate them. It may even be desirable for a system to have the ability to reconfigure itself to avoid system failure. Automated fault detection and isolation has therefore become an essential means of obtaining highly fault tolerant systems. Because of this, the design of the diagnostic system, including any built-in-test (BIT) features and the overall testability of the design are important tradeoffs that need to be made as part of the fault tolerant design process. Table 5-6 presents a sample list of hardware fault tolerant design approaches, and their impact on diagnostic approaches and BIT.

(1) No matter which technique is chosen to implement fault tolerance in a design, the ability to achieve fault tolerance is becoming increasingly dependent on the ability to detect, and isolate malfunctions as they occur or are anticipated to occur. Alternate maintainability diagnostic concepts must be carefully reviewed for effectiveness before committing to a final design approach. BIT design has become very important to achieving a fault tolerant system. When using BIT in fault tolerant system design, the BIT system must do the following:

- (a) Maintain real-time status of the system's assets (on-line and off-line, or standby, equipment).
- (b) Provide the operator with the status of available system assets.
- (c) Maintain a record of hardware faults for post-mission evaluation and corrective maintenance.

(2) The essence of fault tolerance is that the system is able to perform its mission despite experiencing some failures. In systems where redundancy is used, this fault tolerance is achieved by one or more redundant units taking over the function previously being performed by another unit. When standby redundancy is used, the failed unit must be detected and the standby unit "brought online." In still other cases principally involving electronics, failures can be repaired by rerouting signals or functions to other units. These repairs can be done upon a failure or in anticipation of a failure. In such cases, the BIT should, in addition to the actions identified in paragraph 5-2.4.2; maintain a record of any reconfiguration events that were required for system recovery during the mission.

(3) For fault tolerant systems, it is important that the design's inherent testability provisions include the ability to detect, identify, recover, and if possible, reconfigure, and report equipment malfunctions to operational personnel. The RBDs for fault tolerant systems are complex, with non-serial connections. Fault tolerant systems often have a multitude of backups with non-zero switch-over time and imperfect fault detection, isolation, and recovery. Therefore, it is imperative that effective testability provisions be incorporated in the system design concept. If they are not, the fielded design will exhibit long troubleshooting times, high false alarm rates, and low levels of system readiness.

Table 5-6 Diagnostic Implications of Fault Tolerant Design Approaches

Fault Tolerant Design Technique	Description	Diagnostic Design Implications	BIT Implications
Active Redundancy simple parallel	All parallel units are on whenever the system is operating. K of the N units are needed, where $0 < k < N$. External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails. Since the redundant units are always operating, they automatically pick up the load of the failed unit. An example is a multi-engine aircraft. The aircraft can continue to fly with one or more of engines out of operations	Hardware/Software is more readily available to perform multiple functions.	N/A
Active Redundancy with voting logic	Same as Active Redundancy but where a majority of units must agree (for example, when multiple computers are used)	Performance/status-monitoring function assures the operator that the equipment is working properly: failure is easily isolated to the locked-out branch by the voting logic	N/A
Stand-by redundancy (Non-operating)	The redundant units aren't operating and must be started if a failure is detected in the active unit (for example a spare radio is turned on when the primary radio fails.)	Test capability and diagnostic functions must be designed into each redundant or substitute functional path (on-line AND off-line) to determine their status.	Passive, periodic, or manually initiated BIT
Stand-by redundancy (Operating)	The redundant units are operating but not active in system operation; must be switched "in" if a failure is detected in the active unit (for example a redundant radar transmitter feeding a dummy load is switched into the antenna when the main transmitter fails)	N/A	Limited to passive BIT (such as, continuous monitoring) supplemented with periodic BIT

5-2.4.3 Role of RAM Concepts in the Fault Tolerant Design Process.

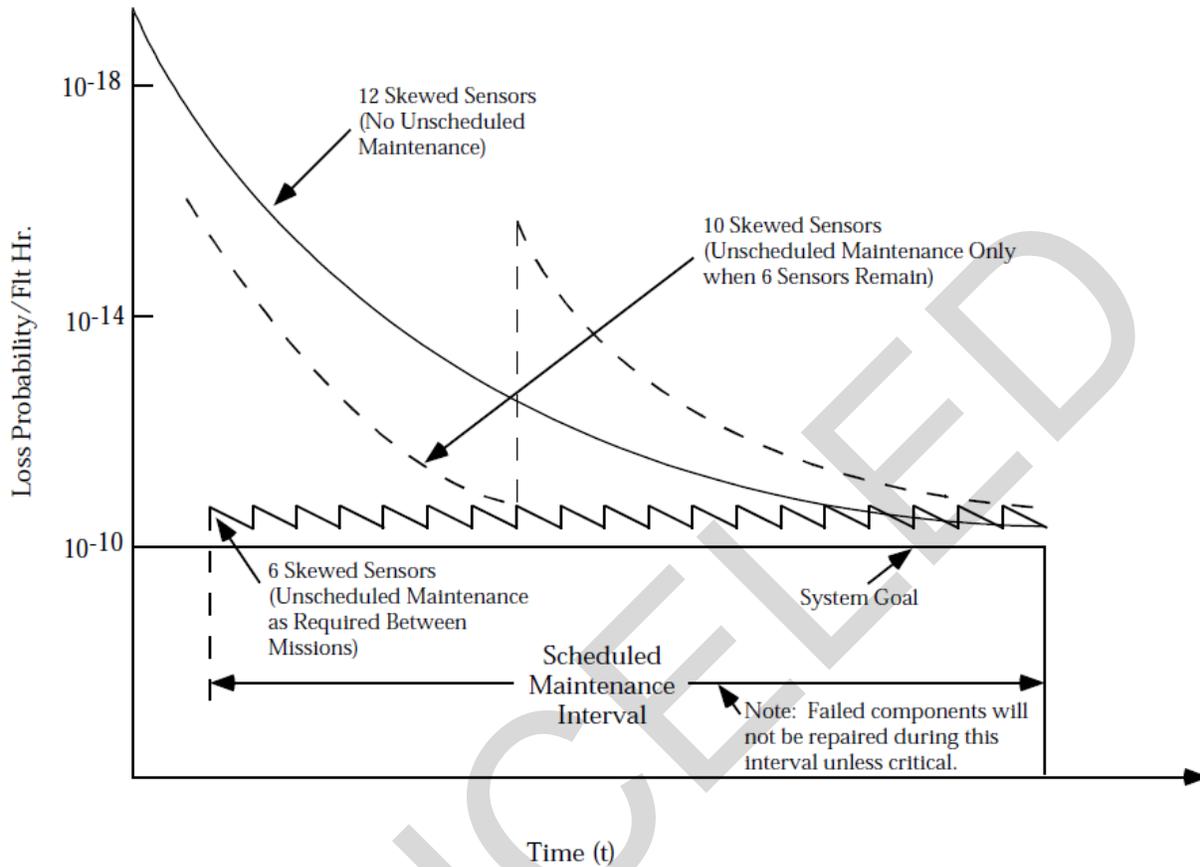
The role of the reliability engineer in regard to fault tolerant design requirements is to ensure that system RAM requirements are achievable for each of the fault tolerant design approaches being considered. Furthermore, to properly design a fault tolerant system, including a diagnostic scheme, the designer needs to understand the modes in which the system can fail, and the effects of those failure modes. This requires that a failure mode and effects analysis (FMEA) be performed, as a minimum. The FMEA will identify which faults can lead to system failure and therefore must be detected, isolated, and removed to maintain system integrity. In general, the reliability design manager must ask a series of questions, as listed below. Additionally, the RCM process helps to direct RAM concepts throughout the facility life cycle. The applicability of that process is further described in Chapter 7.

1. How do the system fault tolerance requirements impact the overall reliability, maintainability, and availability requirements?
2. Where should fault tolerant design methods be applied?
 - Which functions involve the most risk to mission success?
 - What is the effect of the operating environment?
 - What maintenance strategy/policy needs to be considered?
3. What is the effect of maintainability and testability?
4. What are the constraints that affect fault tolerance?
 - Cost
 - Size & Weight
 - Power
 - Interface Complexity
 - Diagnostic Uncertainties

5-2.4.4 Fault Tolerance and Tradeoffs.

The designer needs to consider each of the questions, listed above, and others as part of the overall fault tolerant design process. Other reliability tradeoffs to be considered involve analysis of the redundancy approaches being considered for the fault tolerant design. In addition to reliability concerns, fault tolerance also requires analysis of the impacts on maintainability and testability. As an example, consider Figure 5-9. This figure illustrates a design vs. corrective maintenance tradeoff analysis performed early in the product development phase. In particular, the figure shows the tradeoff of restoration frequency versus the number of sensors being used to meet requirements. This program requires a time period for allocating a scheduled maintenance activity and a probability of less than one in 10 billion per flight hour that a total loss of the skewed sensor function would occur. The tradeoff is made between the number of sensors and the cost of unscheduled maintenance activity associated with each approach. Other tradeoffs, such as cost, power, weight, etc. are also necessary. In general, as in any design analysis support function, an analysis of the impacts on reliability, availability, and maintainability (including support for system testing) of a chosen fault tolerant design approach must be performed.

Figure 5-9 Effect of Maintenance Concept on Level of Fault Tolerance



Note: More Frequent Restoration of Redundancy Lowers Fault Tolerance Requirements, But Results in Higher Maintenance Manhours

5-2.4.5 General Rules in Applying Redundancy.

In applying redundancy to a C5ISR facility, the following general rules should be followed:

5-2.4.5.1 Rule 1.

Determine the weak links in the system to know where to add redundancy. These weak links may be portions of the system prone to single point failures or, where redundancy is already used, the reliability is still too low to meet availability requirements.

(a) As an example of applying Rule 1, consider the simple system shown in Figure 5-10.

This system has five subsystems (lettered) with seven major components (numbered). The MTBF and MTRR for each component are shown. Using these figures, the overall system availability can be calculated using Monte Carlo simulation (see paragraph 5-3 for methods of calculating complicated system availability models). The results of a

Monte Carlo simulation of the system yielded the results shown in Table 5-7. The areas of weakness from an availability perspective can be determined from simply looking at the relative contribution to system unreliability as summarized in Table 5-8 (also resultants from a Monte Carlo simulation). Note that subsystem C is the weakest link, even though it is not subject to a single point failure. Subsystem D is the next weakest link; it is subject to a single point failure. It may have been obvious that D, representing a potential single point failure, is a weak link. It may not have been as obvious that C, even though it already incorporates redundancy, is a weak point. Looking at the relative availability of component 3, we see that it is much less reliable than the other components. Even dual redundancy is insufficient to compensate for the low MTBF. As this example shows, although it may be tempting to always add redundancy to those portions of a system subject to single point failures, it is sometimes more effective to add it elsewhere.

Figure 5-10 Analyzing the Contribution to System Reliability Helps Determine Where Redundancy is Needed

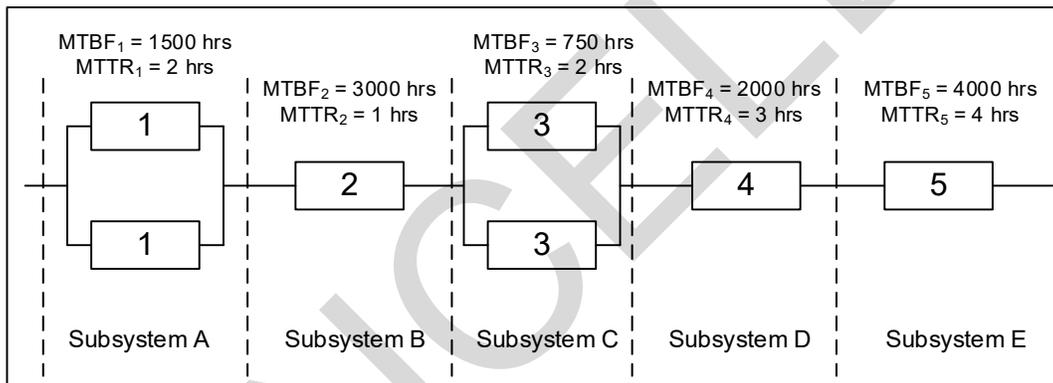


Table 5-7 Availability of System Depicted in Figure 5-10

MTBM	Mean System Failures	MTTR	Availability %
258.77	1.0658	2.5695	99.7236

Notes:

1. For ease of calculation, the times to failure and the times to repair were assumed to be distributed exponentially.
2. 10,000 simulation trials were run using an operating time of 1,000 hours.

Table 5-8 Relative Unreliability of Subsystems (Repairs Ignored)

Subsystem	Reliability in 1000 hours	Expected Failures per 1000 Hours	% Contribution to System Unreliability	Contribution to System Unreliability Ranking
A	0.7632	0.2368	14.12	4
B	0.7165	0.2835	16.90	3
C	0.4577	0.5423	32.33	1
D	0.6065	0.3935	23.46	2
E	0.7788	0.2212	13.19	5
SYSTEM	0.1182	1.6773	-	-

5-2.4.5.2 Rule 2.

Add redundancy in a way that avoids undesirable interactions. Rule 2 implies that some components cannot be used in some forms of redundancy, depending on the failure modes, application, and other factors. The type of redundancy shown in Figure 5-10 is active redundancy, in which all components are on all the time that the system is operating. In some cases, such a redundant configuration would result in undesired interactions or interference among the redundant units. As will be seen later in this chapter, certain forms of redundancy are preferable to others in a given application.

5-2.4.5.3 Rule 3.

Adding redundancy increases support requirements and costs. Rule 3 refers to the added costs incurred with redundancy. The most obvious increase is because more components must be purchased and installed. An additional cost comes from an increase in the total failures within the system. The increase in complexity results in an increase in unscheduled maintenance. If nothing is done to improve the reliability of the individual components in a system, but additional components are added to provide redundancy, the total failure rate of the components will increase. System reliability will improve but more component failures will occur. These failures will increase support requirements and costs. Redundancy also increases weight, space requirements, complexity, and time to design. Thus, safety and mission reliability are gained at the expense of adding an item(s) in the unscheduled maintenance chain.

(a) The decision to use redundant design techniques must be based on analysis of the tradeoffs involved. Redundancy may prove to be the only available method, when other techniques of improving reliability (for example, derating, simplification, better components) have been exhausted, or when methods of item improvement are shown to be more costly than duplications.

(b) When preventive maintenance is planned, the use of redundant equipment can allow for repair with no system downtime. Occasionally, situations exist in which equipment cannot be maintained. In these cases, redundant elements may be the best way to significantly prolong operating time.

5-2.4.5.4 Rule 4.

Ensure that any one redundant unit can be maintained without shutting down the other redundant units. Assume that two generators, for example, are sharing a load. If one fails and the operators must shut the other generator down to either gain access to or repair the failed generator, then there is no effective redundancy. An implicit assumption in using redundancy is that availability increases because a failed component can be repaired while the remaining redundant components continue to operate. If this assumption is violated, redundancy will not increase availability.

5-2.4.6 Design Considerations.

The FMEA is a primary reliability analysis, critical to the fault tolerant design process. The reliability engineer will use additional techniques as well for analyzing a fault tolerant design to verify that it meets reliability requirements. However, many of the evaluation tools used in the past are no longer adequate to deal with more sophisticated fault tolerant designs that include more complex fault handling capabilities. Because fault handling methods include the use of fault detection and fault recovery approaches, any evaluation tool must include the ability to properly account for the effects of imperfect fault detection and fault recovery.

5-2.4.6.1 Monte Carlo Simulation and Markov Techniques.

Monte Carlo simulation and Markov techniques continue to be used as the primary means of analyzing highly sophisticated fault tolerant designs. These approaches have been modified to incorporate situations where the sequence of failure is important, where the failure is transient or intermittent, or where the response to failure (such as, detection, isolation, recovery, and reconfiguration) is imperfect. In these situations, Markov methods continue to lead the way in evaluation methods. In general, the Markov approach, which is used to define the specific states that a system can occupy, has been used to incorporate fault handling and recovery. A major limitation to the Markov approach is that the number of system states that must be defined to comprehensively describe a large system and model the behavior of complex fault management schemes can become very large (approaching 10⁵ system states for highly complex systems). A common solution to this problem is to partition the system into smaller systems, evaluate each partition separately, and then combine the results at the system level. However, such an approach is only exact when each partitioned subsystem's fault tolerant behavior is mutually independent of each other. If subsystem dependencies do exist, then an assumption of independence will result in only an approximate solution.

5-2.4.6.2 Other Approaches.

Other approaches that are now becoming more common involve decomposing the system into separate fault-occurrence and fault handling submodels. However, the inputs for this type of approach require knowledge of the distribution and parameter values of detection, isolation, recovery, rates, etc. The following is a list of assumptions, limitations and sources of error found in existing reliability models:

- (a) Solving a fault-handling model in isolation and then reflecting its results in an aggregate model is, itself, an approximation technique. The assumptions necessary to determine a solution typically result in a lower bound (conservative) approximation of the system reliability.
- (b) Separate fault-handling models have been assumed to be independent of system state. This requires that the same fault-handling model and choice of parameters be used irrespective of the system's level of degradation. This ignores the fact that for many systems the recovery process is faster if the number of active units is smaller or that the recovery process may be different, depending on the sequence of events in different subsystems.
- (c) The common technique of partitioning the system into independent functional subgroups for computational ease is a potential source of error. The magnitude and direction of the error is a function of how truly independent/dependent the subgroups are of each other. If subgroups are assumed independent when in fact they are not, the effect is an overstatement of system reliability/availability. If subgroups are assumed completely dependent when some degree of independence exists, the effect is an understatement of the system's RAM capabilities.
- (d) Some models assume a constant instantaneous fault-protection coverage factor in lieu of a separate fault handling model. These fail to recognize that during time spent in the intermediate fault-handling states to detect, isolate, and recover/reconfigure, a second item failure could result in system failure. Further, as with fault handling models, these times are generally not constant, but depend on the current state of the system.
- (e) Most models require the assumption that the system is perfect at the mission start. Therefore, they cannot evaluate the effects of latent defects (for example, handling, manufacturing, transportation, and prior mission), nor assist in determining the testability payoff or requirements for detection and removing them before the start of the mission. Models with this limitation cannot be used to evaluate alternate maintenance concepts that include degradation between missions as an acceptable strategy.
- (f) Some models require that spares be treated exactly like active units, irrespective of their actual utilization in the system mechanization. This requires that spares are assumed to be "hot" and have the same failure rates and failure modes as the active units. This assumption will cause the model to understate the system reliability in those situations where spares are "cold" or in "stand-by" and/or where their failure rates may be less than those of the active units.
- (g) As indicated previously, some models require the assumption that item failure rates are constant throughout time. This will result in an overstatement of system reliability if the items have failure rates that increase with mission time. Some models remove this restriction and permit time-varying failure rates. However, the solution algorithms employed require the use of global time (as opposed to local time of entry into a state), thus precluding the use of the model for repairable systems and availability analysis.

5-3 ASSESSING RELIABILITY AND AVAILABILITY.

5-3.1 Purpose of the Assessment.

As systems become more and more complex, good methods for specifying and analyzing the systems and their sub-systems become more important. Reliability modeling (including prediction, evaluation, and control) is vital for proper design, dependable operation, and effective maintenance of systems. The popularity of designing redundancy into systems poses additional challenges to reliability professionals. For the various kinds of redundant systems, the reliability and availability are extremely sensitive to even small variations in certain parameters; thus, precise understanding and insight can be gained only by modeling.

The need to assess the reliability, availability, and maintainability of a system is becoming more important as organizations understand the potential effects of failures and downtime for the systems. Regardless of what mission is being served, or who the intended customer may be, it should be a reasonable assumption to state that the degree of product/service success is directly related to the ability of that product/service to meet or exceed customer expectations.

The eight-step process shown below should be adhered to during a reliability study. Validation is essential throughout the eight-step process.

- 1) **Problem Definition:** define problem and its objectives.
- 2) **Model Building:** description of system's entities and their interaction.
- 3) **Data Collection:** quantify probability distributions for system's entities.
- 4) **Program:** select programming language or software package to execute.
- 5) **Verification:** check that code is achieving expected results.
- 6) **Experimental Design:** determine initial conditions, simulation period and number of runs (must be statistically valid).
- 7) **Implementation:** run model and test its sensitivity to variations.
- 8) **Documentation:** document reliability study to verify problem definition objectives are reached (document enough for functional model in future).

5-3.2 Prediction.

There are many valid reasons for predicting reliability. One purpose for reliability prediction is to assess the reliability of a proposed design and to provide a quantitative basis for selection among competing approaches or components. In addition, prediction results can be used to rank design problem areas and assess trade study results. A combination of prediction methods should be used to assess progress in meeting

design goals, identifying environmental concerns, controlling critical items, and determining end-of-life failure mechanisms. Making predictions should be an ongoing activity that starts with the initial design concept and continues through the evaluation of alternate design approaches, redesigns, and corrective actions. Each iteration of prediction should provide a better estimate of system reliability as better information on the system design approach becomes available.

5-3.3 Analytical Methodologies.

Analytical methods of evaluating systems are based on a variety of logical and mathematical principles. Some utilize logical algebraic formulas to arrive at a closed-form, exact, solution to a model of a system. Others use simulation processing to empirically arrive at model solutions. Simple systems can be calculated with pencil and paper. Those exercises grow linearly as the model grows linearly. Several techniques/software algorithms streamline the process of calculating availability for large systems.

5-3.3.1 Cut Set.

The cut-set method can be applied to systems with simple as well as complex configurations and is a very suitable technique for the reliability analysis of power distribution systems. A cut-set is a “set of components whose failure alone will cause system failure,” and a minimal cut-set has no proper subset of components whose failure alone will cause system failure. The components of a minimal cut-set are in parallel since all of them must fail to cause system failure and various minimal cut-sets are in series as any one minimal cut-set can cause system failure.

5-3.3.2 Network Reduction.

The network reduction method is useful for systems consisting of series and parallel subsystems. This method consists of successively reducing the series and parallel structures by equivalent components. Knowledge of the series and parallel reduction formulas is essential for the application of this technique.

5-3.3.3 Boolean Algebra and Block Diagrams.

One of the most useful tools in evaluation methods has been the use of a combination of block diagrams and Boolean algebra. The use of software to these analyses is critical given that the logic and algebra become immense as systems grow. The GO algorithm is one such instrumental method.

5-3.3.3.1 GO Algorithm.

The GO algorithm, a success-oriented system analysis technique, was originally developed for defense industry applications in the early 1960s. The capability of the GO methodology was drastically improved under the sponsorship of the Electric Power Research Institute (EPRI) with the development of additional analytical techniques

(such as system interactions, system dependencies, and man-machine interactions) and improved computer software reliability. The popularity of the GO method can be linked to basic characteristics that fault trees do not possess. The hardware is modeled in a manner more or less the same way as in the system drawings, model modifications can be easily introduced to reflect configuration changes, and the modeling capability is extremely flexible. GO's success-oriented technique analyzes system performance through straightforward inductive logic. The GO representation of a system, or GO model, can often be constructed directly from engineering drawings, which makes GO a valuable tool for many applications, since it is relatively easy to build and review models.

5-3.3.3.2 System Model.

A system model is first constructed within the GO methodology using a top-down (forward-looking) approach to identify the functions required for successful operation following normal process flow or operational sequences. Secondly, in the GO methodology each of the systems that provide the functionality is modeled to the required level of detail. The level of detail may be at the system, subsystem, or component level depending upon the type of information required and the plant specific information available. The GO models determine all system-response modes: successes, failures, prematures, etc.

5-3.3.3.3 Go Models.

GO models consist of arrangements of GO operator symbols and represent the engineering functions of components, subsystems, and systems. The models are generally constructed from engineering (one-line) drawings by replacing engineering elements (valves, motors, switches, etc.) with one or more GO symbols that are interrelated to represent system functions, logic, and operational sequences. The GO software uses the GO model to quantify system performance. The method evaluates system reliability and availability, identifies fault sets, ranks the relative importance of the constituent elements, and places confidence bounds on the probabilities of occurrence of system events reflecting the effects of data uncertainties. Some key features of the GO method are:

- Models follow the normal process flow
- Most model elements have one-to-one correspondence with system elements
- Models accommodate component and system interactions and dependencies
- Models are compact and easy to validate
- Outputs represent all system success and failure states
- Models can be easily altered and updated

- Fault sets can be generated without altering the basic model
- System operational aspects can be incorporated
- Numerical errors due to pruning are known and can be controlled

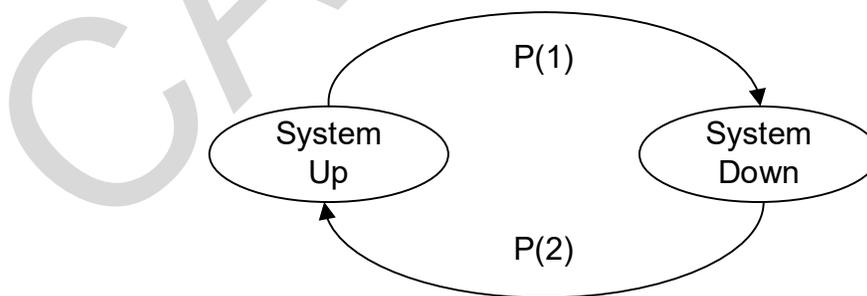
5-3.3.3.4 Go Procedure.

The GO procedure uses a set of seventeen standard logical operators to represent the logic operation, interaction, and combination of physical equipment and human actions. For example, a type 1 operator represents the logical operation of equipment which either performs, or fails to perform, its function given a proper input or stimulus. The type 2 operator performs the logical OR gate operation where a successful response is generated if any of several inputs is proper, etc. The Random variables of the GO methodology include operator inputs called stimuli ($S_1, S_2 \dots S_n$) and outputs referred to as responses ($R_1, R_2 \dots, R_n$). An operator, which represents equipment responses or human actions, and which may itself have associated performance probabilities, process the input random variable in a prescribed and well-defined way to generate the output random variables. These random variables are given the electrical term “signals” in the GO models.

5-3.3.4 State Space.

The State Space methodology is founded on a more general mathematical concept called Markov Chains. Markov Chains employ a modeling technique that describes a system by the possible states in which it can possess (such as State Space). For this purpose, a system essentially resides in two distinct states: up or down. The probability of transitioning from one state to the other in a given time period is the critical reliability metric used. Figure 5-11 shows this simple Markov model.

Figure 5-11 Simple Markov Model



Where

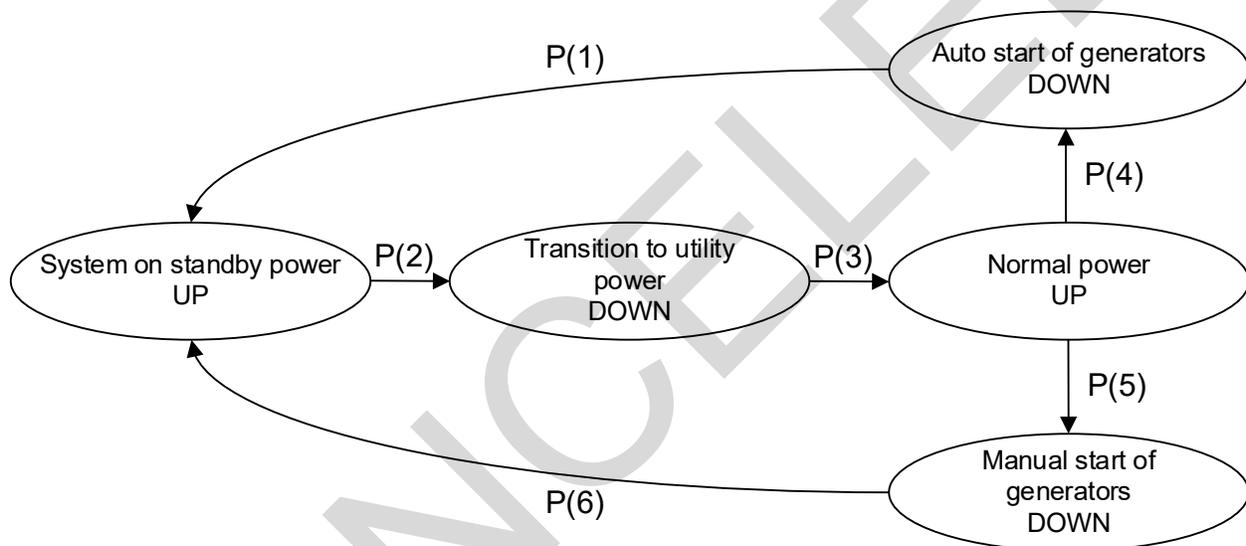
$P(1)$ is the probability of the system going down in time t

$P(2)$ probability of the system coming up in time t

(1) However, the true goal of availability analysis is to determine the probability of being in the up state – or the time spent in the up state for an indefinite time period. To show this, consider a simple scenario including only a system with backup generation. Given loss of utility power, the generators will either start automatically or, if that functionality fails, the generators can be started manually. In those starting phases, the system is ‘down.’ Once started, the system is ‘up.’ The system will then switch to utility power once available. The system could be down during that switching.

(2) Figure 5-12 shows the associated Markov model for this system. Between each of the possible states are state transitional probabilities that must be known. The solution to the model will be the system’s time spent in the up states vs. the down states.

Figure 5-12 Less Simple Markov Model



(3) Solving Markov models is simple only for very simple models, by solving a set of linear equations. The complexity solving these models grows exponentially as the sizes of the models grow linearly. Solutions can be found by using complex Numerical Analysis methods involving Linear Algebraic matrix operations, etc. Markov models can also be solved by Monte Carlo techniques described below.

5-3.3.5 Monte Carlo Simulation.

Monte Carlo Simulation is the most versatile modeling methodology available. The methodology can be implemented in many forms from simple models in a spreadsheet environment to complex models that are ‘hand crafted’ in a programming language of choice. There are also a variety of simulation software packages that provide drag-and-drop environments that can automate the creation of simulated models for the casual analyst.

(1) The Monte Carlo Simulator operates on an iterative process where each ‘iteration’

represents a description of what the system could experience through a set mission life. For instance, consider the past experience of a system, including what really failed, that experience was only one of infinite possible outcomes that depended on the failure characteristics of that system.

(2) Thus, Monte Carlo Simulation looks forward by considering possible scenarios that could occur in the future – and those scenarios, with their associated likelihoods, are dependent on the failure characteristics applied to the system components. For each iteration, failure times and the associated repair attributes are picked for each component in the system. The simulation will then implement the logical relationships of the system to determine:

(a) If a failure has occurred in the system prior to the defined mission life.

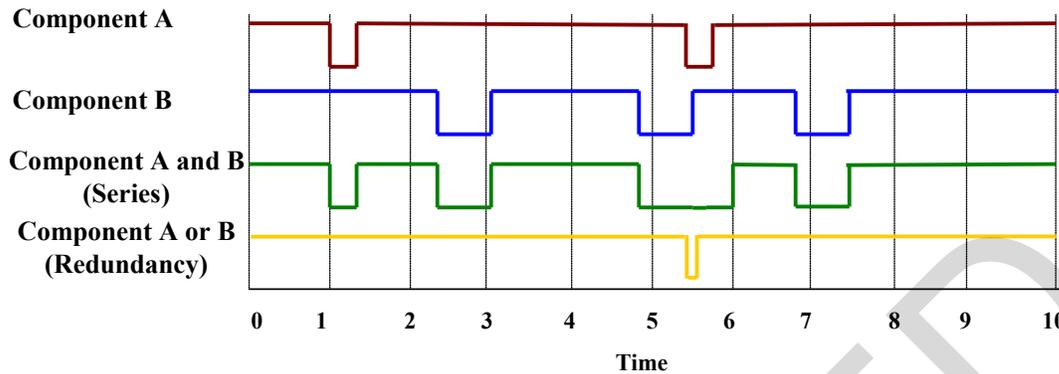
(b) If a failed component(s) takes the system down, what is the duration of downtime?

(3) With these items determined, the availability for the system in that particular iteration can be calculated. Then, as this single iteration is repeated, an average is tabulated of uptime vs. downtime, and duration of downtime. The average of all the iterations yields expected system availability.

(4) This method is extremely useful in calculating downtime based on different types of failure distributions. A component in a system may be repaired or replaced upon failure. Because many components that are replaced have failure distributions that are based on time in service, calculations must incorporate time-based failure distributions to accurately predict system availability.

(5) Figure 5-13 shows a sample timeline of the operation of two components. In this example, both components start in the available state. As the simulated time progresses, component failures are randomly generated based on that component's operational RAM statistics. The figure shows the difference in series and redundant component orientation. In series, downtime occurs when either component fails; with redundancy, both components are required to fail to incur downtime.

Figure 5-13 Timeline of a Monte Carlo Simulation



5-3.4 Analysis Considerations.

The results of availability analyses are extremely sensitive to factors such as underlying assumptions, techniques for calculating availability, and the data used to support the analysis. No results of an analysis should be distributed – let alone trusted – without documentation supporting those attributes. Subtle differences in those attributes can produce drastically different results – results that might be used to drive design decision making. It is the ultimate responsibility of the analyst to be aware of those sensitivities and perform and present analyses with integrity.

5-3.4.1 Modeling Limitations.

Cut set, State Space, Network Reduction and Boolean algebra are techniques that lend themselves to the casual reliability engineer to analyze small systems; primarily because they can all be accomplished with common desktop PC tools such as spreadsheets, etc. A series of studies recently performed on the IEEE Gold Book (IEEE 493-2007) standard network have shown that, provided that the assumptions are held equal, each technique produces similar results. However, model size and data sophistication make algebraic methods more complicated and therefore, more difficult to use.

5-3.4.1.1 Large Systems.

As larger systems are modeled, the sheer size of the analysis becomes burdensome for the analyst. Furthermore, ‘what-if’ sensitivity analyses also become impractical because models must be redrawn and formulas, rewritten. For the number of formulas and conditions that can be involved, peer reviews are of utmost importance to compensate for the high probability of error involved in such an extensive effort.

5-3.4.1.2

Data collection efforts have expanded the analysts’ tools beyond the classical ‘MTBF’ analysis. MTBF relies on the exponential distribution, sometimes referred to “point estimates.” These estimates give the average MTBF (such as one point). Failure

distributions such as the Normal, Lognormal, Weibull, etc. are being fitted to common failure modes of many critical components in electrical and mechanical distribution networks. These distributions capture the fact that the failure rate of a component likely changes over time, capturing initial and wear-out failure modes. These distributions require more precise data collection: time-to-failure data. With point estimates, the data collector need only count operational hours and failure events for a component. For time-to-failure data, each interval of time between installation and failures, making the data collection and processing effort extremely challenging, but extremely valuable.

5-3.4.1.3 Time-To-Failure Data.

Time-to-failure data has become substantially important to system analyses. For many components such as belts, valves, and batteries, availability figures may not be specific enough to characterize the likelihood of failure. In these cases, failures are more likely to occur toward the end of a component's life – not evenly throughout its life. Simulation methods provide the means to include these considerations.

5-3.4.2 Modeling Hurdles.

There are several system attributes that are challenging to model. UPS battery life, for instance, had historically been assumed to be limitless in many analyses – whereas their contribution to power availability is not. Furthermore, data has shown that standby equipment has differing distributions from their primary counterparts. Spare parts availability, human factors, etc. are difficult to capture with the classical approaches to availability analysis.

5-3.4.3 Modeling Data.

The underlying data that supports a reliability assessment can be as important as the model itself. Data must be scrutinized to ensure that the results are realistic and defensible. There are a variety of sources of component reliability data. Army technical manual Survey of Reliability and Availability Information for Power Distribution, Power Generation and Heating, Ventilating and Air Conditioning (HVAC) Components for Commercial, Industrial and Utility Installations (TM 5-698-5) contains data collected by the US Army Corps of Engineers. This dataset was collected and summarized for the distinct propose of modeling C5ISR facilities.

5-3.4.4 Modeling Solutions.

The typical engineer can perform 'back of the envelope' analyses easily. Results from these analyses are only as good as the assumed ground rules and the data used. Experience has shown that analysts who wish to perform availability studies often and consistently should choose a software package to aid in this effort. Packages exist that perform analyses via most of the described methodologies. Once a package is selected, the user should become familiar with the package behavior, the analytical or numerical methodology used, and the underlying limitations of that package.

5-3.5 Modeling Examples.

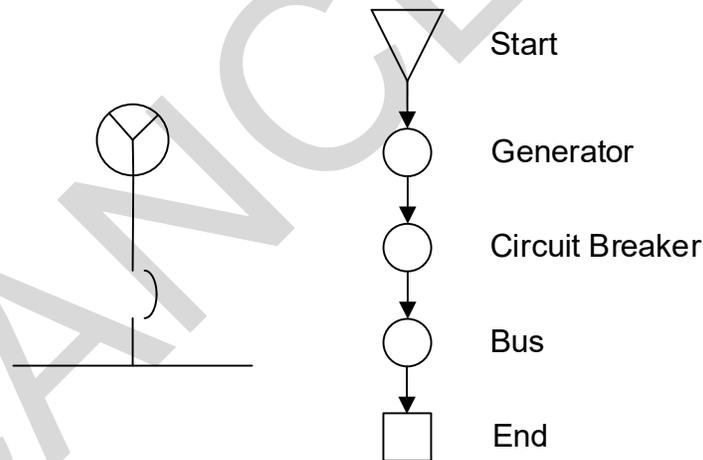
No matter what methodology is chosen for a reliability analysis, the expected results, provided that the underlying assumptions are held fixed, should be consistent across all methods. The analyst should develop a sense of the expected results of small systems and have a feel for the effects of increments changes to a system when made. Below are a series of small examples that will illustrate typical results in simple models.

5-3.5.1 Modeling Basics.

Reliability modeling generally begins with referring to a one-line drawing for the electrical, mechanical, and control systems. In addition to these resources, the analyst should have a firm understanding of the theory of operation of the system to be modeled. These sources of information will form the basis for the structure and behavior of the system that is to be modeled.

(1) For this UFC, a pseudo diagramming technique is adopted that can be applied to, or converted to, whichever modeling technique is chosen. The convention can be most accurately described as an RBD. Figure 5-14 shows a typical one-line diagram representation of a generator/bus and its corresponding RBD representation.

Figure 5-14 Simple Series Model



(2) Figure 5-14 represents a typical series diagram – the most common scenario observed in electrical and mechanical one-line drawings and can be solved simply by series calculations, such as for power to be available at the bus, the following must be available: generator, breaker, and the bus.

(3) Assume that the generator has an availability of 0.99, the breaker is 0.9999, and the bus is 0.99999. Then the series can be calculated by the following equation:

Equation 5-12. Availability for Figure 5-14

$$A = 0.99 \times 0.99999 \times 0.9999 = 0.989891$$

Where:

$A = \text{Availability}$

(4) Typical generator models often require an N of M calculation. If, for example a plant has three generators, of which two are required to carry the critical load, then a 2 of 3 generator availability calculation must be made. The calculation for this can be quite complex, but is reasonable for small values of M:

Equation 5-13. Availability for Typical Generator Models

$$A = \sum_{k=m}^n \frac{n!}{k!(n-k)!} (A')^k (1 - A')^{(N-K)}$$

Where:

$A = \text{Availability}$

$n = \text{the total number of components}$

$m = \text{the required components}$

(5) Figure 5-15 represents a simplistic parallel-redundant system commonly found in C5ISR facilities. Note that the model consists of series calculations and parallel calculations. This model implies that there is a pure redundancy, where switching between A and B happens without risk of failure. In most cases, there are reliability considerations in the switching between redundant systems.

(6) The model described by Figure 5-15 can also be solved with simple calculations. Assume that the bus has an availability of 0.99999, the breakers are 0.9999, and the UPS is 0.999. To determine the system availability, one must reduce the network to simpler series and parallel models. The general sequence is to reduce the breaker-UPS-breaker series to one value. Then calculate the redundant OR operator followed by treating that result as a value in series with the bus. The breaker-UPS-breaker series can be computed by

Equation 5-14. Breaker-UPS-Breaker Reduction for Figure 5-15

$$A_{UPS} = 0.9999 \times 0.999 \times 0.9999 = 0.9988002$$

Where:

$A_{ups} = \text{the UPS Availability}$

Now, with that reduction, the model can be represented by Figure 5-16.

Figure 5-15 Simple Parallel Model

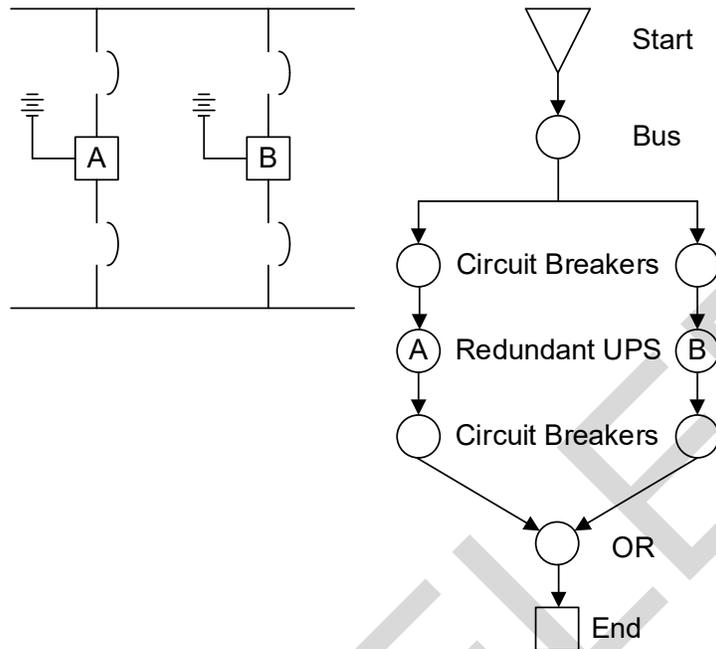
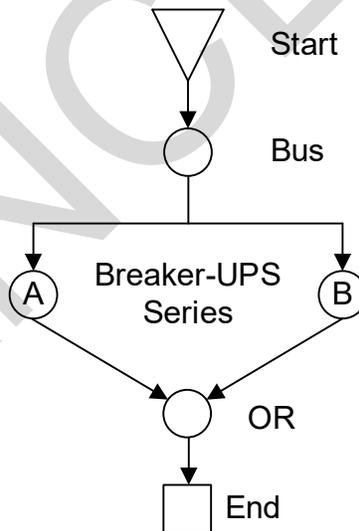


Figure 5-16 Simple Parallel Model, First Reduction



Next reduce the OR calculation to one availability value:

Equation 5-15. OR Availability for Figure 5-16

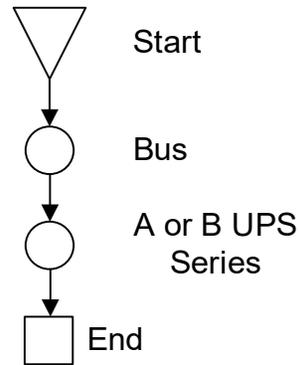
$$A_{OR} = 1 - [(1 - 0.9988002) \times (1 - 0.9988002)] = 0.99999856$$

Where:

A_{OR} = OR Availability

Figure 5-17 shows this further reduction.

Figure 5-17 Simple Parallel Model, Second Reduction



Then, this system, now reduced to a series system, can be easily calculated by

Equation 5-16. Final Availability for Figure 5-17

$$A_{Final} = 0.99999 \times 0.99999856 = 0.99998856$$

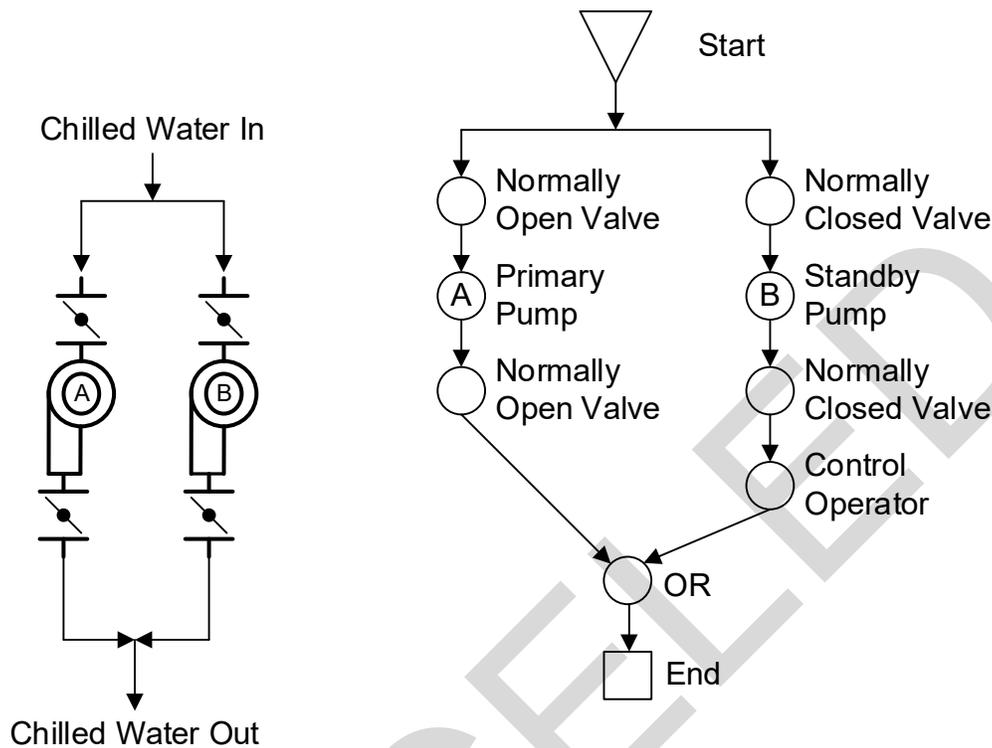
Where:

A_{Final} = Final Availability

(7) Building controls contingencies into reliability models is prudent. Often pure OR gates result in availability values that are inflated because they do not include the probability of the switching action itself. Whether the control is automatic via PLC or SCADA, or requires maintenance personnel to manually make the switch, the redundancy is limited by that switching action.

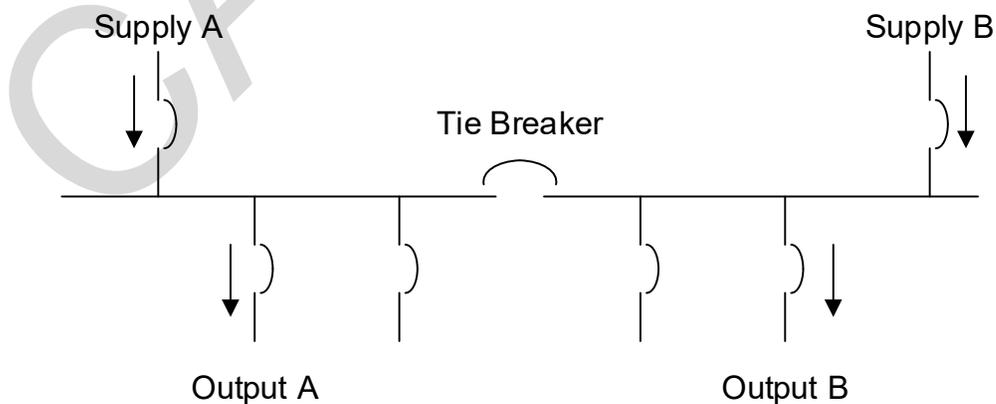
(8) Consider Figure 5-18 where a facility utilizes dual chilled water pumps. If Pump A fails (or is taken down for maintenance) the valves supporting Pump A must be closed and the valves supporting Pump B must be opened. The model shows a control node with the B series to represent the reliability of the switching. Note that the A path, the 'normal day' operating mode, has no controls contingency. Only when path B is required does the availability of the system need to be reduced due to the switching function.

Figure 5-18 Parallel Model with Controls Contingency



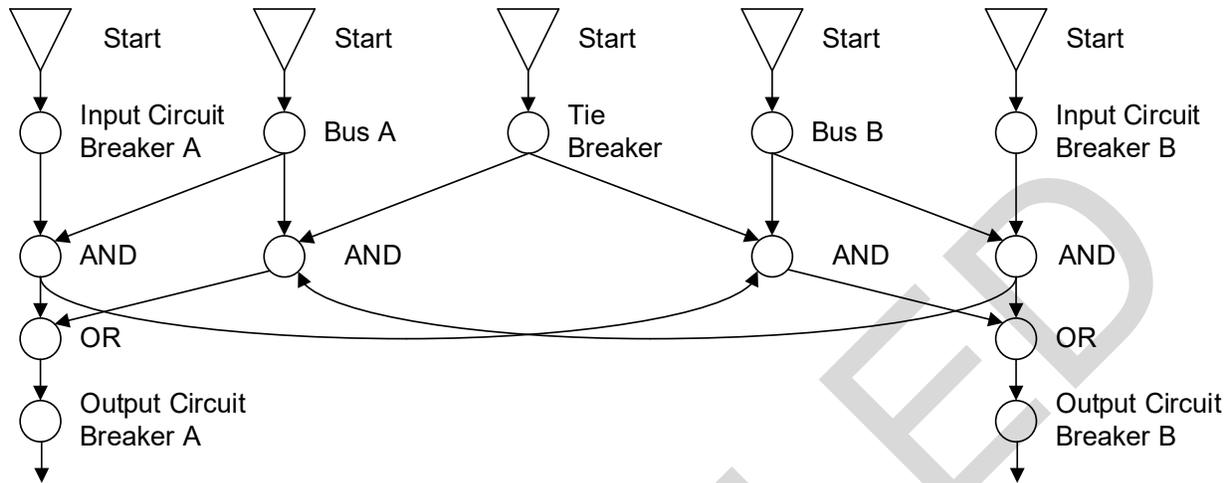
(9) Modeling becomes significantly more complicated when redundant paths are added. Even the most common scheme found in C5ISR facilities, the Double-Ended Bus with a tie, can begin to complicate modeling. Consider Figure 5-19. The gear essentially receives power from two sources and passes it through via two paths (thus retaining the redundancy). If one source is lost, then the Tie, which is normally open, closes to provide power to both output paths.

Figure 5-19 Double Ended Bus



A typical model of this system is illustrated in Figure 5-20

Figure 5-20 Model of Double Ended Bus



(10) The key to the logic lies in the fact that typical modeling cannot readily emulate that power can pass through the tie in both directions. Thus, the availabilities of the tie and the busses are created independently and used within the logic where required.

(11) If one looks at the logic behind the availability of power out of a breaker on bus A, then the critical 'OR' statement is joining the following two scenarios:

- (a) Power available from source A
- (b) Power required from source B

(12) In case (a), the only required components are the incoming breaker, (on side A) the Bus A, and the outgoing breaker A. Case (b) requires much more. In order of how the power will flow if source A is unavailable: Input Breaker B, Bus B, Tie, Bus A, output Breaker A. Figures 5-21 and 5-22 show these two cases, with the pivotal OR block shaded black.

Figure 5-21 Model of Double Ended Bus, Case 1

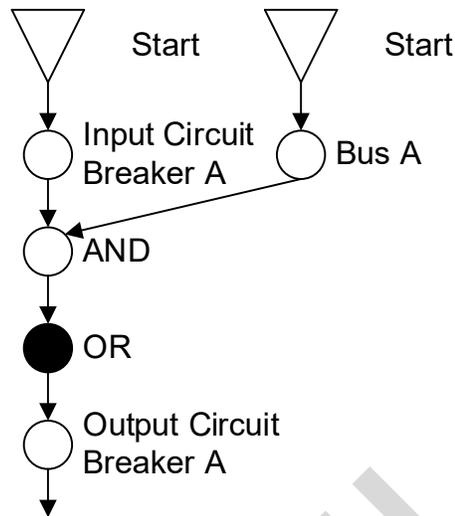
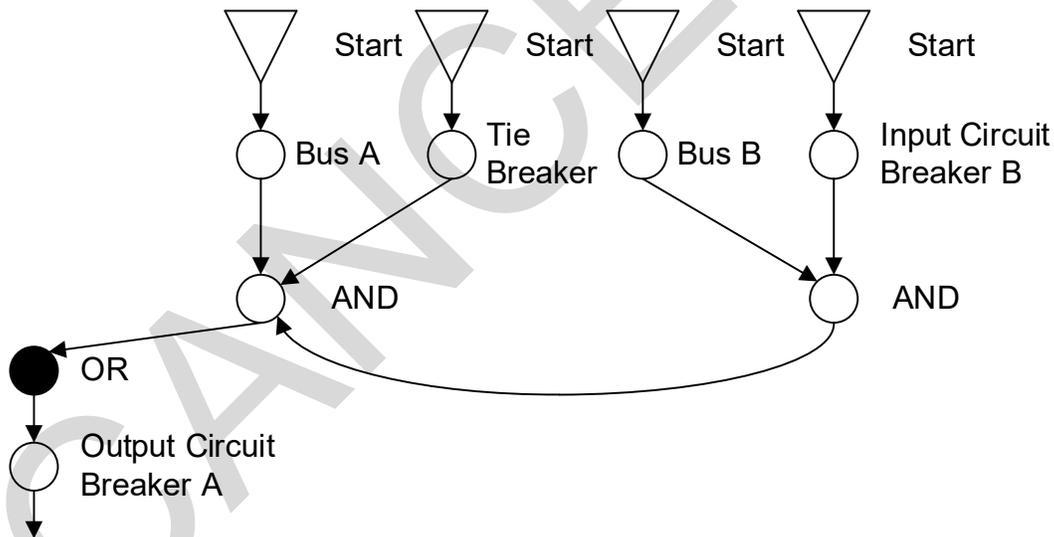


Figure 5-22 Model of Double Ended Bus, Case 2



5-3.6 Modeling Complexities.

The modeling examples discussed previously represent a top-down style of modeling and is the most common type of modeling. The model has a beginning and an end. Failures within the model interrupt the availability of downstream components. This style has a variety of advantages, one being that it loosely follows the intuitive paths of, say, power or chilled water. There are some disadvantages and limitations to top-down modeling: upstream effects of failures, loop systems, and UPS systems. In most cases, advanced simulation methods need to be employed to capture these complexities.

5-3.6.1 Effects of Unique Failure Modes.

The failure of a component in a system typically influences the remainder of the system downstream of the failure only. Unfortunately, there are some failures, or failure modes of a component, that can have effects on the system upstream. For example, if a circuit breaker fails to open on command, such as there is a downstream fault that the breaker is intended to protect against but doesn't. That fault can be passed upstream and influence a much larger portion of the entire system than just those components downstream of the fault. The sequence of Figure 5-23 shows how a downstream fault can affect other sub-systems.

5-3.6.2 Interdependencies and Loop Systems.

Interdependencies and loop systems are common in C5ISR facilities. Two scenarios often create a modeling hurdle. One instance is the interdependency between power, chilled water, and controls. The mechanical systems are dependent on power and the controls system, the power system depends on the controls system, and the control system requires power. These interdependencies are possible to model, though typically only through special means, such as Monte Carlo Analysis.

5-3.6.3 UPS Systems.

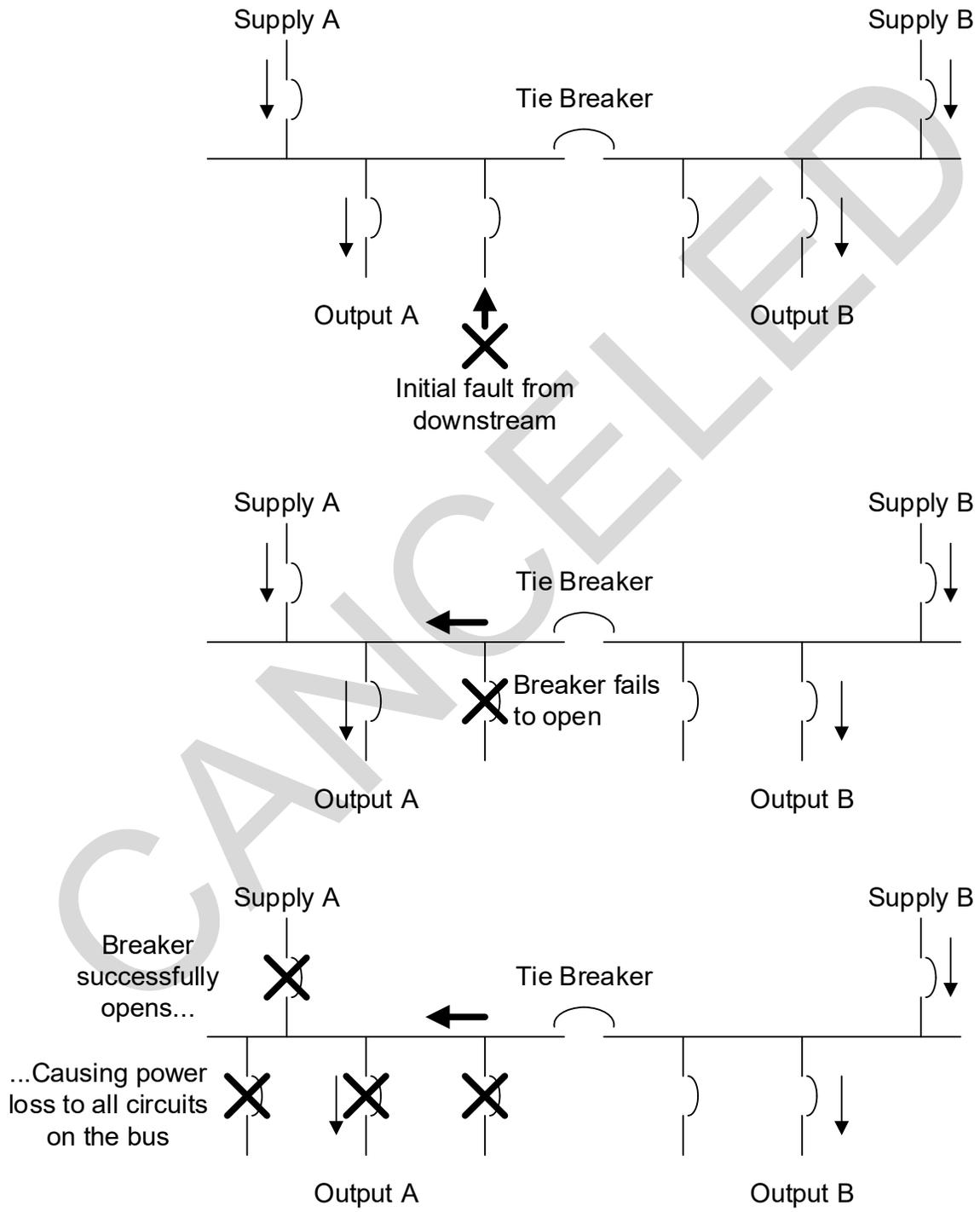
Uninterruptible power supply systems present a unique challenge to the analyst because capturing the effects on availability from the added battery backup can be difficult. The concept of operation for a UPS is limited to the fact that the battery has a limited life. If, for instance, a UPS has 45 minutes of ride-through time, then any upstream interruption less than 45 minutes will essentially be mitigated. However, if an interruption lasts longer than 45 minutes, the total interruption time is essentially shortened by 45 minutes before the downstream mission is lost. Below are two simple cases to illustrate this point.

Assume that over the course of one year, a system experiences a failure upstream of the UPS:

Case 1: the failing component is repaired within 30 minutes. In this case the UPS provides sufficient downstream power and the mission remains available. This case yields an availability of $8766/8766 = 1$. Availability is retained.

Case 2: the failing component requires 24 hours to repair. In this case the UPS merely reduces the downtime of the mission to 24 hrs – 45 minutes, or 23.25 hrs. In this case the availability for the case-year is $(8766-23.25)/8766$ or 0.9973.

Figure 5-23 Downstream Fault



5-3.6.4 Conclusion of Complexities.

Complex modeling scenarios need complex modeling techniques. In most cases Monte Carlo methods need to be employed. Monte Carlo methods capture true operating scenarios, one iteration at a time, as set up by the analyst. Simulation allows the analyst to interject nearly any conceivable operating anomaly that might occur in a facility.

5-3.7 Conclusion.

RAM studies should be conducted with the intent of capturing the actual behavior of the facility. This goal will force the analyst to continually seek better data and better modeling techniques. Although, in design, RAM can not be perfectly captured; it is still just a prediction. Refined assessment techniques can uncover previously unforeseen contingencies that may cause a mission to be lost.

5-3.7.1 RAM Analysis.

RAM analysis must be continuously improved to converge with the behavior of a system. As systems become more complex, the methods will undoubtedly become more complex as well. The analyst should always compare their modeling assumptions and attributes captured to the actual operation of the system being modeled. New techniques must continuously be explored to see that the gap between the models and the true system narrows.

5-3.7.2 Verification.

Facility managers must verify that the model is valid – capturing their system accurately. They must also be aware of the reliability data that supports the model. The model is only as good as the data that it uses. In a sense, the data is a single-point vulnerability for the accuracy of the model. Facility managers and reliability analysts alike should always consult the most recent IEEE DOT STD 3006.8 for reliability data. Further, adoption of a continuous RAM process such as RCM will provide actual system behavior data that will continue to serve the reliability, availability, and maintainability goals over the life of the system.

CHAPTER 6 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS

6-1 BACKGROUND ON FMECA.

6-1.1 Define FMECA.

The FMECA is composed of two separate analyses, the Failure Mode and Effects Analysis (FMEA) and the Criticality Analysis (CA). The FMEA analyzes different failure modes and their effects on the system while the CA classifies or prioritizes their level of importance based on failure rate and severity of the effect of failure. The ranking process of the CA can be accomplished by utilizing existing failure data or by a subjective ranking procedure conducted by a team of people with an understanding of the system. Although the analysis can be applied to any type of system, this manual will focus on applying the analysis to a C5ISR facility.

6-1.1.1 Initiating a FMECA.

The FMECA should be initiated as soon as preliminary design information is available. The FMECA is a living document that is not only beneficial when used during the design phase but also during system use. As more information on the system is available the analysis should be updated to provide the most benefit. This document will be the baseline for safety analysis, maintainability, maintenance plan analysis, and for failure detection and isolation of subsystem design. Although cost should not be the main objective of this analysis, it typically does result in an overall reduction in cost to operate and maintain the facility.

6-1.2 FMECA Benefits.

The FMECA will:

- Highlight single point failures requiring corrective action.
- Aid in developing test methods and troubleshooting techniques.
- Provide a foundation for qualitative reliability, maintainability, safety, and logistics analyses.
- Provide estimates of system critical failure rates.
- Provide a quantitative ranking of system and/or subsystem failure modes relative to mission importance; and identify parts & systems most likely to fail.

6-1.2.1 Developing a FMECA.

Developing a FMECA during the design phase of a facility, the overall costs will be minimized by identifying single point failures and other areas of concern prior to construction, or manufacturing. The FMECA will also provide a baseline or a tool for troubleshooting to be used for identifying corrective actions for a given failure. This

information can then be used to perform other analyses such as a FTA or an RCM analysis.

6-1.2.2 FTA.

The FTA is a tool used for identifying multiple point failures; more than one condition to take place for a particular failure to occur. This analysis is typically conducted on areas that would cripple the mission or cause a serious injury to personnel.

6-1.2.3 RCM Analysis.

The RCM analysis is a process that is used to identify maintenance actions that will reduce the probability of failure at the least amount of cost. This includes utilizing monitoring equipment for predicting failure and for some equipment, allowing it to run to failure. This process relies on up-to-date operating performance data compiled from a computerized maintenance system. This data is then plugged into a FMECA to rank and identify the failure modes of concern.

6-1.2.4 Additional Analysis Information.

For more information regarding these types of analyses refer to the following publications:

- (1) Ned H. Criscimagna, Practical Application of Reliability Centered Maintenance Report No. RCM, Reliability Analysis Center, 201 Mill Street, Rome, NY, 2001.
- (2) David Mahar, James W. Wilbur, Fault Tree Analysis Application Guide, Report No. FTA, Reliability Analysis Center, 201 Mill St., Rome, NY: 1990
- (3) NASA's Reliability Centered Maintenance Guide for Facilities and Collateral Equipment, February 2000.

6-1.3 Team Effort.

The FMECA should be a catalyst to stimulate ideas between the design engineer, operations manager, maintenance manager, and a representative of the maintenance personnel (technician). The team members should have a thorough understanding of the systems operations and the mission's requirements. A team leader should be selected that has FMECA experience. If the leader does not have experience, then a FMECA facilitator should be sought. If the original group of team members discovers that they do not have expertise in a particular area during the FMECA then they should consult an individual who has the knowledge in the required area before moving on to the next phase. The earlier a problem in the design process is resolved, the less costly it is to correct it.

- Knowledge of mission requirements
- An understanding of component, subsystem, & systems operations

b. Once the team has all the information available to them, the analysis can proceed. The team leader should organize a meeting place for all team members with enough space to display schematics, block diagrams or bill of materials for all members to view. Setting the ground rules and establishing the goals of the mission should be discussed at the first meeting.

6-1.6 Goals.

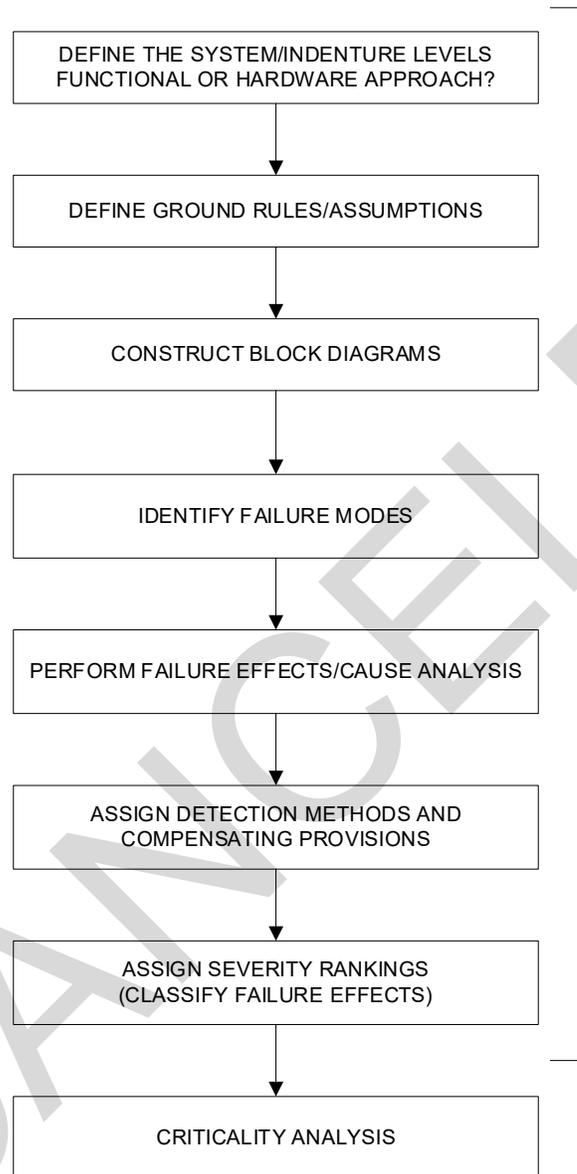
Questions from all participants should be addressed. It is essential to the analysis that all "gray" areas concerning the goal(s) of the analysis should be clarified early on. For the analysis to be successful, all team members must be cooperative and have a positive outlook regarding the goals of the analysis.

6-2 FAILURE MODES AND EFFECTS ANALYSIS (FMEA) METHODOLOGY.

6-2.1 Methodology – Foundation.

To perform a FMECA the analysts must perform a FMEA first then the CA. The FMEA will then be used as the foundation of the CA. This paragraph will discuss the process flow of a FMEA, see Figure 6-2, and explain when and how to perform a FMEA at an upper system level and lower system level approach. The FMEA will identify systems and/or components and their associated failure modes. This part of the analysis will also provide an assessment of the cause and effects of each failure mode.

Figure 6-2 Typical FMEA Flow



6-2.2 Define the System to be Analyzed (Functional/Hardware Approach)

Provide schematics and operational detail of the system. Clarify the mission of the system or the goal of the system. The mission may be to provide emergency power or maintain a certain temperature to the facility. Whatever it is, it must be identified prior to analysis. Identify failure definitions, such as conditions which constitute system failure or component failure.

6-2.2.1 System Indenture Levels.

The system indenture levels must be identified. Figure 6-3 depicts typical system indenture levels. At these system indenture levels; a functional approach is usually applied. Each system's function is known and possibly the major pieces of equipment are known. However, it is possible to conduct a hardware analysis to these levels as well. But they must begin at the lower levels and propagate them up to the higher system levels. An example of the hardware approach is shown in Figure 6-4.

Figure 6-3 Functional Method

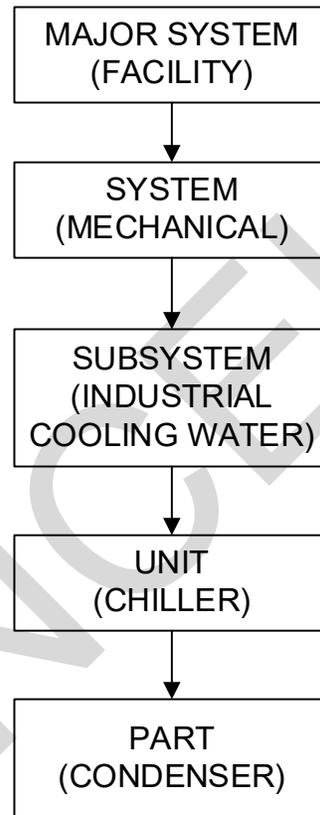
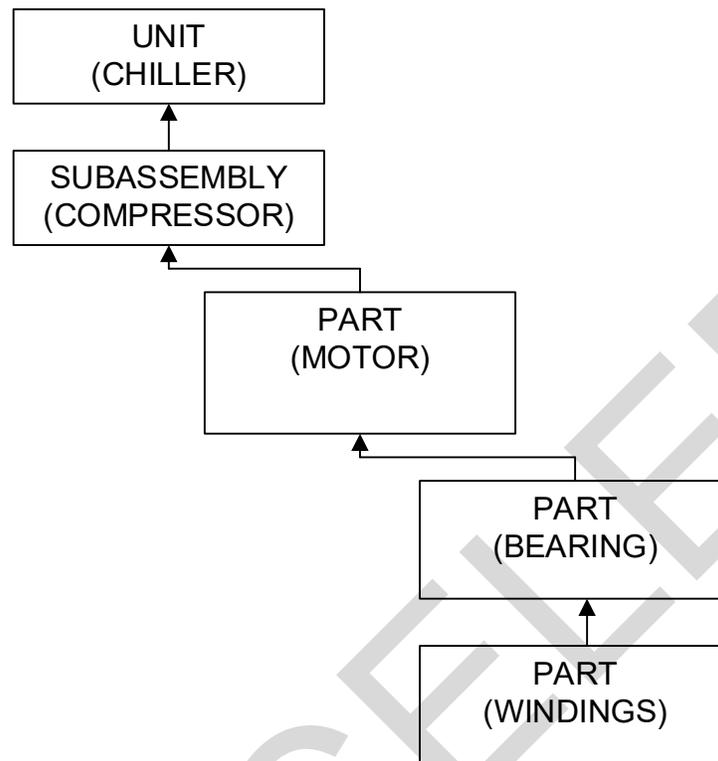


Figure 6-4 Hardware Method



6-2.2.2 Functional Approach.

Early in a design, the functional approach will be used to analyze a system's or sub-system's affects on the specified mission. This approach is performed from the upper system level down to quickly provide a general assessment of the major system's requirements to meet mission objectives. Specific parts or components are initially unknown. Once the major components are known a hardware approach can be conducted as well. This type of analysis is conducted at the indenture levels shown in Figure 6-4. To perform a functional FMEA the analyst will need:

- System definition and functional breakdown
- Block diagrams of the system
- Theory of operation
- Ground rules and assumptions including mission requirements
- Software specifications

6-2.2.3 Define and Identify.

The analyst performing a functional FMEA must be able to define and identify each system function and its associated failure modes for each functional output. Redundant components are typically not considered at the upper levels. The failure mode and effects analysis is completed by determining the potential failure modes and failure causes of each system function. For example, the possible functional failure modes of a pump are pump does not transport water; pump transports water at a rate exceeding requirements; pump transports water at a rate below requirements.

6-2.2.4 Failure Mechanisms or Causes.

The failure mechanisms or causes would be motor failure; loss of power; over voltage to motor; degraded pump; motor degraded; and, under voltage to motor.

6-2.2.5 Observing.

The functional approach should start by observing the effects of each major system, heating, ventilation, and air conditioning (HVAC) and power generation/distribution, has on each other. The next level down would analyze either just the required components within the HVAC or the required components of the power generation/distribution.

6-2.2.6 Functional FMEA.

The functional FMEA is crucial to the success of understanding the equipment and to determine the most applicable and effective maintenance. Once failure rates on each component within each system can be established, they are added up to assign a failure rate of the system. This failure rate will aid in determining where redundant components are required.

6-2.2.7 Hardware Approach.

The hardware approach is much more detailed. It lists individual hardware or component items and analyzes their possible failure modes. This approach is used when hardware items, such as what type of motors, pumps, cooling towers, or switchgear, can be uniquely identified from the design schematics and other engineering data.

6-2.2.8 Hardware Failures.

The possible hardware failure modes for a pump could be pump will not run; pump will not start; and, pump is degraded. The mechanisms would be motor windings are open; a coupling broke; starter relay is open; loss of power; impeller is worn; and, seal is leaking.

6-2.2.9 Bottom-Up.

The hardware approach is normally used in a bottom-up manner. Analysis begins at the lowest indenture level and continues upward through each successive higher indenture level of the system. This type of analysis is usually the final FMEA for the design. To perform a hardware FMEA the analyst will need:

- Complete theory or knowledge of the system
- RBDs/functional block diagrams
- Schematics
- Bill of materials/parts list
- Definitions for indenture levels
- Ground rules and assumptions including mission requirements

6-2.2.10 Utilizing Both Hardware and Functional Approaches.

Depending on the complexity of the system under analysis, it is sometimes necessary to utilize both the hardware and functional approach. The major difference between the two approaches is the amount of “parts” the component has and the descriptions of the failure modes. The failure mode description for a functional approach is a functional description whereas the hardware approach may identify a particular part that failed.

6-2.2.11

To help the reader understand the FMEA and FMECA results, the analyst must clearly document the ground rules and/or assumptions made when performing each part of the analysis. The ground rules generally apply to the system/equipment, its environment, mission, and analysis methods. Ground rules require customer approval and generally include:

- a. The mission of the item being analyzed (example: Power-Electricity)
- b. The phase of the mission the analysis will consider (example: Main Power Outage)
- c. Operating time of the item during the mission phase (example: Run Time of Generators)
- d. The severity categories used to classify the effects of failure
- e. Derivation of failure mode distributions (vendor data, statistical studies, analyst's judgment)

- f. Source of part failure rates when required (nonelectronic parts reliability data (NPRD), vendor data, Power Reliability Enhancement Program (PREP) data)
- g. Fault detection concepts and methodologies (SCADA, alarms, warnings)

6-2.2.12 Block Diagrams.

A functional and RBD representing the operation, interrelationships, and interdependencies of functional entities of the system should be constructed. The block diagrams provide the ability to trace the failure mode effects through each level of indenture. The block diagrams illustrate the functional flow sequence as well as the series or parallel dependence or independence of functions and operations.

6-2.2.12.1 Item Input and Output.

Each input and output of an item should be shown on the diagrams and labeled. A uniform numbering system which is developed for the functional system breakdown order is essential to provide traceability through each level of indenture.

6-2.2.12.2 Functional Block Diagram.

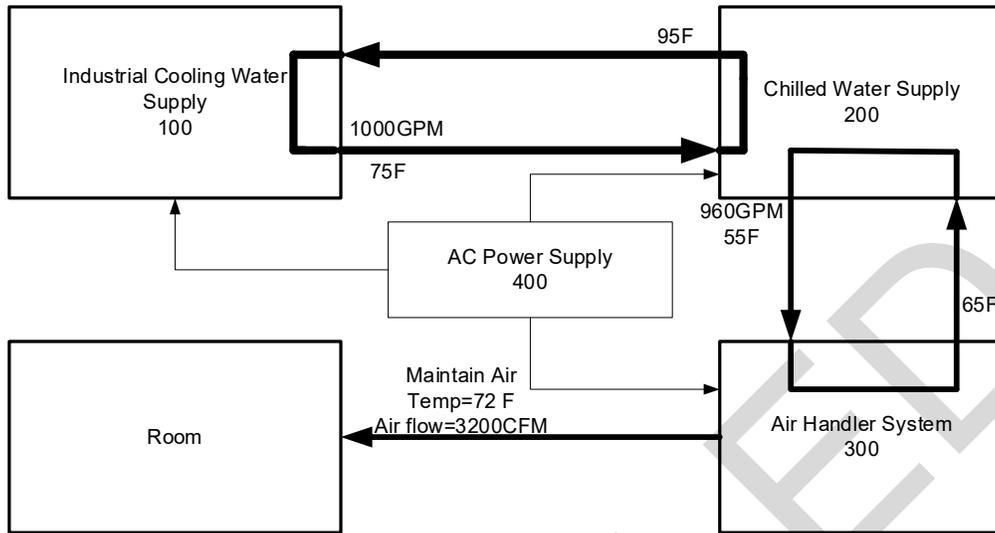
The functional block diagram shows the operation and interrelationships between functional parts of the system as defined by the schematic drawings and engineering data. It depicts the system functional flow, the indenture level of analysis, and the present hardware indenture level. This type of diagram should be used for hardware and functional FMEAs.

6-2.2.12.3 Functional Block Diagram Subsystems.

The functional block diagram in Figure 6-5 would be used at the earliest part of a design. It indicates what subsystems a facility will need to supply a room with temperature control. These subsystems are:

- (1) The Industrial Cooling Water system; used to remove the heat generated by the chiller.
- (2) The Chilled Water Supply; used to supply water at a temperature of 55°F to the Air Handling System.
- (3) The Air Handling system; used to provide air flow at 3200cfm to the room and maintain a temperature of 72°F.
- (4) AC Power Supply; used to provide power to each of the above subsystems.

Figure 6-5 Functional Block Diagram of System



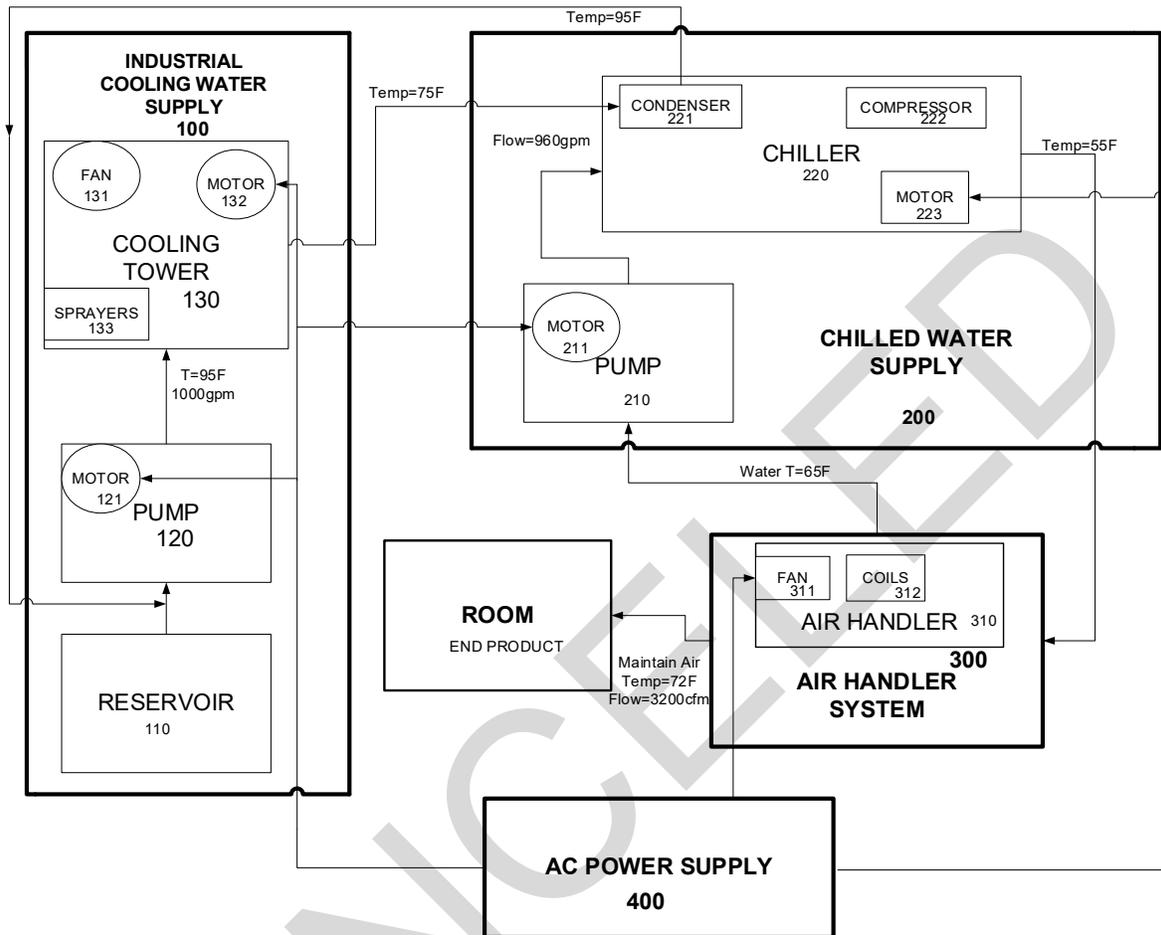
6-2.2.12.4 Functional Block Diagram Subsystem Components.

The next step is to provide a functional diagram within each sub-system indicating what types of components are required and their outputs. Figure 6-6 is an example of the same system but provides the basic components and their relationship within their system and other systems.

6-2.2.12.5 Functional or Hardware FMEA.

If a functional or hardware FMEA is to be conducted, a reliability diagram should be constructed down to the component level after the functional diagram of the system is completed. This will visually provide information to the team of any single point failures at the component level.

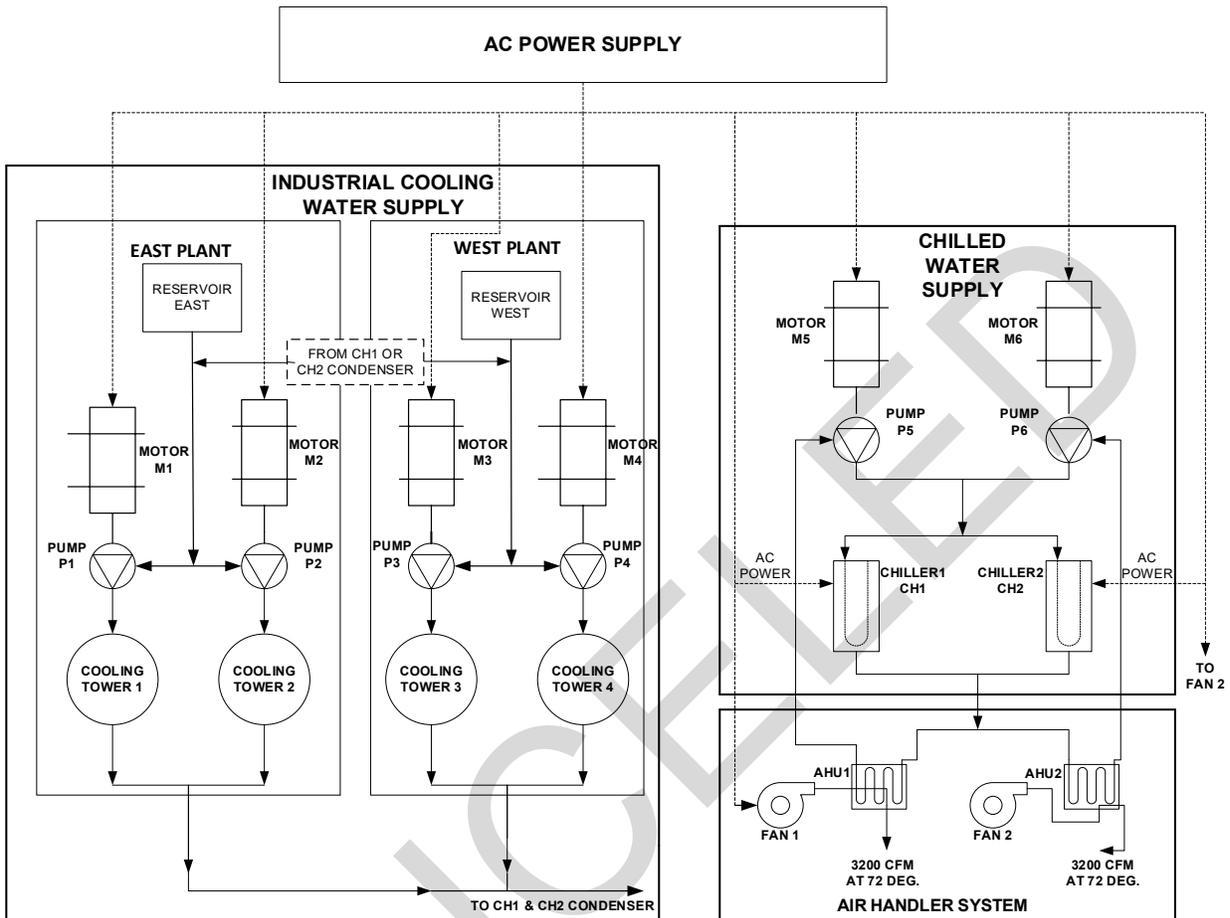
Figure 6-6 Functional Block Diagram of the Sub-Systems



6-2.2.12.6 Reliability Diagram.

The RBD of the same system is shown in Figure 6-7. It is used to illustrate the relationship of all the functions of a system or functional group. All the redundant components should be shown. This diagram should also indicate how many of the redundant components are required for the whole system to be operational. In other words, it should be stated that there may be four pumps but only two are required to accomplish the mission.

Figure 6-7 Reliability Block Diagram



6-2.2.12.7 Reliability Block Diagram Figure 6-7 Case.

In this case: one cooling tower is required from either the East or West Plant Industrial Cooling Water Supply. Either the East Plant or the West Plant is sufficient enough with one cooling tower operational for mission success.

6-2.2.12.8 Reliability Block Diagram Figure 6-7 Chilled Water and Air Handling System.

Within the Chilled Water Supply and the Air Handling System, one pump, one chiller, and one air handling unit is required to supply enough air flow and heat exchange (cooling) to the room.

6-2.2.12.9 Reliability Block Diagram Figure 6-7 AC Power Supply.

The AC Power Supply is not shown broken down for clarity reasons. This system should also be broken down similar to the "Mechanical Systems" in the HVAC. When

conducting the HVAC analysis, the AC power supply should be referenced to for possible failure mechanisms.

6-2.2.12.10 Reliability Block Diagram Figure 6-7 Blocks.

The example shown provides symbols for components, but “blocks” clearly labeled are all that is necessary to be effective. There are numerous software programs available to aid in the construction of these diagrams.

6-2.2.12.11 Entering Reliability Block Diagram Information into FMEA Sheet.

From the reliability or functional block diagram, each system, component, part number and name under analysis can now be entered in the corresponding columns of the FMEA sheet (Table 6-1, DA Form 7610). Important: The FMEA should be filled out in a column-by-column manner. Never go across the sheet. Start by filling in all the item numbers and the item names/functions before identifying the failure modes. Using this method will allow the team to stay focused and consistent when assigning inputs into each category. This should be repeated across the worksheet.

6-2.2.12.12 Entering Reliability Block Diagram Information into FMEA Sheet Exception.

The only exception to this rule is when it comes time to assign item numbers for failure modes/mechanisms. Each failure mode/mechanism identified should have its own unique number that can associate it to the component. For example, if the component number is 100 then a number assigned to the mechanism should be 100.1 or 100.01 depending on how many failure modes/mechanisms are possible for the item. This is shown in Table 6-2.

6-2.2.12.13 HVAC System Components.

The components that make up the HVAC system in a typical facility are AC power; industrial cooling water; chilled water supply; and, air handling/heat exchanger.

6-2.2.12.14 Industrial Cooling Water Sample FMEA Worksheet.

A sample FMEA worksheet for just the industrial cooling water is presented in Table 6-1 to indicate the flow of the process using DA Form 7610, Failure Modes and Effects Analysis.

Table 6-1 Example of DA Form 7610, FMEA Worksheet Flow (One Column at a Time)

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)										
SYSTEM: Mechanical System							DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply							SHEET: 1 of 1			
REFERENCE DRAWINGS:							COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room							APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
100	Ind cool water /supply water to condenser at 75° F & 1000GPM									

DA FORM 7610, AUG 2006

Table 6-2 Example of DA Form 7610, Functional FMEA System Level

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)										
SYSTEM: Mechanical System							DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply							SHEET: 1 of 1			
REFERENCE DRAWINGS:							COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room							APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
100.0	Ind cool water /supply water to condenser at 75° F & 1000GPM	Provide water greater than 75° F	Cooling tower malfunction, pump degraded, fan will not start							
100.1		Provide water less than 75° F	Fan will not turn off							
100.2		Provide water less than 1000GPM	Degraded pump							
100.3		Provide no water	Broken pipe							
100.4			Blockage in pipe or pump failure							

DA FORM 7610, AUG 2006

6-2.3 Failure Mode Identification.

The failure mode is the manner that a failure is observed in a function, subsystem, or component. There are many modes a component or system may fail. Failure modes of concern depend on the specific component, system, environment, and history of failures in similar systems. All probable independent failure modes for each item should be identified.

6-2.3.1 Conditions to be Examined.

To assure that a complete analysis has been performed, each component failure mode and/or output function should be examined for the following conditions:

- Failure to operate at the proper time
- Intermittent operation
- Failure to stop operating at the proper time
- Loss of output
- Degraded output or reduced operational capability

6-2.3.2 Functional Approach of Analyzing System.

The example used in Table 6-6 is a functional approach of analyzing the upper system level's ability to perform its intended function. The systems were identified in the functional block diagram as: industrial cooling water supply; chilled water system; air handling system; and the AC power supply. All failure modes of specific components are not analyzed. Only the system's ability to perform a function is evaluated. As the analysis steps down a level, a specific component can be identified and then a failure mechanism(s) associated with the component can be analyzed as is shown in Table 6-7.

6-2.3.3 Failure Mode Cause or Failure Mechanism.

The cause or failure mechanism of a failure mode is the physical or chemical processes that cause an item to fail. It is important to note that more than one failure cause is possible for any given failure mode. All causes should be identified including human induced causes. These can occur more frequently when initiating a redundant system upon a failure of the primary system. When analyzing the cause of each failure mode one should be careful not to over analyze why a part failed. For example, failure mode-bearing seized:

(1) Why did it seize? – Contamination was in the bearing.

(2) Why was there contamination? – Seal was cracked.

(3) Why was the seal cracked? – Scheduled PM could not be completed.

(4) Why was seal not replaced? – Because there were none in stock.

6-2.3.4 Root Cause.

The root cause should be the "seal was cracked". By analyzing further, the cause can be chased "out of bounds". The analysts must use their judgment to decide how far to investigate root causes while considering economical constraints and probability of failure vs mission criticality and acceptable risks.

6-2.4 Failure Effects Analysis.

A failure effects analysis is performed on each item of the RBD. The consequence of each failure mode on item operation, and the next higher levels in the block diagram should be identified and recorded. The failure under consideration may affect several indenture levels in addition to the indenture level under analysis. Therefore, local, next higher and end effects are analyzed. Failure effects must also consider the mission objectives, maintenance requirements and system/personnel safety.

6-2.4.1 Failure Effect Levels.

Example failure effect levels are shown in Table 6-3 and are defined as follows:

(1) Local effects are those effects that result specifically from the failure mode of the item in the indenture level under consideration. Local effects are described to provide a basis for evaluating compensating provisions and recommending corrective actions. The local effect can be the failure mode itself.

(2) Next higher-level effects are those effects which concentrate on the effect of a particular failure mode has on the operation and function of items in the next higher indenture level.

(3) End effects are the effects of the assumed failure on the operation, function and/or status of the system.

6-2.4.2 Item Failures.

Example end or system level effects of item failures are also shown in Table 6-3 and generally fall within one of the following categories:

(1) System failure where the failed item has a catastrophic effect on the operation of the system.

(2) Degraded operation where the failed item has an effect on the operation of the system, but the system's mission can still be accomplished.

(3) No immediate effect where the failed item causes no immediate effects on the system operation.

6-2.4.3 Assigning the Effect.

Try to be specific when assigning the effect. The above items are just categories and are not intended to be the only input for "end effect". Detailed effects will provide the analyst the most useful information later in the analysis.

6-2.4.4 System Level Failures.

Failures (shown in Table 6-3) at the system level are those failures which hinder the performance or actual completion of the specified mission. Failures at each indenture level is defined below.

(1) A major system failure would be failure in the main mission of the facility. A failure at the major system level would be defined as the inability to command, control, & communicate.

(2) A system failure of a mechanical system. A failure at the system level would be defined as the inability of the mechanical system to cool the facility to within a minimally acceptable temperature range allowed for the computers.

(3) A subsystem failure would be failure of the industrial cooling water. A failure at the subsystem level would be defined as the inability to provide cooling water to the facility.

(4) A component failure would be failure of a chiller. A failure at the system component level could be defined as the inability of the chiller to provide chilled water.

(5) A sub-component failure would be the failure of a condenser. A failure at the sub-component level would be defined as the inability of the condenser to remove heat from the water supply.

6-2.4.5 Typical Entries into the Failure Effects Categories.

Table 6-3 provides an example of typical entries into the failure effects categories. Remember to be as specific as necessary so that anyone who reads this will be able to decipher what the effects are without asking questions. Note the progression of one column at a time.

Table 6-3 Example of DA Form 7610, FMEA Progression

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)										
SYSTEM: Mechanical System							DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply							SHEET: 1 of 1			
REFERENCE DRAWINGS:							COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room							APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
100.0	Ind cool water /supply water to condenser at 75° F & 1000GPM	Provide water greater than 75° F	Cooling tower malfunction, pump degraded, fan will not start	The required amount of heat is not removed from water	Condenser not efficient, Chiller will use more energy \$\$	Air temp may rise but not significant				
100.1		Provide water less than 75° F	Fan will not turn off	Too much cooling will take place	Chiller will be less efficient and use more energy	No effect to air temp				
100.2		Provide water less than 1000GPM	Degraded pump	Pump will not be able to provide enough flow or pressure	Condenser not efficient, Chiller will use more energy	Air temp may rise but not significant				
100.3		Provide no water	Broken pipe	Excess water consumption, isolation actions will be required	Condenser in chiller will not function, Chiller will overheat	Air temp will rise above maximum allowed mission				
100.4			Blockage in pipe or pump failure	No water will be provided through the system	Condenser in chiller will not function, Chiller will overheat	Air temp will rise above maximum allowed mission				

DA FORM 7610, AUG 2006

6-2.5 Failure Detection Methods.

The FMEA identifies the methods by which occurrence of failure is detected by the system operator. Visual or audible warnings devices and automatic sensing devices, such as a SCADA system, are examples of failure detection means. Any other evidence to the system operator that a system has failed should also be identified in the FMEA. If no indication exists, it is important to determine if the failure will jeopardize the system mission or safety. If the undetected failure does not jeopardize the mission objective or safety of personnel and allows the system to remain operational a second failure situation should be explored to determine whether an indication will be evident to the operator or maintenance technician.

6-2.5.1 Failure Detection Methods – Indications.

These indications can be described as follows:

- (1) A normal indication is an indication to the operator that the system is operating normally.
- (2) An abnormal indication is an indication to the operator that the system has malfunctioned or failed. (alarm-chiller overheated)
- (3) An incorrect indication is an erroneous indication to the operator that a malfunction has occurred when there is no fault. Conversely, an indication that the system is operating normally when, in fact, there is a failure.

6-2.5.2 Periodic Testing.

Periodic testing of stand-by equipment would be one method used to detect a hidden failure of the equipment. This testing helps to assure that the stand-by equipment will be operational at the inopportune time the primary equipment fails. The ability to detect a failure to reduce the overall effect will influence the severity of the failure. If the detection method does not reduce the overall effect, then the severity will not be influenced. The analysts should explore an alternative method for detection if this is the case.

6-2.5.3 Failure Mode Detection Prior to Occurring.

Typically, if the failure mode can be detected prior to occurring, the operator can prevent further damage to the system or take some other form of action to minimize the effect. An "over-temperature" alarm for a compressor would be an example. If the compressor had a loss of lubrication and was overheating, the alarm/SCADA would shut that chiller down prior to seizure. If the compressor were allowed to run to seizure, costly damage would occur, and the system would not be able to function.

6-2.6 Compensating Provisions.

Compensating provisions are actions that an operator can take to negate or minimize the effect of a failure on the system. Any compensating provision built into the system that can nullify or minimize the effects of a malfunction or failure must be identified.

6-2.6.1 Examples of Design Compensating Provisions.

Examples of design compensating provisions are:

- (1) Redundant item that allows continued and safe operation.
- (2) Safety devices such as monitors or alarm systems that permit effective operation or limit damage.
- (3) Automatic self-compensating devices that can increase performance as unit degrades such as variable speed drives for a pump.
- (4) Operator action such as a manual over-ride.

6-2.6.2 Multiple Compensating Provisions.

When multiple compensating provisions exist, the compensating provision which best satisfies the fault indication observed by the operator must be highlighted. The consequences of the operator taking the wrong action in response to an abnormal indication should also be considered and the effects of this action should be recorded in the remarks column of the worksheet.

6-2.6.3 Ability to Detect a Failure and React.

To be able to detect a failure and react correctly can be extremely critical to the availability of the system. For example, if a failure is detected in the primary pump (no flow) then the operator/technician must know what buttons and/or valves to actuate to bring in the backup pump. If by chance the operator/technician inadvertently actuates the wrong valve, there may be undesirable consequences because of their actions. This is a basic example but should be considered in the analysis on all failure modes.

6-2.7 Severity Rankings.

After all failure modes and their effects on the system have been documented in the FMEA the team now needs to provide a ranking of the effect on the mission for each failure mode. Make sure that prior to assigning these rankings that all prior columns of the FMEA are filled in. This will help the analyst in assigning each severity ranking relative to each other. This ranking will be used later in the CA to establish relative "severity" rankings of all potential failure modes.

6-2.7.1 Evaluating Item Failure Mode.

Each item failure mode is evaluated in terms of the worst potential consequences upon the system level which may result from item failure. A severity classification must be assigned to each system level effect. A lower ranking indicates a less severe failure effect. A higher ranking indicates a more severe failure effect. Severity classifications provide a qualitative measure of the worst potential consequences resulting from an item failure.

6-2.7.2 Assigning Severity Classification.

A severity classification is assigned to each identified failure mode and each item analyzed in accordance with the categories in Table 6-4.

Table 6-4 Severity Ranking Table

Ranking	Effect	Comment
1	None	No reason to expect failure to have any effect on Safety, Health, Environment or Mission.
2	Very Low	Minor disruption to facility function. Repair to failure can be accomplished during trouble call.
3	Low	Minor disruption to facility function. Repair to failure may be longer than trouble call but does not delay mission.
4	Low to Moderate	Moderate disruption to facility function. Some portion of Mission may need to be reworked or process delayed.
5	Moderate	Moderate disruption to facility function 100% of Mission may need to be reworked or process delayed .
6	Moderate to High	Moderate disruption to facility function. Some portion of Mission is lost. Moderate delay in restoring function.
7	High	High disruption to facility function. Some portion of Mission is lost. Significant delay in restoring function.
8	Very High	High disruption to facility function. All of Mission is lost. Significant delay in restoring function
9	Hazard	Potential Safety, Health, or Environmental issue. Failure will occur with warning
10	Extreme Hazard	Potential Safety, Health, or Environmental issue. Failure will occur without warning

6-2.7.3 Items with High Severity.

Although this chart can be used for a qualitative (without data) analysis or a quantitative (with data) analysis, some facilities may choose the following categories to assign another familiar format of severity classifications for the quantitative CA, Table 6-5. These categories are used to "flag" the analysts to items with high severity.

6-2.7.4 Items with High Severity.

Although this chart can be used for a qualitative (without data) analysis or a quantitative (with data) analysis, some facilities may choose the following categories to assign another familiar format of severity classifications for the quantitative CA, Table 6-5. These categories are used to "flag" the analysts to items with high severity.

Table 6-5 Severity Classification for Qualitative CA

Category	Effect	Comment
I	Minor	A failure not serious enough to cause injury, property damage or system damage, but which will result in unscheduled maintenance or repair.
II	Marginal	A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation.
III	Critical	A failure which may cause severe injury or major system damage which will result in mission loss. A significant delay in restoring function to the system will occur.
IV	Catastrophic	A failure which may cause death or lack of ability to carry out mission without warning (power failure, over-heating).

6-2.7.5 Exception when using Qualitative Analysis.

Do not use this method to categorize severity in a qualitative analysis. The qualitative analysis requires an equal scale (such as 1 through 10, or 1 through 5) for both severity and occurrence. If they are not equal, one category will hold more "weight" than the other in the CA.

6-2.7.6 System Level vs Component Level Severity.

A FMEA at the component level will have high severity rankings because there is no redundancy at that level. At the system level, however, the severity may decrease because when there is loss of one component in the system, there is a backup in place. The mission of the system at this indenture level is not compromised assuming the backup component or system is functional.

6-2.7.7 Special Remarks or Components.

If there are any special remarks or comments that need to be recorded should be included in the "REMARKS" category at the end of the FMEA. This should include specific hazards or explanations of the failure mode effects or other categories associated with it.

6-2.7.8 Example of a Completed FMEA.

An example of a completed functional FMEA of only the Industrial Cooling Water Supply is provided in Table 6-6. Hardware FMEA's on all the systems are shown in Table 6-7. Notice that the functional FMEA did not include any redundancy as a consideration when assigning the effects.

6-2.8 Results of FMEA.

The team should now review the information on the FMEA to determine if any changes should be made. It is not uncommon for people to think of more failure modes or detection methods on items during the process. Make these changes or additions prior to proceeding on to the CA.

6-2.8.1 Critical Analysis Foundation.

Once all the information has been entered into the FMEA, the foundation for the CA has been established. The FMEA sheet will be referenced while creating the CA. Due to the amount of information on the FMEA, it is not feasible to include all of it on the CA.

6-2.8.2 FMEA on Subsystems Example.

In this example, a FMEA should also be conducted on the remaining systems of the HVAC System: the chilled water supply; the air handling system; and the AC power supply system.

6-2.8.3 Applying Critical Analysis to Example.

Once they are completed the steps discussed in the next paragraph for the CA should be applied to complete the FMECA process.

Table 6-6 Example of DA Form 7610, Completed FMEA (functional) for Industrial Water Supply

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)										
SYSTEM: Mechanical System							DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply							SHEET: 1 of 1			
REFERENCE DRAWINGS:							COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room							APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
100.0	Ind cool water /supply water to condenser at 75° F & 1000GPM	Provide water greater than 75° F	Cooling tower malfunction, pump degraded, fan will not start	The required amount of heat is not removed from water	Condenser not efficient, Chiller will use more energy \$\$	Air temp may rise but not significant	Temp sensor/water analysis	SCADA indicator	6	If drainpipe breaks the secondary containment will be filled
100.1		Provide water less than 75° F	Fan will not turn off	Too much cooling will take place	Chiller will be less efficient and use more energy	No effect to air temp	Alarm temp sensor	SCADA indicator	2	
100.2		Provide water less than 1000GPM	Degraded pump	Pump will not be able to provide enough flow or pressure	Condenser not efficient, Chiller will use more energy	Air temp may rise but not significant	Flow/pressure sensor	SCADA indicator	10	
100.3		Provide no water	Broken pipe	Excess water consumption, isolation actions will be required	Condenser in chiller will not function, Chiller will overheat	Air temp will rise above maximum allowed mission	Inspection	SCADA indicator	4	Safety hazard when pipe ruptures injury could occur
100.4			Blockage in pipe or pump failure	No water will be provided through the system	Condenser in chiller will not function, Chiller will overheat	Air temp will rise above maximum allowed mission	Water analysis or flow/pressure sensor	SCADA indicator	5	In case of blockage, a secondary path may be available

DA FORM 7610, AUG 2006

Table 6-7 Example of DA Form 7610, Completed FMEA (hardware) for HVAC System

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)										
SYSTEM: Mechanical System							DATE (YYYYMMDD): 20050819			
PART NUMBER: HVAC System							SHEET: 1 of 3			
REFERENCE DRAWINGS: C-20005-B							COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room							APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
110.0	Reservoir/contains 6000 gallons of water	Leak;	Crack in wall, Drainpipe broke	Water will not be contained	Lower condenser efficiency. Chiller uses more energy	No immediate effect	Inspection	SCADA Redundant reservoir	4	
120.0	Pump #1/ Transport Industrial water supply at 1000GPM	Transport water at a rate below 1000GPM	Impeller degraded, gasket leak, motor degraded	Pump can-not produce required rate of water	Lower condenser efficiency. Chiller uses more energy	No immediate effect	Flow sensor	SCADA Redundant system	4	
120.1		Produce no water flow	Broken coupling, leak on suction line, motor inoperable	Pump will not be able to pump	No condenser function. Chiller will lose ability to remove heat	Room temp above max allowed temp Mission failure	Flow sensor	SCADA Redundant system	5	
130.0	Cooling Tower #1/ maintain a water temp of 75°F	Scaling (deposits) on media	Untreated water	Fan will operate longer period of time. Poor cooling	Lower condenser efficiency. Chiller uses more energy	Room temperature will rise slightly	Inspection/ water analysis	SCADA Redundant system	6	
130.1		Clogged sprayers	Untreated/ unfiltered water	Water will not be cooled	Condenser will not be efficient	Room temperature will rise slightly	Inspection/ water analysis	SCADA Redundant system	5	

DA FORM 7610, AUG 2006

Table 6-7 Example of DA Form 7610, Completed FMEA (hardware) for HVAC System (cont'd)

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)										
SYSTEM: Mechanical System							DATE (YYYYMMDD): 20050819			
PART NUMBER: HVAC System							SHEET: 1 of 3			
REFERENCE DRAWINGS: C-20005-B							COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room							APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
130.2		Fan failure	Motor winding open, No supply voltage to motor	Low evaporative cooling will take place	Lower condenser efficiency. Chiller uses more energy	Slight rise in air temp. No severe effect. Mission compromised	Flow sensor	Redundant system	4	
210.0	Pump #5/ Transport Industrial water supply at 960GPM	Degraded operation – produce water at rate less than 960GPM	Impeller degraded, gasket leak, motor degraded	Pump can-not produce required rate of water	Chiller needs to decrease water temp to satisfy air handler	No effect	Flow sensor	Redundant system	4	
210.1		Produce no water flow	Broken coupling, leak on suction line, motor inoperable	Damage to motor or pump shafts	Chiller will not be able to remove heat from water	No air-cooling Room temp above max. Mission failure.	Flow sensor	Redundant system	5	
220.0	Chiller/ Remove heat(10°F) from chilled water supply	Degraded operation – remove less than 10°F	Refrigerant leak degraded compressor, tube leak, dirty coil	Compressor will cycle on frequently/ chiller will be less efficient	Air handling unit will run continuously trying to meet demand	Air temp will rise but not above maximum allowed.	Temp sensor	Redundant chiller	5	
200.1		Remove no heat	Compressor seizure, motor failure	Chiller will be unable to function	Air handling unit will run continuously trying to meet demand	Minimal air cooling-temp rise above max. Mission failure	Temp sensor	Redundant chiller	7	This failure is costly and time consuming to repair.

DA FORM 7610, AUG 2006

6-3 CRITICALITY ANALYSIS (CA) METHODOLOGY.

6-3.1 Methodology – Moving into Criticality Analysis.

The FMECA is composed of two separate analyses, the FMEA and the CA. The FMEA must be completed prior to performing the CA. It will provide the added benefit of showing the analysts a quantitative ranking of system and/or subsystem failure modes. The CA allows the analysts to identify reliability and severity related concerns with particular components or systems. Even though this analysis can be accomplished with or without failure data, there are differences on each approach which are discussed in the following paragraphs. Figure 6-8 shows the process for conducting a FMECA using quantitative and qualitative means.

6-3.2 Criticality Analysis.

The CA provides relative measures of significance of the effects of a failure mode, as well as the significance of an entire piece of equipment or system, on safe, successful operation and mission requirements. In essence, it is a tool that ranks the significance of each potential failure for each component in the system's design based on a failure rate and a severity ranking. This tool will be used to prioritize and minimize the effects of critical failures early in the design.

6-3.2.1 Quantitative or Qualitative Approach.

The CA can be performed using either a quantitative or a qualitative approach. Tables 6-8 and 6-9 identify the categories for entry into their respective CA using DA Forms 7611 and 7612, respectively. Availability of part configuration and failure rate data will determine the analysis approach. As a general rule, use Table 6-8 when actual component data is available and use Table 6-9 when no actual component data or only generic component data is available.

6-3.2.2 Levels of Data.

Figure 6-9 is a representation of the different levels of data that a facility may have. Depending on the level of data available, the analysts must determine which approach they will use for the CA. The areas where there are overlaps between quantitative and qualitative, the analyst will have to assess what the expectations are for conducting the analysis to determine which approach will be used.

Figure 6-8 FMECA Flow

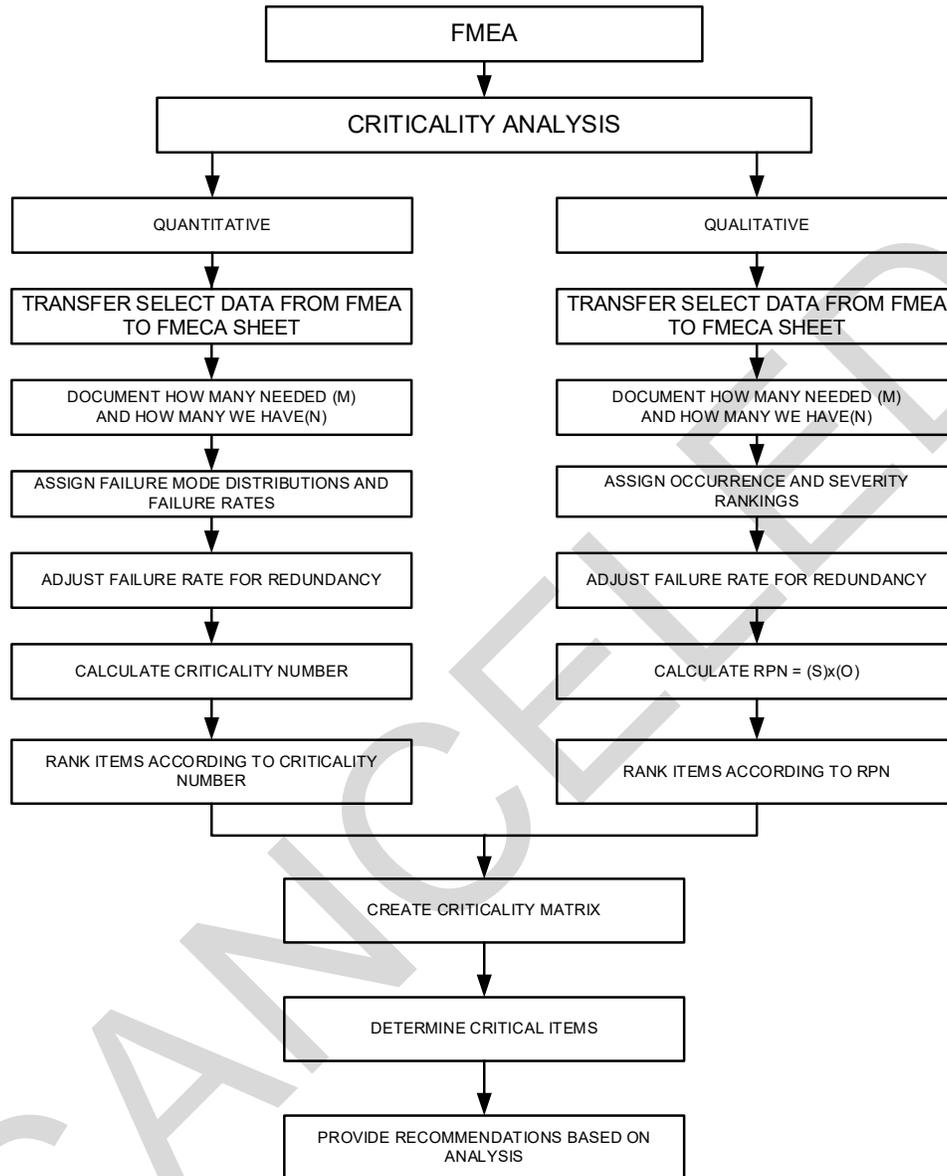


Table 6-8 Example of DA Form 7611, FMECA Worksheet – Quantitative

QUANTITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

For use of this form, see TM 5-698-4; the proponent agency is USACE.

SYSTEM: Mechanical System

DATE (YYYYMMDD): 20050819

PART NUMBER: Industrial Water Supply

SHEET: 1 of 1

REFERENCE DRAWINGS:

COMPLIED BY: AAA

MISSION: Provided Temperature Control to Room

APPROVED BY: BBB

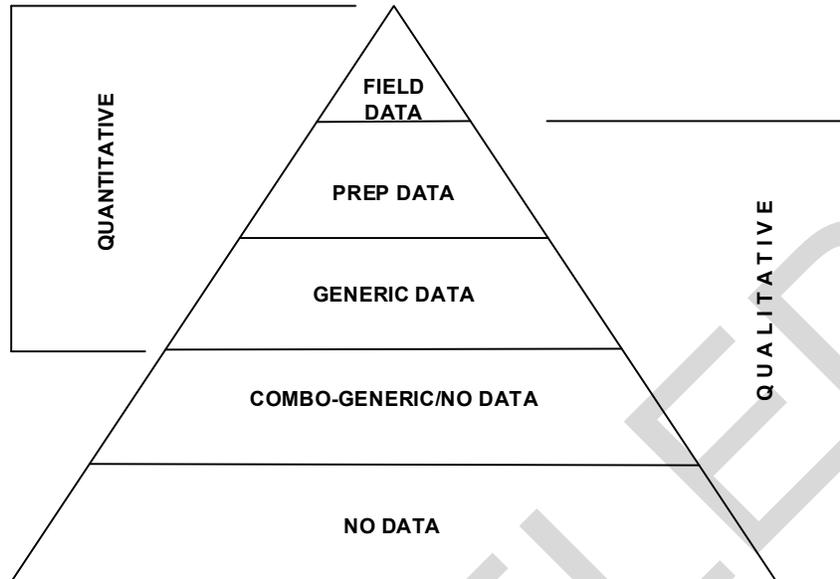
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	REDUNDANCY		FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	FAILURE MODE CRITICALITY NUMBER (C_p)	ITEM CRITICALITY NUMBER (ϵC_p)	REMARKS
					HAVE (N)	NEED (M)							

Table 6-9 Example of DA Form 7611, FMECA Worksheet – Qualitative

QUALITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)												
SYSTEM: Mechanical System										DATE (YYYYMMDD): 20050819		
PART NUMBER: Industrial Water Supply										SHEET: 1 of 1		
REFERENCE DRAWINGS:										COMPLIED BY: AAA		
MISSION: Provided Temperature Control to Room										APPROVED BY: BBB		
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM			REMARKS AND/OR RECOMMENDED ACTIONS	
					OCCUR	SEVERITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR		SEVERITY

DA FORM 7611, AUG 2006

Figure 6-9 Data Triangle



(1) Quantitative method is used when failure rates, failure modes, failure mode ratios, and failure effects probabilities are known. These variables are used to calculate a "criticality number" to be used to prioritize items of concern. This is used typically after the design has been completed when confident data on the system can be collected. However, in certain instances data may be available from other sources. This type of analysis will provide concrete figures which can be used for other types of analyses including FTA and RCM program.

(2) Qualitative method is used when no known failure rates and failure modes are available. The criticality or risk associated with each failure is subjectively classified by the team members. The use of a subjective ranking system is applied to the severity, and occurrence of the failures. This method will provide a relative ranking of item failure mode's effects for identifying areas of concern and for initiating other analyses such as RCM, fault tree, and logistics. As the system matures it is recommended that data be collected to enhance the analysis through a quantitative method.

6-3.3 Transfer Select Data from FMEA.

The information from the FMEA sheet that will be used in the FMECA worksheet will aid in developing the CA. Given the fact that not all the information will be shown on the FMECA sheet, does not mean that the excluded information will be ignored. The FMEA sheet will still be referenced frequently for data.

(1) All of the information on the FMEA can sometimes be difficult to read. This can be a major contributing factor to not include all information. This is just a suggestion that may or may not be desirable at every facility. In fact, some facilities may choose to add more

categories. Keep in mind, this UFC is just a guide and is meant to be flexible to achieve the objective of the analysis.

(2) Once it is determined which type of analysis will be conducted, qualitative or quantitative, the appropriate FMECA worksheet can be chosen. Examples of FMECA sheets for the two different types of analyses are provided in Tables 6-8 and 6-9.

(3) The following categories will be transferred from the FMEA sheet:

- Item Number
- Item/Functional ID
- Failure Modes
- Failure Mechanisms
- Failure Effects (qualitative only due to space limitations)
- Severity Classification/Ranking

(4) All other categories from the FMEA will be referenced during the CA.

6-3.4 Quantitative Criticality Analysis.

Once it is determined that sufficient failure rate data and failure mode distributions are available, a criticality worksheet for conducting a quantitative analysis that looks like Table 6-8 will be used. Note that some of the categories are derived from the FMEA sheet. The additional categories will be used to calculate the criticality number. Traditional methods will be used to derive this number except where redundant components are used, which is typical with a C5ISR facility. The required number of components necessary (M) to perform the function and the amount of components that are redundant (N) should be recorded. The effect of redundancy will be discussed in paragraph 6-3.5. A description of each category and variable used in the CA is listed below.

6-3.4.1 Beta.

Beta (β) is defined as the failure effect probability and is used to quantify the described failure effect for each failure mode indicated in the FMECA. The beta (β) values represent the conditional probability or likelihood that the described failure effect will result in the identified criticality classification, given that the failure mode occurs. The β values represent the analyst's best judgment as to the likelihood that the loss or end effect will occur. For most items the failure effect probability (β) will be one. An example would be if the generator engine shuts down (failure mode), it can be confidently stated that 100% of the time the effect will be loss of power.

(1) However, if the failure mode was that the generator produces low voltage (brown out condition), the end effect could vary. Effects such as degraded motor function or motor burns up condition on various pieces of equipment could occur. Therefore, there are two possible effects for the generator's failure mode low voltage: degraded motor function and motor burns up.

(2) Now the analyst must make a judgment call of what percentage of time or probability each effect may occur. If the analyst determined that 80% of the time the motor is degraded, then beta (β) for that effect would be (.80). This would leave 20% of the time the effect would be motor burns up and would be assigned a beta (β) of (.20).

6-3.4.2 Alpha.

Alpha (α) is the probability, expressed as a decimal fraction, that the given part or item will fail in the identified mode. If all the potential failure modes for a device are considered, the sum of the alphas will equal one. Determining alpha is done as a two-part process for each component being analyzed. First, the failure modes are determined and secondly, modal probabilities are assigned.

(1) Modal failures represent the different ways a given part is known, or has been "observed", to fail. It is important to make the distinction that a failure mode is an "observed" or "external" effect so as not to confuse failure mode with failure mechanism. A failure mechanism is a physical or chemical process flaw caused by design defects, quality defects, part misapplication, wear out, or other processes. It describes the basic reason for failure or the physical process by which deterioration proceeds to failure.

(2) For example, when there is no air flow from an air handling unit caused by a broken belt. In this example, the failure mode would be the "no air flow from air handling unit" while the failure mechanism would be the "broken belt". Another failure mode could be low air flow and the mechanism would be belt slippage (loose belt).

(3) Once common part failure modes have been identified, modal probabilities (α) are assigned to each failure mode. This number represents the percentage of time, in decimal format, that the device is expected to fail in that given mode. This number is given as a percentage of the total observed failures. Using the air handler example, the probabilities of occurrence for each failure mode are shown in Table 6-10.

Table 6-10 Failure Mode Ratio (α)

Part Failure Modes	Failure Mode Ratio (α)
Blows to little air	0.55 or 55%
Blows too much air	0.05 or 5%
Blows no air	0.40 or 40%
The sum of modal probabilities is	1.00 or 100%

Note: These are hypothetical failure mode ratios.

(4) Alpha and beta are commonly confused. It is best to memorize that alpha is the failure mode ratio, the percentage of time how or in what manner an item is going to fail. However, beta is the conditional probability of a failure effect occurring given a specific failure mode; when a failure mode occurs, what percentage of time is this going to be the end effect. Beta typically is assigned 1 to only consider the worst possible end effect as a result of a failure mode.

6-3.4.3 Failure Rate.

The failure rate (λ_p) of an item is the ratio between the numbers of failures per unit of time and is typically expressed in failures per million hours or failures/ 10^6 hours. Although failure data compiled from actual field test are recommended, other sources for failure information are available for use until actual field data can be obtained.

(1) When analyzing system failure rates where redundant like components are used to accomplish a mission, the failure rate must be adjusted to reflect the “system failure rate”. This is explained in paragraph 6-3.5. When entering in the failure rate on the FMECA sheet, in parentheses it should be identified that the failure rate is the single item component failure rate or the failure rate of the redundant system. The example in this chapter provides an example of how to show this. It indicates the single failure rate and the redundant failure rate.

(2) The source of the failure rate should also be noted in this category as well so that anyone who looks at the analysis will know if the data was derived by field data or some other source for reference purposes. This will be important if someone does question the validity of the data.

6-3.4.4 Modal Failure Rate.

The modal failure rate is the fraction of the item's total failure rate based on the probability of occurrence of that failure mode. The sum of the modal failure rates for an item will equal the total item failure rate providing all part failure modes are accounted for. If there are three different failure modes, then all three failure rates (modal failure rates) will equal the item failure rate. The modal failure rate is given by the equation:

Equation 6-1. Modal Failure Rate

$$\lambda_m = \alpha \lambda_p$$

Where:

λ_m = the modal failure rate

α = the probability of occurrence of the failure mode (failure mode ratio)

λ_p = the item failure rate

6-3.4.5 Failure Mode (Modal) Criticality Number.

The failure mode criticality number is a relative measure of the frequency of a failure mode. In essence it is a mathematical means to provide a number to rank importance based on its failure rate. The equation used to calculate this number is as follows:

Equation 6-2. Failure Mode Criticality Number

$$C_m = (\beta \alpha \lambda_p t)$$

Where:

C_m = Failure mode criticality number

β = Conditional probability of the current failure mode's failure effect

α = Failure mode ratio

λ_p = Item failure rate

t = Duration of applicable mission phase (expressed in hours or operating cycles)

(1) This number is derived from the modal failure rate which was explained in paragraph 6-3.4.4. It also takes into consideration of the operating time that the equipment or system is running in hours or operating cycles.

(2) Below is an example of a centrifugal pump used for condenser water circulation. The failure rates were derived from the Non-electric Parts Reliability Data-95 (NPRD-95) publication and the failure mode probability was derived from the Failure Mode/Mechanism Distribution-97 (FMD-97) publication. The failure effect probability (β) will equal 1.

Failure mode criticality:

Component type: Centrifugal pump condenser circulation

Part number: P1

Failure rate (λ_p): 12.058 failures per million hours

Source: NPRD-95

Failure Mode probability (α):

No output (0.29)

Degraded (0.71)

Source: FMD-97

Time (t): 1 hour

Failure effect probability (β): 1

Failure mode criticality (C_m):

$$C_m = \beta \alpha \lambda_p t$$

$$C_m (\text{No output}) = (1 \times .29 \times 12.058 \times 1)$$

$$C_m (\text{No output}) = 3.5 \times 10^{-6}$$

$$C_m (\text{Degraded}) = (1 \times .71 \times 12.058 \times 1)$$

$$C_m (\text{Degraded}) = 8.56 \times 10^{-6}$$

6-3.4.6 Item Criticality Number.

Item criticality number. The item criticality number is a relative measure of the consequences and frequency of an item failure. This number is determined by totaling all the failure mode criticality numbers of an item with the same severity level. The severity level was determined in the FMEA. The equation used to calculate this number is as follows:

Equation 6-3. Item Criticality Number

$$C_r = \sum (C_m)$$

Where:

C_r = Item criticality number

C_m = Failure mode criticality number

(1) If an item has three different failure modes, two of which have a severity classification of 3 and one with a classification of 5, the sum of the two "failure mode criticality numbers" (C_m) with the severity classification of 3 would be one "item criticality number" (C_r). The failure mode with the severity classification of 5 would have an "item criticality number" equal to its "failure mode criticality number".

(2) The example below was used in the failure mode criticality example. Both failure modes for this example have the same severity classification of 3. If the severity classifications were different, then the item criticality numbers would be calculated as separate items. In this case, since there are only two failure modes, the item criticality number for each severity level would equal the failure mode criticality number.

Item criticality:

Component type: Centrifugal pump condenser circulation

Part Number: P1

Failure rate (λ_p): 12.058 failures per million hours

Source: NPRD-95

Failure mode probability (α):

No output (0.29)

Degraded (0.71)

Source: FMD-97

Time (t): 1 hour

Failure effect probability (β): 1

Item criticality (C_r):

$$C_r = \sum_{n=1}^j (\beta \alpha \lambda_p t)_n \quad n = 1, 2, 3 \dots j \text{ or } C_r = \sum_{n=1}^j (C_m)_n$$

$$C_r = (1 \times .29 \times 12.058 \times 1) + (1 \times .71 \times 12.058 \times 1)$$

$$C_r = 12.058$$

6-3.5 Effects of Redundancy – Quantitative.

When redundancy is employed to reduce system vulnerability and increase uptime, failure rates need to be adjusted prior to using the preceding formula. This can be accomplished by using formulas from various locations depending on the application. Below are a few examples from the Reliability Toolkit: Commercial Practices Edition, page 161, which is based on an exponential distribution of failure (constant time between failures).

6-3.5.1 Failure Rate with Repairs.

Example 1: For a redundant system where all units are active "on-line" with equal failure rates and (n-q) out of n required for success. This equation takes repair time into consideration.

Equation 6-4. Failure Rate with Repairs

$$\lambda_{(n-q)/n} = \frac{n! (\lambda)^{q+1}}{(n-q-1)! (\mu)^q}, \text{ with repairs}$$

Where:

n = number of active online units; $n!$ is n factorial.

λ = failure rate for on-line unit (failures/hour)

q = number of online units that can fail without system failure

μ = repair rate ($\mu=1/MTTR$; where MTTR is the mean time to repair (hour)).

6-3.5.2 Failure Rate with Repairs Example.

Therefore, if a system has five active units, each with a failure rate of 220 f/10⁶ hours, and only three are required for successful operation. If one unit fails, it takes an average of three hours to repair it to an active state. What is the effective failure rate of this configuration?

6-3.5.3 Failure Rate with Repairs Example Inputs.

Substituting the following values into the equation:

$$n = 5, q = 2, \mu = 1/3$$

$$\lambda(5-2) / 5 = \lambda_{3/5}$$

$$\lambda_{3/5} = \frac{5! (220 \times 10^{-6})^3}{(5-2-1)! (1/3)^2} = 5.75 \times 10^{-9} \text{ failures/hour}$$

$$\lambda_{3/5} = .00575 \text{ failures}/10^6 \text{ hours}$$

6-3.5.4 Determining Criticality Number of Example.

Then this new failure rate ($\lambda_{3/5}$) would be substituted for (λ_p) to determine criticality numbers of the system.

6-3.5.5 Failure Rate without Repairs Example.

Example 2: If by chance in the above sample, the unit was never repaired then the formula to use would be:

Equation 6-5. Failure Rate without Repairs

$$\lambda_{(n-q)/n} = \frac{\lambda}{\sum_{i=n-q}^n \frac{1}{i}}, \text{ without repairs}$$

Where:

n = number of active online units; $n!$ is n factorial

λ = failure rate for on-line unit (failures/hour)

q = number of online units that can fail without system failure

6-3.5.6 Failure Rate without Repairs Example Inputs.

Using the same problem from above and substituting into this formula

$$\lambda_{3/5} = \frac{200 \times 10^{-6}}{\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right) + \frac{1}{5}} = \frac{220 \times 10^{-6}}{\frac{47}{60}}$$

$$\lambda_{3/5} \approx 280 \times 10^{-6} \text{ failures/hour}$$

$$\lambda_{3/5} \approx 280 \text{ failures}/10^6 \text{ hours}$$

6-3.5.7 Failure Rate with Repairs vs without Repairs.

A noticeable increase in failure rate because the components are not repaired.

6-3.5.8 Other Failure Rate Formulas.

Other useful failure rate formulas used for redundant systems are as follows:

6-3.5.8.1 Active Units and Standby Units.

Example 3 & 4: One standby off-line unit with n active on-line units required for success. Off-line spare assumed to have a failure rate of zero. On-line units have equal failure rates.

Equation 6-6. Example 3

$$\lambda_{\frac{n}{n+1}} = \frac{n[n\lambda + (1 - P)\mu]\lambda}{\mu + n(P + 1)\lambda}, \text{with repair}$$

Equation 6-7. Example 4

$$\lambda_{\frac{n}{n+1}} = \frac{n\lambda}{P + 1}, \text{without repair}$$

Where:

n = number of active online units; $n!$ is n factorial.

λ = failure rate for on-line unit (failures/hour)

q = number of online units that can fail without system failure

μ = repair rate ($\mu=1/MTTR$; where MTTR is the mean time to repair (hr).

P = probability that the switching mechanism will operate properly when needed ($P=1$ with perfect switching)

6-3.5.8.2 Active Units with Different Failure and Repair Rates.

Example 5 & 6: Two active on-line units with different failure and repair rates. One of two is required for success.

Equation 6-8. Example 5

$$\lambda_{1/2} = \frac{\lambda_A + \lambda_B[(\mu_A + \mu_B) + (\lambda_A + \lambda_B)]}{(\mu_A)(\mu_B) + (\mu_A + \mu_B)(\lambda_A + \lambda_B)}, \text{with repair}$$

Equation 6-9. Example 6

$$\lambda_{1/2} = \frac{\lambda_A^2 \lambda_B + \lambda_B^2 \lambda_A}{\lambda_A^2 + \lambda_B^2 + \lambda_A \lambda_B}, \text{ without repair}$$

Where:

λ = failure rate for on-line unit (failures/hour)

6-3.5.9 Calculating Criticality Number for Examples 5 and 6.

These new failure rates (λ) should then be placed back in the equation,

$$C_{rc} = \sum_{n=1}^j (\beta \alpha \lambda_p t)_n$$

to calculate the new Criticality Number which accounts for redundancy.

6-3.5.10 Additional Redundancy Reference Material.

There is a technical publication that exclusively addresses various redundancy situations that may be of use, Rome Air Development Center, RADC-TR-77-287, A Redundancy Notebook, Rome Laboratory, 1977.

6-3.5.11 Additional Relative Ranking Approach.

If the facility does have failure rate data but does not have failure mode distribution data, a relative ranking can still be achieved, allowing for redundancy, by using the method described in the qualitative analysis, paragraph 6-3.6.

6-3.6 Qualitative Criticality Analysis.

Qualitative analysis will be used when specific part or item failure rates are not available. However, if failure rates are known on some components and not known on others, the failure rate data can be used to support the rankings below. This will provide a relative ranking between all the components. Failure mode ratio and failure mode probability are not used in this analysis. This analysis will allow the analysts the ability to subjectively rank each failure modes level of severity in relationship to its probability of failure. The items of most concern will be identified and evaluated to decrease the negative impact on the mission.

6-3.6.1 Criticality Worksheet.

Once it is determined that a qualitative approach will be used the Criticality worksheet that looks like Table 6-9 will be used. Note that some of the categories are derived from the FMEA sheet. The information from the FMEA should be transferred into the respective columns of the criticality worksheet. The additional categories will be used to

support and calculate the Risk Priority Number (RPN), which will be explained in paragraph 6-3.6.7. Adjustments to occurrence rankings to compensate for redundant components within a typical C5ISR facility must be addressed as well and will be discussed in paragraph 6-3.7. Therefore, it is essential that the required amount of components necessary (M) to perform the function and the amount of components that are redundant (N) should be recorded in the respective categories of the criticality worksheet. Table 6-11 is an example of the quantitative FMECA worksheet with redundant components.

6-3.6.2 Occurrence Ranking.

The occurrence ranking is a method used to subjectively assign a failure rate to a piece of equipment or component. Each step in the ranking will correspond to an estimated failure rate based on the analyst's experience with similar equipment used in a similar environment. As mentioned previously, a known failure rate can be cross referenced to an occurrence ranking thereby allowing a complete analysis of a system that does not have failure rate and failure mode information on every item or component. When known failure rate data is used in this type of analysis, it not only adds merit to the ranking for the equipment with failure data, but also adds merit to the occurrence rankings of unknown equipment by providing benchmarks within the ranking scale. These values will establish the qualitative failure probability level for entry into a CA worksheet format. Rates can be hours, days, cycles ...etc.

Table 6-11 Example of DA Form 7611, Quantitative FMECA with Redundant Components

QUANTITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

For use of this form, see TM 5-698-4; the proponent agency is USACE.

SYSTEM: Mechanical System

DATE (YYYYMMDD): 20050819

PART NUMBER: Industrial Water Supply

SHEET: 1 of 1

REFERENCE DRAWINGS:

COMPLIED BY: AAA

MISSION: Provided Temperature Control to Room

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	REDUNDANCY		FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	FAILURE MODE CRITICALITY NUMBER (C_p)	ITEM CRITICALITY NUMBER (ϵC_p)	REMARKS
					HAVE (N)	NEED (M)							
110.0	Reservoir/ contains 6000 gallons of water	Leak	Crack in wall, Ruptured drainpipe	4	2	1	1.500X10 ⁻⁶ (single) NPRD-95 .0104X10 ⁻⁶ (redundant)	1	1	61,320	6.38X10 ⁻⁴	6.38X10 ⁻⁴	
120.0	Pump #1/ Transport Industrial water supply at 1000GPM	Transport water at a rate below 1000GPM	Impeller degraded, gasket leak, motor degraded	3	4	1	12.508X10 ⁻⁶ (single) NPRD-95 1.4X10 ⁻¹⁷ (redundant)	1	.35	61,320	3.00X10 ⁻¹³	8.58X10 ⁻¹³	
120.1		Produce no water flow	Broken coupling, suction line leak, motor inoperable	3				1	.65	61,320	5.58X10 ⁻¹³		
130.0	Cooling Tower #1/ maintain a water temp of 75°F	Scaling (deposits) on media	Untreated water	4	4	1	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	.36	61,320	2.87X10 ⁻¹²	6.38X10 ⁻¹²	
130.1		Clogged sprayers	Untreated/ unfiltered water	4				1	.44	61,320	3.51X10 ⁻¹²		

DA FORM 7611, AUG 2006

Table 6-11 Example of DA Form 7611, Quantitative FMECA with Redundant Components (cont'd)

QUANTITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

For use of this form, see TM 5-698-4; the proponent agency is USACE.

SYSTEM: Mechanical System

DATE (YYYYMMDD): 20050819

PART NUMBER: Industrial Water Supply

SHEET: 1 of 1

REFERENCE DRAWINGS:

COMPLIED BY: AAA

MISSION: Provided Temperature Control to Room

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	REDUNDANCY		FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	FAILURE MODE CRITICALITY NUMBER (C_p)	ITEM CRITICALITY NUMBER (ϵC_p)	REMARKS
					HAVE (N)	NEED (M)							
130.0		Fan failure	Motor winding open, No supply voltage to motor	3				1	.2	61,320	1.54×10^{-12}	1.54×10^{-12}	
210.0	Pump #5/ Transport Industrial water supply at 960GPM	Degraded operation – produce water at rate less than 960GPM	Impeller degraded, gasket leak, motor degraded	3	2	1	12.508X10 ⁻⁶ (single) NPRD-95 8.72X10 ⁻¹⁰ (redundant)	1	.35	61,320	3.00×10^{-13}	8.58×10^{-13}	
210.1		Produce no water flow	Broken coupling, suction line leak, motor inoperable	3				1	.65	61,320	5.58×10^{-13}		
220.0	Chiller/ Remove heat(10°F) from chilled water supply	Degraded operation – remove less than 10°F	Refrigerant leak degraded compressor, tube leak, dirty coil	3	2	1	9.279X10 ⁻⁶ (single) NPRD-95 1.72X10 ⁻¹⁰ (redundant)	1	.92	61,320	9.70×10^{-6}	9.70×10^{-6}	
220.1		Remove no heat	Compressor seizure, motor failure	4				1	.08	61,320	8.45×10^{-6}	8.45×10^{-6}	Expensive and time-consuming repair

DA FORM 7611, AUG 2006

Table 6-11 Example of DA Form 7611, Quantitative FMECA with Redundant Components (cont'd)

QUANTITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)													
SYSTEM: Mechanical System										DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply										SHEET: 1 of 1			
REFERENCE DRAWINGS:										COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room										APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	REDUNDANCY		FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	FAILURE MODE CRITICALITY NUMBER (C_p)	ITEM CRITICALITY NUMBER (ϵC_p)	REMARKS
					HAVE (N)	NEED (M)							
310.0	Air handler/ Maintain room temp of 72°F 3200cfm	Maintain air temp higher than 72°F	Dirty coils	3	2	1	1.7657X10 ⁻⁶ (single) NPRD-95 6.24X10 ⁻¹² (redundant)	1	.35	61,320	1.34X10 ⁻⁷	3.826X10 ⁻⁷	
310.1		Provide air flow at a rate less than 3200cfm	Reduced motor output, Dirty intake filter	3				1	.40	61,320	1.53X10 ⁻⁷		
310.2		Produce no air flow	Broken belt, motor failure, fan bearing seizure, No AC power	3				1	.25	61,320	9.56X10 ⁻⁸		

DA FORM 7611, AUG 2006

6-3.6.3 Qualitative Occurrence Rankings.

Possible qualitative occurrence rankings (O) are shown in Table 6-12.

Table 6-12 Occurrence Rankings

Ranking	Failure Rate	Comment
1	1/10,000	Remote probability of occurrence; unreasonable to expect failure to occur
2	1/5,000	Very low failure rate. Similar to past design that has had low failure rates for given volume/loads
3	1/2,000	Low Failure rate based on similar design for volume/loads
4	1/1,000	Occasional failure rate. Similar to past design that has similar failure rates for given volume/loads.
5	1/500	Moderate failure rate. Similar to past design having moderate failure rates for given volume/loads.
6	1/200	Moderate to high failure rate. Similar to past design having moderate failure rates for given volume/loads.
7	1/100	High failure rate. Similar to past design having frequent failures that caused problems
8	1/50	High failure rate. Similar to past design having frequent failures that caused problems
9	1/20	Very high failure rate. Almost certain to cause problems
10	1/10+	Very high failure rate. Almost certain to cause problems

6-3.6.4 Severity Ranking.

The severity ranking, as mentioned in paragraph 6-2.7, is also important in determining relative concerns amongst failure modes. The severity of the consequences of the failure effect is evaluated in terms of worst potential consequences upon the system level which may result from item failure. A severity classification must be assigned to each system level effect. A lower ranking indicates a less severe failure effect. A higher ranking indicates a more severe failure effect. Severity classifications provide a qualitative measure of the worst potential consequences resulting from an item failure.

6-3.6.5 Severity Rankings Table.

The severity rankings (S) from Table 6-4 are again shown here in Table 6-13.

Table 6-13 Severity Rankings

Ranking	Effect	Comment
1	None	No reason to expect failure to have any effect on Safety, Health, Environment or Mission
2	Very Low	Minor disruption to facility function. Repair to failure can be accomplished during trouble call
3	Low	Minor disruption to facility function. Repair to failure may be longer than trouble call but does not delay mission.
4	Low to Moderate	Moderate disruption to facility function. Some portion of Mission may need to be reworked or process delayed.

Ranking	Effect	Comment
5	Moderate	Moderate disruption to facility function 100% of Mission may need to be reworked or process delayed .
6	Moderate to High	Moderate disruption to facility function. Some portion of Mission is lost. Moderate delay in restoring function.
7	High	High disruption to facility function. Some portion of Mission is lost. Significant delay in restoring function.
8	Very High	High disruption to facility function. All of Mission is lost. Significant delay in restoring function
9	Hazard	Potential Safety, Health, or Environmental issue. Failure will occur with warning
10	Extreme Hazard	Potential Safety, Health, or Environmental issue. Failure will occur without warning

6-3.6.6 Risk Priority Number.

The Risk Priority Number (RPN) is the product of the Severity (1-10) and the Occurrence (1-10) ranking.

Equation 6-10. Risk Priority Number

$$RPN = (S) \times (O)$$

Where:

RPN = Risk Priority Number

S = Severity Ranking

O = Occurrence Ranking

6-3.6.7 Risk Priority Number – Identify the Concerns or Risks.

The Risk Priority Number is used to rank and identify the concerns or risks associated with the operation due to the design. This number will provide a means to prioritize which components should be evaluated by the team to reduce their calculated risk through some type of corrective action or maintenance efforts. However, when severity is at a high level, immediate corrective action may be given regardless of the resultant RPN.

6-3.6.8 Automotive Industry Action Group Risk Priority Number.

This method was developed by the Automotive Industry Action Group (AIAG) and can be found in the reference manual titled Potential Failure Mode and Effects Analysis – FMEA. However, this manual also considers detection to determine the Risk Priority Number.

Equation 6-11. Risk Priority Number

$$RPN = (S) \times (O) \times (D)$$

Where:

RPN = Risk Priority Number

S = Severity Ranking

O = Occurrence Ranking

D = Detection Ranking

6-3.6.9 Detection Rankings.

Where detection is ranked (1-10), shown in Table 6-14, in a similar fashion as severity and occurrence.

Table 6-14 Detection Rankings

Ranking	Detection	Comment
1	Almost Certain	Current control(s) almost certain to detect failure mode. Reliable controls are known with similar processes.
2	Very High	Very high likelihood current control(s) will detect failure mode.
3	High	High likelihood current control(s) will detect failure mode.
4	Moderately High	Moderately high likelihood current control(s) will detect failure mode.
5	Moderate	Moderate likelihood current control(s) will detect failure mode.
6	Low	Low likelihood current control(s) will detect failure mode.
7	Very Low	Very low likelihood current control(s) will detect failure mode.
8	Remote	Remote likelihood current control(s) will detect failure mode.
9	Very Remote	Very remote likelihood current control(s) will detect failure mode.
10	Almost Impossible	No known control(s) available to detect failure mode.

6-3.6.10 Excluding Detection.

Detection was not included in the examples because in mission critical facilities, the team considers detection of a failure mode when assigning a severity ranking. They also consider a compensating provision such as redundancy. The end effect is altered due to these two contributing factors, therefore changing the severity of the consequences of this failure by design of the facility.

6-3.6.11 Severity Ranking vs Occurrence Ranking based on System.

Given the scenario that a compressor overheats due to the lack of lubrication, the effects would be "compressor seizes, room temperature rises, and computers malfunction". This would produce a severity ranking of "7" or "8". But due to the ability of the system to detect a problem, shut down the one component, and activate a redundant component in its place, a severity of "2" or "3" may be assigned for the failure mode. Note that it is also possible that the occurrence ranking will also be altered as well due to the redundant system. Even if there was no redundant component the end effect is altered because the ability to detect and shut down the compressor will prevent

it from seizing thus saving repair or replacement costs and shortening the duration of down time by minimizing the damage.

6-3.6.12 C5ISR vs Auto Industry Goals.

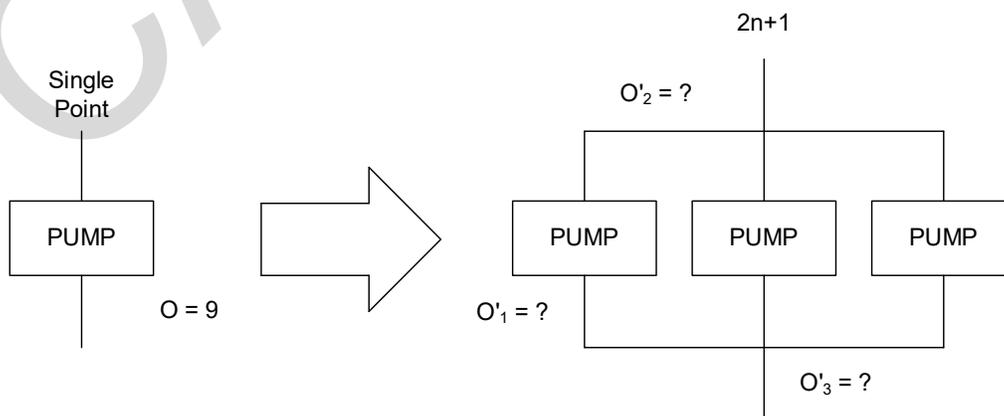
In addition, a C5ISR facility has a different "product" than the auto industry. The auto industry is producing parts and designers of the C5ISR facilities are primarily concerned with producing consistent temperature control and high-quality electricity. The auto industry does not want, under any circumstance, to allow a defective part out of their facility. If it does, the consequences would cost them immensely on recalls or warranty work. Therefore, it makes sense that they would consider detection of a faulty part prior to leaving their facility as important as severity in their analysis. This is not the case with a C5ISR facility. The designer's goal in producing a C5ISR facility is to be available without interruption. Just because a failure has been detected does not necessarily mean that the end level effect is prevented. However, it may minimize the downtime, thus increasing availability. When severity is assigned, this would be taken into consideration. For that reason, even though detection is considered in classifying severity, it does not hold the same relative importance.

6-3.7 Effects of Redundancy – Qualitative.

Traditional methods for dealing with redundancy's effect on failure rate are rather lengthy and difficult to apply to a qualitative analysis. Therefore, further explanation is required for how to deal with criticality rankings for like components within a single redundant system.

For example, consider an occurrence ranking of 9 for a chilled water supply pump (see Figure 6-10). In essence, the analysis is ranking the failure rate associated with the loss of function of that component relative to the equipment operation, or mission as a whole, and not the component itself. So, the question becomes "how to subjectively, but meaningfully, rank like redundant components with the same system function?"

Figure 6-10 Single Point System vs Redundant System



6-3.7.1 Redundant Systems.

By design, a redundant system is more reliable and less vulnerable than a single component, with respect to system function and mission requirements. So, it makes sense that qualitative ranking of redundant components should take such concepts as degree of redundancy and presumed individual component reliability into consideration.

As a result of decreased system vulnerability, each individual component is less critical to the system function and mission requirement. Therefore, it is evident that O'_1 , O'_2 , and O'_3 should not all have the same ranking number as the single component system (9). Furthermore, the relationship between degree of redundancy and occurrence is not linear. So, it is also evident that the value for O'_1 , O'_2 , and O'_3 cannot be a strict division by n of the ranking number assigned to the redundant system's function (3, 3, and 3). This is supported with the redundancy formula in the quantitative criticality analysis in paragraph 6-3.5.1, Equation 6-4.

6-3.7.2 Occurrence Rankings.

The occurrence ranking number for a single component function must be weighted to reflect the operation, presumed reliability, and severity of loss of function of the redundant component system as accurately as possible. Furthermore, it should be observed that for mission critical facilities, the presence of one more component than needed is not sufficient to confidently assure mission availability. Therefore, a conservative factor should also be observed when determining individual occurrence rankings of redundant components, relative to the single point function.

6-3.7.3 Adjusted Occurrence Level.

The following mathematical equations can be used to emulate a non-linear redundancy/occurrence relationship while introducing a conservative mission critical factor:

Equation 6-12. Adjusted Occurrence Level

$$O' = O_x \frac{M}{N - 1}$$

Where:

O = Occurrence level for loss of subsystem / system function, reliability data

O' = The adjusted occurrence level for the current redundant component being analyzed

M = The minimum number of components necessary

N = The number of components available

6-3.7.4 N+1 Occurrence Ranking.

Using this formula with only one redundant component will result in an occurrence ranking equal to the original. This formula reinforces the importance of having at least one extra component than necessary in a mission critical facility. The only way to decrease the occurrence ranking is to have 2 or more additional components than required.

$$O' = O \times \frac{M}{N - 1}$$

Using:

$$\begin{aligned} M &= 2 \\ N &= 3 \end{aligned}$$

$$O' = O \times \frac{2}{3 - 1}$$

$$O' = O \times \frac{2}{2}$$

$$O' = O \times 1$$

Where:

O = Occurrence level for loss of subsystem / system function

M = The minimum number of components necessary

N = The number of components available

O' = The adjusted occurrence level for the current redundant component

6-3.7.5 Risk Priority Number.

If only two items are needed and four are available and the occurrence is nine:

$$\begin{aligned} M &= 2 \\ N &= 4 \end{aligned}$$

$$O' = O \times \frac{2}{4 - 1}$$

$$O' = 9 \times \frac{2}{3}$$

$$O' = 6$$

Insert *O'* into the equation $RPN = O' \times S$ using the new severity ranking since the consequences of a failure of one component is not as severe to the end failure effect.

$$\text{Original: } RPN = O \times S = 9 \times 8 = 72$$

$$\text{New: } RPN = O' \times S = 6 \times 5 = 30$$

When sufficient failure rate data is available it is always recommended that quantitative CA be conducted through calculation or modeling. However, when a complete and detailed quantitative analysis is not necessary, realistically feasible, or desirable, the use of Equation 6-12 can be incorporated to quickly emulate the redundancy/occurrence relationship as part of a qualitative analysis.

6-3.7.6 Combined Method.

This “combined” method allows for an analysis to be conducted using the qualitative (subjective) approach and using supportive data to rank occurrence. Ranking occurrence with supportive data not only provides more merit to the results but offers flexibility by allowing the analyst to use data for components when available in the same analysis as other components that may not have any supportive data.

This is accomplished by allowing the failure rate (λ), failure mode probability (α), and the failure effect probability (β) to be multiplied to determine a failure rate for a particular failure mode. This rate can then be cross referenced in the occurrence ranking chart and assigned a new ranking (O'). Substituting in the formula:

$$RPN = (O') \times (S)$$

6-3.7.7 Adjusted Risk Priority Number.

This adjusted RPN will then be used in the final ranking process. Table 6-15 is an example of a FMECA using the qualitative method utilizing the redundancy formula to adjust the occurrence ranking. After the redundancy formula was applied, the number was rounded to the nearest whole number for this example. The components that only had one additional backup component did not have their occurrence rankings altered by this equation. Note: Rounding is not mandatory. This was done in the example for simplicity.

Table 6-15 Example of DA Form 7612, FMECA Worksheet Using Qualitative Rankings

QUALITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)													
SYSTEM: Mechanical System										DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply										SHEET: 1 of 1			
REFERENCE DRAWINGS:										COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room										APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM			REMARKS AND/OR RECOMMENDED ACTIONS		
					OCCUR	SEVERITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR		SEVERITY	RPN (O)X(S)
110.0	Reservoir/contains 6000 gallons of water	Leak	Crack in wall, Drainpipe breaks	No immediate effect. The surrounding area will be saturated.	2	6	12	2	1	2	4	8	If drainpipe breaks secondary containment will be filled
120.0	Pump #1/ Transport Industrial water supply at 1000GPM	Transport water at a rate below 1000GPM	Impeller degraded, gasket leak, motor degraded	No immediate effect. Chiller inefficiency will cost \$\$.	3	4	12	4	1	1	3	3	
120.1		Produce no water flow	Broken coupling, leak on suction line, motor inoperable	Room temp will rise above max allowed temp. Mission failure.	6	5	30	4	1	2	3	6	
130.0	Cooling Tower #1/ maintain a water temp of 75°F	Scaling (deposits) on media	Untreated water	Room temperature will rise slightly	3	6	18	4	1	1	4	4	
130.1		Clogged sprayers	Untreated/unfiltered water	Room temp will rise, Chiller efficiency decreases	3	5	15	4	1	1	4	4	

DA FORM 7612, AUG 2006

Table 6-15 Example of DA Form 7612, FMECA Worksheet Using Qualitative Rankings (cont'd)

QUALITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)													
For use of this form, see TM 5-698-4; the proponent agency is USACE.													
SYSTEM: Mechanical System										DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply										SHEET: 1 of 1			
REFERENCE DRAWINGS:										COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room										APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM			REMARKS AND/OR RECOMMENDED ACTIONS		
					OCCUR	SEVERITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR		SEVERITY	RPN (O)X(S)
130.2		Fan failure	Motor winding open, No power to motor	Air temp rise. No severe effect. Chiller efficiency decreases	3	4	12	4	1	1	3	3	
210.0	Pump #5/ Transport Industrial water supply at 960GPM	Degraded operation – produce water at rate less than 960GPM	Impeller degraded, gasket leak, motor degraded	No immediate effect. Chiller efficiency decreases \$\$\$	1	4	4	2	1	1	3	3	
210.1		Produce no water flow	Broken coupling, leak on suction line, motor inoperable	No air cooling. Room temp rise above allowed. Mission failure	2	8	16	2	1	2	3	6	
220.0	Chiller/ Remove heat(10°F) from chilled water supply	Degraded operation – remove less than 10°F	Refrigerant loss, degraded compressor, leaky tube, dirty coil	Air temperature will rise but not above max allowed	7	6	42	2	1	7	3	21	
220.1		Remove no heat	Compressor seizure, motor failure	Min. air cooling. Temp above max. Mission failure	2	8	16	2	1	2	4	8	

DA FORM 7612, AUG 2006

Table 6-15 Example of DA Form 7612, FMECA Worksheet Using Qualitative Rankings (cont'd)

QUALITATIVE FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)													
SYSTEM: Mechanical System										DATE (YYYYMMDD): 20050819			
PART NUMBER: Industrial Water Supply										SHEET: 1 of 1			
REFERENCE DRAWINGS:										COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room										APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM			REMARKS AND/OR RECOMMENDED ACTIONS		
					OCCUR	SEVERITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR		SEVERITY	RPN (O)X(S)
310.0	Air Handler/ Provide air to room at 72°F, 3200cfm	Provide air at a temp higher than 72°F	Dirty coils	Minimal change in temperature	3	4	12	2	1	3	3	9	
310.1		Provide airflow at a rate less than 3200cfm	Reduced motor output, dirty intake filter	Temperature variations in room dependent on location	2	3	6	2	1	2	3	6	
310.2		Provide no air flow	Broken belt, motor failure bearing seizure in fan, Loss of power	Temp rise above max allowed. Mission failure	2	7	14	2	1	2	3	6	

DA FORM 7612, AUG 2006

6-4 RANKINGS.

6-4.1 Criticality Rankings.

A criticality ranking is a list used to rank the failure modes of most concern first, down to the least concern, at the bottom. This procedure is essentially conducted in the same fashion whether it is a quantitative analysis or the more widely used qualitative (subjective) analysis.

6-4.1.1 Analyzing Failure Modes in Terms of RPN.

When failure modes are analyzed in terms of RPN, the highest RPN must be listed first (qualitative analysis). When failure rate data is used to calculate criticality numbers (quantitative analysis) the highest criticality number should be listed first. See Table 6-16 for an example failure mode criticality ranking using DA Form 7613. Table 6-17 using DA Form 7614 is another type of ranking that only ranks the item criticality number (Equation 6-3) that was discussed in paragraph 6-3.4.6. This is called an item criticality ranking. Both rankings have advantages, but the failure mode criticality ranking provides the most detail regarding failure rates and failure modes and is therefore the preferred type when conducting a quantitative analysis.

CANCELLED

Table 6-16 Example of DA Form 7613, Failure Mode Criticality Rankings

FAILURE MODE CRITICALITY RANKING (QUANTITATIVE)									
For use of this form, see TM 5-698-4; the proponent agency is USACE.									
SYSTEM: Mechanical System						DATE (YYYYMMDD): 20050819			
PART NUMBER: HVAC System						SHEET: 1 of 3			
REFERENCE DRAWINGS: C-20005-B						COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room						APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	MODAL CRITICALITY NUMBER (C_p)
220.0	Chiller/ Remove heat (10°F) from chilled water supply	Degraded operation – remove less than 10°F	Refrig. loss, degraded comp., tube leak, dirty coil	3	9.2791X10 ⁻⁶ (single) NPRD-95 1.72X10 ⁻¹⁰ (redundant)	1	.92	61,320	9.70X10 ⁻⁶
310.2	Air Handler/ Provide 3200cfm of air, keep room at 72°F	Provide no air flow	Broken belt, motor failure fan bearing seizure, Loss of power	3	1.7657X10 ⁻⁶ (single) NPRD-95 6.24X10 ⁻¹² (redundant)	1	.25	61,320	9.56X10 ⁻⁸
220.1	Chiller/ Remove heat (10°F) from chilled water supply	Remove no heat	Compressor seizure, motor failure	4	9.2791X10 ⁻⁶ (single) NPRD-95 1.72X10 ⁻¹⁰ (redundant)	1	.08	61,320	8.45X10 ⁻⁶
110.0	Reservoir/ contain 6000 gallons of water	Leak	Crack in wall	4	1.500X10 ⁻⁶ (single) .0104X10 ⁻⁶ (redundant)	1	1	61,320	6.38X10 ⁻⁴
120.1	Pump #1/ Transport Industrial water supply at 1000gpm	Produce no water flow	Broken coupling, suction line leak, motor inoperable	3	12.058X10 ⁻⁶ (single) NPRD-95 1.4X10 ⁻¹⁷ (redundant)	1	.65	61,320	5.58X10 ⁻¹³

DA FORM 7613, AUG 2006

Table 6-16 Example of DA Form 7613, Failure Mode Criticality Rankings (cont'd)

FAILURE MODE CRITICALITY RANKING (QUANTITATIVE)									
For use of this form, see TM 5-698-4; the proponent agency is USACE.									
SYSTEM: Mechanical System						DATE (YYYYMMDD): 20050819			
PART NUMBER: HVAC System						SHEET: 1 of 3			
REFERENCE DRAWINGS: C-20005-B						COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room						APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	MODAL CRITICALITY NUMBER (C_p)
210.1	Pump #5/ Transport chilled water supply at 960gpm	Produce no water flow	Broken coupling, suction line leak, motor inoperable	3	12.058X10 ⁻⁶ (single) NPRD-95 8.724X10 ⁻¹⁰ (redundant)	1	.65	61,320	5.58X10 ⁻¹³
130.1	Cooling Tower #1/ Maintain a water temp of 75°F	Clogged sprayers	Untreated/unfiltered water	4	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	.44	61,320	3.51X10 ⁻¹²
120.0	Pump #1/ Transport Industrial water supply at 1000gpm	Transport water a rate below 1000gpm	Impeller degraded, gasket leak, motor degraded	3	12.058X10 ⁻⁶ (single) NPRD-95 1.4X10 ⁻¹⁷ (redundant)	1	.35	61,320	3.00X10 ⁻¹³
210.0	Pump #5/ Transport chilled water supply at 960gpm	Degraded operation – produce water at a rate less than 960gpm	Impeller degradation, gasket leak, motor degraded	3	12.058X10 ⁻⁶ (single) NPRD-95 8.724X10 ⁻¹⁰ (redundant)	1	.35	61,320	3.00X10 ⁻¹³
130.0	Cooling Tower #1/ Maintain a water temp of 75°F	Sealing (deposits) on media	Untreated water	4	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	.36	61,320	2.87X10 ⁻¹²

DA FORM 7613, AUG 2006

Table 6-16 Example of DA Form 7613, Failure Mode Criticality Rankings (cont'd)

FAILURE MODE CRITICALITY RANKING (QUANTITATIVE)									
For use of this form, see TM 5-698-4; the proponent agency is USACE.									
SYSTEM: Mechanical System						DATE (YYYYMMDD): 20050819			
PART NUMBER: HVAC System						SHEET: 1 of 3			
REFERENCE DRAWINGS: C-20005-B						COMPLIED BY: AAA			
MISSION: Provided Temperature Control to Room						APPROVED BY: BBB			
ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	MODAL CRITICALITY NUMBER (C_p)
130.2	Cooling Tower #1/ Maintain a water temp of 75°F	Fan failure	Motor winding open, Loss of power to motor	3	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	.20	61,320	1.54X10 ⁻¹²
310.1	Air Handler/ Provide 3200cfm of air to room, maintain	Provide airflow at a rate less than 3200cfm	Reduced motor output, dirty intake filter	3	1.7657X10 ⁻⁶ (single) NPRD-95 6.24X10 ⁻¹² (redundant)	1	.40	61,320	1.53X10 ⁻⁷
310.0	Air Handler/ Provide 3200cfm of air to room, maintain	Maintain air at a temp higher than 72°F	Dirty coils	3	1.7657X10 ⁻⁶ (single) NPRD-95 6.24X10 ⁻¹² (redundant)	1	.35	61,320	1.34X10 ⁻⁷
130.0	Cooling Tower #1/ Maintain a water temp of 75°F	Sealing (deposits) on media	Untreated water	4	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	.36	61,320	2.87X10 ⁻¹²

DA FORM 7613, AUG 2006

Table 6-17 Example of DA Form 7614, Item Criticality Rankings

ITEM CRITICALITY RANKING (QUANTITATIVE) For use of this form, see TM 5-698-4; the proponent agency is USACE.						
SYSTEM: Mechanical System 20050819				DATE (YYYYMMDD):		
PART NUMBER: HVAC System				SHEET: 1 of 3		
REFERENCE DRAWINGS: C-20005-B				COMPLIED BY: AAA		
MISSION: Provided Temperature Control to Room				APPROVED BY: BBB		
ITEM NUMBER	ITEM/FUNCTION	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	OPERATING TIME (t)	ITEM CRITICALITY NUMBER (ϵC_p)
220.0	Chiller/ Remove heat (10°F) from chilled water supply	3	9.2791X10 ⁻⁶ (single) NPRD-95 1.72X10 ⁻¹⁰ (redundant)	1	61,320	9.70X10 ⁻⁶
120.0	Pump #1/ Transport water through Industrial water supply at 1000gpm	3	12.058X10 ⁻⁶ (single) NPRD-95 1.4X10 ⁻¹⁷ (redundant)	1	61,320	8.58X10 ⁻¹³
210.0	Pump #5/ Transport water through chilled water supply at 960gpm	3	12.058X10 ⁻⁶ (single) NPRD-95 8.724X10 ⁻¹⁰ (redundant)	1	61,320	8.58X10 ⁻¹³
220.1	Chiller/ Remove heat (10°F) from chilled water supply	4	9.2791X10 ⁻⁶ (single) NPRD-95 1.72X10 ⁻¹⁰ (redundant)	1	61,320	8.45X10 ⁻⁶
110.0	Reservoir/ contain 6000 gallons of water	4	1.500X10 ⁻⁶ (single) .0104X10 ⁻⁶ (redundant)	1	61,320	6.38X10 ⁻⁴

Table 6-17 Example of DA Form 7416, Item Criticality Rankings (cont'd)

ITEM CRITICALITY RANKING (QUANTITATIVE) For use of this form, see TM 5-698-4; the proponent agency is USACE.						
SYSTEM: Mechanical System 20050819				DATE (YYYYMMDD):		
PART NUMBER: HVAC System				SHEET: 1 of 3		
REFERENCE DRAWINGS: C-20005-B				COMPLIED BY: AAA		
MISSION: Provided Temperature Control to Room				APPROVED BY: BBB		
ITEM NUMBER	ITEM/FUNCTION	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	OPERATING TIME (t)	ITEM CRITICALITY NUMBER (ϵC_p)
130.0	Cooling Tower #1/ Maintain a water temp of 75°F	4	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	61,320	6.38X10 ⁻¹²
310.0	Air Handler/ Provide 3200cfm of air to room, maintain room at 72°F	3	1.7657X10 ⁻⁶ (single) NPRD-95 6.24X10 ⁻¹² (redundant)	1	61,320	3.826X10 ⁻⁷
130.2	Cooling Tower #1/ Maintain a water temp of 75°F	3	10.0518X10 ⁻⁶ (single) NPRD-95 1.3X10 ⁻¹⁶ (redundant)	1	61,320	1.54X10 ⁻¹²

6-4.1.2 Failure Mode Criticality, Item Criticality and RPN Ranking.

The failure mode criticality ranking, item criticality ranking, and RPN ranking lists can be useful tools but should not be solely used to determine which items are of most concern. Where these rankings fall short are their inability to allow the analyst to be judgmental to determine higher risk or higher consequences of failures. It is quite possible that two or more failure modes have similar RPN's or criticality numbers, but one has a much higher severity or consequence of the failure. These items typically need to be addressed first. Therefore, it is highly suggested that this ranking should be complimented by developing a criticality matrix. The matrix is explained in paragraph 6-4.2.

6-4.1.3 Not Constructing a Criticality Matrix Approach.

If the analysts do not wish to construct a criticality matrix, the next best approach would be to organize the Criticality Ranking by not only the Criticality Number or RPN, but also list the items by severity. This can be accomplished quite easily in an Excel program sorting first by severity and then by Criticality Number or RPN. The analysts can then review all the higher severity items first and make sound judgments regarding what type of actions, if any, should be taken to decrease the severity. This critical ranking list is to be used in a flexible manner according to the best judgment of the analysts. If done correctly it will aid in safety, maintainability, and FTA, thereby enabling improvements in the design.

6-4.2 Criticality Matrix.

The Criticality Matrix is a graphical or visual means of identifying and comparing failure modes for all components within a given system or subsystem and their probability of occurring with respect to severity. It is used for quantitative and qualitative analyses. The matrix can be used along with the Critical Item List or by itself to prioritize components.

6-4.2.1 Differentiate Criticality of Components.

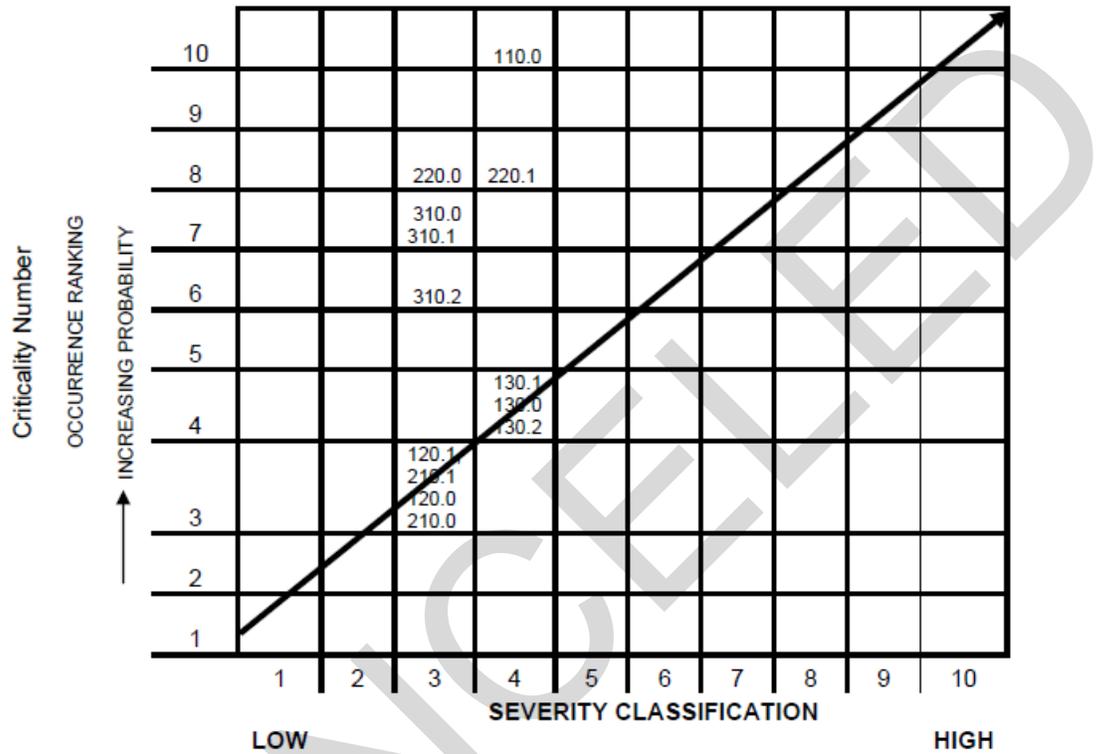
The matrix has the distinctive ability to differentiate criticality of components with the same or similar RPN and criticality number. For example: two components could have the same RPN, one with the severity of three and an occurrence ranking of ten, the other with a severity of ten and an occurrence ranking of three, thus producing a RPN of 30. Consequently, listing them only by RPN would produce an equal ranking. By placing them in the matrix it becomes very evident that an item that is in the severity category of "ten" should take priority for some type of corrective action.

6-4.2.2 Criticality Matrix Construction.

The matrix is constructed by inserting the assigned Item number, or other indicator, for each failure mode into matrix locations which represent the severity classification and probability of occurrence ranking. The criticality matrix example shown in Figure 6-11 is

representative of the HVAC system FMECA example in Table 6-11. If there is not sufficient space available in the matrix to paste the Item number, then an alternative method to represent each failure mode should be used. The resulting matrix shows the relative ranking of criticality for each item's failures.

Figure 6-11 Criticality Matrix



Item #	Failure Mode	Modal Criticality Number
110.0	leak	6.38×10^{-4}
120.0	Transport water at a rate below 1000 gpm	3.00×10^{-13}
120.1	produce no water flow	5.58×10^{-13}
130.0	Scaling(deposits) on media	2.87×10^{-12}
130.1	Clogged sprayers	3.51×10^{-12}
130.2	Fan failure	1.54×10^{-12}
210.0	Degraded operation-produce water at a rate less than 960gpm	3.00×10^{-13}
210.1	produce no water flow	5.58×10^{-13}
220.0	Degraded operation-remove less than 10°F	9.70×10^{-6}
220.1	remove no heat	8.45×10^{-6}
310.0	Maintain air at a temp higher than 72°F	1.34×10^{-7}
310.1	Provide airflow at a rate less than 3200cfm	1.53×10^{-7}
310.2	Provide no air flow	9.56×10^{-8}

6-4.2.3 Criticality Matrix Item Numbers.

Item number's displayed in the upper most right-hand corner of the matrix require the most immediate attention. These failures have a high probability of occurrence and a

catastrophic effect on system operation or personnel safety. Therefore, they should be evaluated first to determine if a redesign (such as, design in redundancy) is an alternative approach. Moving diagonally towards the lower left-hand corner of the matrix, the criticality and severity of potential failures decreases. In cases where failures display the same relative severity and criticality, it must be determined whether safety/mission success or cost is the driving factor of the analysis. If safety/mission success is of more concern, items shown on the right of the diagonal line require the most re-design attention, because the effects of their failures are more severe even though their criticality ranking may be less. If cost is a major concern, items to the left of the diagonal line require attention, because the high criticality numbers (occurrence rankings) reflect higher failure probability.

6-4.2.4 Criticality Matrix with Redundant System.

By employing redundancy, a duplicate system is constructed such that it serves as a backup for a critical single point failure. Though the initial failure of the component or system cannot be avoided, the effect of the failure will no longer be catastrophic since a compensating provision (the redundant system) will serve to operate in its place. If redundancy cannot be employed, then a more robust component with a lower failure rate may be an option. Every means possible should be evaluated to lower the failure rate on any high severity classification failure mode. If this cannot be accomplished, then a reaction plan must be developed to minimize the downtime of the system.

6-5 RESULTS.

6-5.1 Overview.

At the conclusion of the FMECA, critical items/failure modes are identified, and corrective action recommendations made based on the criticality list and/or the Criticality Matrix generated by the CA.

6-5.1.1 Utilizing the Criticality List.

Utilizing the criticality list, the items with the highest criticality number or RPN receive attention first. Utilizing the Criticality Matrix (recommended), items in the upper most right-hand quadrant will receive attention first. Typical recommendations call for design modifications such as the use of higher quality components, higher rated components, design in redundancy or other compensating provisions.

6-5.1.2 Recommendations.

Recommendations cited must be fed back into the design process as early as possible to minimize iterations of the design. The FMECA is most effective when exercised in a proactive manner to drive design decisions, rather than to respond after the fact.

6-5.2 Recommendations – from the Criticality Matrix Example.

Once the items are assigned their respective "squares" in the criticality matrix, the team now has the ability to rank which components need further review. From the above example the items can be quickly judged. If there are items that have similar RPNs and fall in the roughly the same vicinity in the matrix, then the team will have to determine which item should be addressed first. Remember, as the design matures and information is collected, this tool will be able to identify more clearly which items should take priority.

6-5.2.1 Item Number 110.0.

Item number 110.0 is the reservoir and has a high failure rate. Possibly another choice for a reservoir with a lower failure rate and an annual inspection/evaluation of condition of reservoir should be considered.

6-5.2.2 Item Number 220.1.

Item number 220.1 is the inability of the chiller to remove any heat from the chilled water supply. This has a relatively high failure rate and severity. The chiller should have inspections at specified intervals including eddy current testing annually to monitor breakdown of tubes. Motor should be tested annually as well for breakdown of windings. Because there is a redundant component this can be done at a predetermined time. Continuous monitoring of temperature with existing sensors and alarms should prevent catastrophic failure of the chiller. These procedures should address item 220.0 as well.

6-5.2.3 Item Numbers 310.0, 310.1, and 310.2.

Item numbers 310.0, 310.1, & 310.2 are all associated with the air handler system. Number 310.0 and number 310.1 have a higher failure rate and are therefore more likely to occur and possibly predict due to their nature of failure mechanisms which are a "wear out" type mechanism. Therefore, typical preventative maintenance actions at manufacture's recommendations should be employed initially. This interval can be adjusted according to inspection reports from the maintenance actions. The fan should not be driven by one belt. Use a sheave with three grooves for three belts to decrease the chance that one broken belt will make the item fail. A spare motor should be on hand to quickly replace the existing motors in the event one fails. Bearings should be greased quarterly (do not over grease) and air filter(s) changed semiannually.

6-5.2.4 Item Numbers 130.0, 130.1, and 130.2.

Item numbers 130.0, 130.1, and 130.2 have relatively high severities and average failure rates. These items are all related to the cooling towers. Most of the failures associated with this item are related to contamination of the water, therefore monitoring the condition of the water through water analysis and changing the filters at a regular interval (again, adjust this as needed) should also be implemented. An annual inspection should be done as well. Replacement sprayers and fan motors should be readily available to quickly respond to a spontaneous failure in these locations.

6-5.2.5 Remaining Failure Modes.

The final four failure modes are associated with the pumps in both the chilled water supply and the industrial cooling water supply. The chilled water supply ranks higher because in the event of no chilled water there will be no heat removed from the room and therefore would lead to computer failure. This is an immediate effect versus the industrial cooling water system which will affect the efficiency of the chiller and possibly lead to a failure over time. Therefore, if a priority were to be in place, the chilled water pump should take precedence. In either case, the recommendations for both pumps are the same. Along with the manufacture's recommended PM in place for rebuilding the pump and periodic inspections, then a vibration analysis and an electrical test on the motor could be conducted at a semiannual basis. In the event of a spontaneous failure the redundant pump can be transferred over while the failed pump is repaired. It should be noted however, that if the power supply is disrupted to the first pump then there is a possibility that the second pump will also be unable to start. This means there better be a separate power feed line to the secondary pumps.

6-5.3 Incentives.

The FMECA is a valuable tool that can be utilized from early design to functional use of a system. It is most beneficial when initiated early in the design process by providing engineers a prioritized list of areas in the design that need attention. This early assessment will minimize costs associated with constructing a facility and maintaining it. To develop strategies after the facility is built not only costs more but will typically be compromised due to physical restraints.

6-5.3.1 Identifying Critical Items.

Due to the continuous challenge to provide clean reliable power and precise temperature control to a mission critical facility, it is somewhat intimidating to attempt to assess which items should be more critical to mission success. The effects of redundancy, failure rates and severity on this assessment of each component/subsystem can be complex and time consuming when using a pure statistical approach. However, the alternative method explained in this manual should provide a simpler means to make this assessment or ranking possible, with or without failure data.

6-5.3.2 Method Modifications.

The method used in this manual should be used as a guide and tailored to a facility's specific need. It is important that the user makes modifications to the forms to meet those needs. This manual is meant to be used as a tool and must be flexible to accomplish a meaningful analysis at different facilities.

6-5.4 Results.

6-5.4.1 Comparison of Single Component Failures.

The results from this type of analysis are for comparison of single component failures only. The information derived from this analysis will provide a baseline to conduct other analyses. For simultaneous multiple failure event analysis, other techniques, such as FTA, should be used. The FTA is very extensive and is usually applied to areas of concern that are identified through the FMECA process or from prior experience.

6-5.4.2 Strength and Weaknesses of FMECA.

It is very important to know the strengths and weaknesses of this analysis. The FMECA is a living document and should be updated on a continual basis as more and more information is collected on the system. It should provide a valuable resource to support reliability, corrective maintenance actions, and safety.

6-5.4.3 Effects of Redundancy.

The effects of redundancy should be taken into consideration when calculating criticality numbers or assigning occurrence rankings because redundancy reduces the failure rate, thus increasing the availability. After all, availability is the prime objective of the C5ISR facility.

CHAPTER 7 RELIABILITY CENTERED MAINTENANCE (RCM)

7-1 RCM.

7-1.1 The RCM Concept.

Prior to the development of the RCM methodology, it was widely believed that everything had a "right" time for some form of preventive maintenance (PM), usually replacement or overhaul. A widespread belief among many maintenance personnel was that by replacing parts of a product or overhauling the product (or reparable portions thereof), that the frequency of failures during operation could be reduced. Despite this previous commonly held view, the results seemed to tell a different story. In far too many instances, PM seemed to have no beneficial effects. Indeed, in many cases, PM made things worse by providing more opportunity for maintenance-induced failures.

7-1.1.1 Airline Study.

When the airline companies in the United States observed that PM did not always reduce the probability of failure and that some items did not seem to benefit in any way from PM, they formed a task force with the Federal Aviation Administration (FAA) to study the subject of preventive maintenance. The results of the study confirmed that PM was effective only for items having a certain pattern of failures. The study also concluded that PM should be required only when required to assure safe operation. Otherwise, the decision to do or not do PM should be based on economics.

7-1.1.2 RCM Approach.

The RCM approach provides a logical way of determining if PM makes sense for a given item and, if so, selecting the appropriate type of PM. The approach is based on the following precepts.

- (1) The objective of maintenance is to preserve an item's function(s). RCM seeks to preserve system or equipment function, not just operability for operability's sake. Redundancy improves functional reliability but increases life cycle cost in terms of procurement and life cycle cost.
- 2) RCM focuses on the end system. RCM is more concerned on maintaining system function than individual component function.
- (3) Reliability is the basis for decisions. The failure characteristics of the item in question must be understood to determine the efficacy of preventive maintenance. RCM is not overly concerned with simple failure rate; it seeks to know the conditional probability of failure at specific ages (the probability that failure will occur in each given operating age bracket).
- (4) RCM is driven first by safety and then economics. Safety must always be preserved. When safety is not an issue, preventive maintenance must be justified on economic grounds.

(5) RCM acknowledges design limitations. Maintenance cannot improve the inherent reliability – it is dictated by design. Maintenance, at best, can sustain the design level of reliability over the life of an item.

(6) RCM is a continuing process. The difference between the perceived and actual design life and failure characteristics is addressed through age (or life) exploration.

7-1.1.3 RCM Concept.

The RCM concept has completely changed the way in which PM is viewed. It is now a widely accepted fact that not all items benefit from PM. Moreover, even when PM would be effective, it is often less expensive (in all senses of that word) to allow an item to "run to failure" rather than to do PM. In the succeeding discussions, the RCM concept will be examined in more detail. The meaning of terms that are central to the RCM approach will be explored. These terms include failure characteristics, efficiency, run to failure, cost, and function.

7-1.2 Benefits of RCM.

7-1.2.1 Reduced Costs.

A significant reason for creating the joint airline/FAA task force was the new Boeing 747 (B747) jumbo jet. Boeing and United Airlines, the initial buyer of the aircraft, were already considering the development of the PM program for the B747. This new airliner was vastly larger and more complex than any ever built. Given the cost of maintenance on smaller aircraft already in service, the maintenance costs for the B747, using the traditional approach to PM, would have threatened the profitability, and hence the viability, of operating the new aircraft. Examples of the ultimate savings achieved in using RCM to develop the PM program for the B747 and other aircraft are shown in Table 7-1. Similar savings have been achieved by other industries for other equipment when going from a traditional to an RCM-based PM program. It is important to note that these costs savings are achieved with no reduction in safety, an obvious requirement in the airline industry.

Table 7-1 Cost Benefits of using RCM for Developing PM Program

Type of PM	Required Using Traditional Approach	Required Using RCM
Structural Inspections	4,000,000 hours for DC-8	66,000 hours for B747
Overhaul	339 items for DC-8	7 items for DC-10
Overhaul of turbine engine	Scheduled	On-condition (cut shop maintenance costs by 50% compared with DC-8)

7-1.2.2 Increased Availability.

For many systems, including C5ISR facilities, availability is of primary importance. Availability was defined in paragraph 2-1.5. As indicated in the definition, the level of

availability achieved in actual use of a product is a function of how often it fails and how quickly it can be restored to operation. The latter, in turn, is a function of how well the product was designed to be maintainable, the amount of PM required, and the logistics resources and infrastructure that have been put in place to support the product. RCM directly contributes to availability by reducing PM to that which is essential and economic.

7-1.3 Origins of RCM.

7-1.3.1 Airlines.

As stated earlier, RCM had its origins with the airline industry. Nowhere had the then prevailing philosophy of maintenance been challenged more. By the late 1950's, maintenance costs in the industry had increased to a point where they had become intolerable. Meanwhile, the Federal Aviation Agency (FAA) had learned through experience that the failure rate of certain types of engines could not be controlled by changing either the frequency or the content of scheduled fixed-interval overhauls. As a result of these two factors, a task force consisting of representatives of the airlines and aircraft manufacturers was formed in 1960 to study the effectiveness of PM as being implemented within the airline industry.

(1) The task force. The task force developed a rudimentary technique for developing a PM program. Subsequently, a maintenance steering group (MSG) was formed to manage the development of the PM program for the new Boeing 747 (B747) jumbo jet. This new airliner was vastly larger and more complex than any ever built. Given the cost of maintenance on smaller aircraft already in service, the maintenance costs for the B747, using the traditional approach to PM, would have threatened the profitability, and hence the viability, of operating the new aircraft.

(2) MSG-1. The PM program developed by the steering group, documented in a report known as MSG-1, was very successful. That is, it resulted in an affordable PM program that ensured the safe and profitable operation of the aircraft.

(3) MSG-2. The FAA was so impressed with MSG-1 that they requested that the logic of the new approach be generalized, so that it could be applied to other aircraft. So, in 1970, MSG-2, Airline Manufacturer Maintenance Program Planning Document, was issued. MSG-2 defined and standardized the logic for developing an effective and economical maintenance program. MSG-2 was first used on the L1011, DC10, and MD80 aircraft. In 1972, the European aviation industries issued EMSG (European Maintenance System Guide), which improved on MSG-2 in the structures and zonal analysis. EMSG was used on the Concorde and A300 Airbus.

7-1.3.2 Adoption by Military.

The problems that the airlines and FAA had experienced with the traditional approach to maintenance were also affecting the military. Although profit was not an objective common to both the airlines and military, controlling costs and maximizing the availability of their aircraft were. Consequently, in 1978, the DOD contracted with United Airlines to conduct a study into efficient maintenance programs. The study supplemented MSG-2 by emphasizing the detection of hidden failures and moved from a process-oriented concept to a task-oriented concept. The product of the study was MSG-3, a decision logic that was called RCM.

7-1.3.3 Use for Facilities and Other Industries.

Although created by the aviation industry, RCM quickly found applications in many other industries. RCM is used to develop PM programs for public utility plants, especially nuclear power plants, railroads, processing plants, and manufacturing plants. It is no overstatement to say that RCM is now the pre-eminent method for evaluating and developing a comprehensive maintenance program for an item. Today, a variety of documents are available on RCM.

7-1.4 Relationship of RCM to Other Disciplines.

7-1.4.1 Reliability.

It is obvious why the first word in the title of the MSG-3 approach is reliability. Much of the analysis needed for reliability provides inputs necessary for performing an RCM analysis, as will be seen in succeeding paragraphs. The fundamental requirement of the RCM approach is to understand the failure characteristics of an item. As used herein, failure characteristics include the underlying failure rate, the consequences of failure, and whether the failure manifests itself and, if it does, how. Reliability is measured in different ways, depending on one's perspective: inherent reliability, operational reliability, mission (or functional) reliability, and basic (or logistics) reliability. RCM is related to operational reliability.

(1) Inherent versus operational reliability. From a designer's perspective, reliability is measured by "counting" only those failures that are design related. When measured in this way, reliability is referred to as "inherent reliability." From a user's or operator's perspective, all events that cause the system to stop performing its intended function is a failure event. These events certainly include all design-related failures that affect the systems' function. Also included are maintenance-induced failures, no-defect found events, and other anomalies that may have been outside the designer's contractual responsibility or technical control. This type of reliability is called "operational reliability."

(2) Mission or functional reliability versus basic or logistics reliability. Any failure that causes the product to fail to perform its function or mission is counted in "mission reliability." Redundancy improves mission reliability. Consider a case where one part of a product has two elements in parallel where only one is needed (redundant). If a failure

of one element of the redundant part of the product fails, the other continues to function allowing the product to do its job. Only if both elements fail will a mission failure occur. In "basic" reliability, all failures are counted, whether a mission or functional failure has occurred. This measure of reliability reflects the total demand that will eventually be placed on maintenance and logistics.

7-1.4.2 Safety.

Earlier, it was stated that one of the precepts on which the RCM approach is that safety must always be preserved. Given that the RCM concept came out of the airline industry, this emphasis on ensuring safety should come as no surprise. In later paragraphs, the way the RCM logic ensures that safety is ensured will be discussed. For now, it is sufficient to note that the RCM specifically addresses safety and is intended to ensure that safety is never compromised. In the past several years, environmental concerns and issues involving regulatory bodies have been accorded an importance in the RCM approach for some items that is equal (or nearly so) to safety. Failures of an item that can cause damage to the environment or which result in some Federal or state law being violated can pose serious consequences for the operator of the item. So, the RCM logic is often modified, as it is in this UFC, to specifically address environmental, mission, or other concerns.

7-1.4.3 Maintainability.

RCM is a method for prescribing PM that is effective and economical. Whether or not a given PM task is effective depends on the reliability characteristics of the item in question. Whether or not a task is economical depends on many factors, including how easily the PM tasks can be performed. Ease of maintenance, corrective or preventive, is a function of how well the system has been designed to be maintainable. This aspect of design is called maintainability. Providing ease of access, placing items requiring PM where they can be easily removed, providing means of inspection, designing to reduce the possibility of maintenance-induced failures, and other design criteria determine the maintainability of a system.

7-2 MAINTENANCE.

Maintenance is defined as those activities and actions that directly retain the proper operation of an item or restore that operation when it is interrupted by failure or some other anomaly. Within the context of RCM, proper operation of an item means that the item can perform its intended function. These activities and actions include fault detection, fault isolation, removal and replacement of failed items, repair of failed items, lubrication, servicing (includes replenishment of consumables such as fuel), and calibrations. Other activities and resources are needed to support maintenance. These include spares, procedures, labor, training, transportation, facilities, and test equipment. These activities and resources are usually referred to as logistics. Although some organizations may define maintenance to include logistics, it will be used in this document in the more limited sense and will not include logistics.

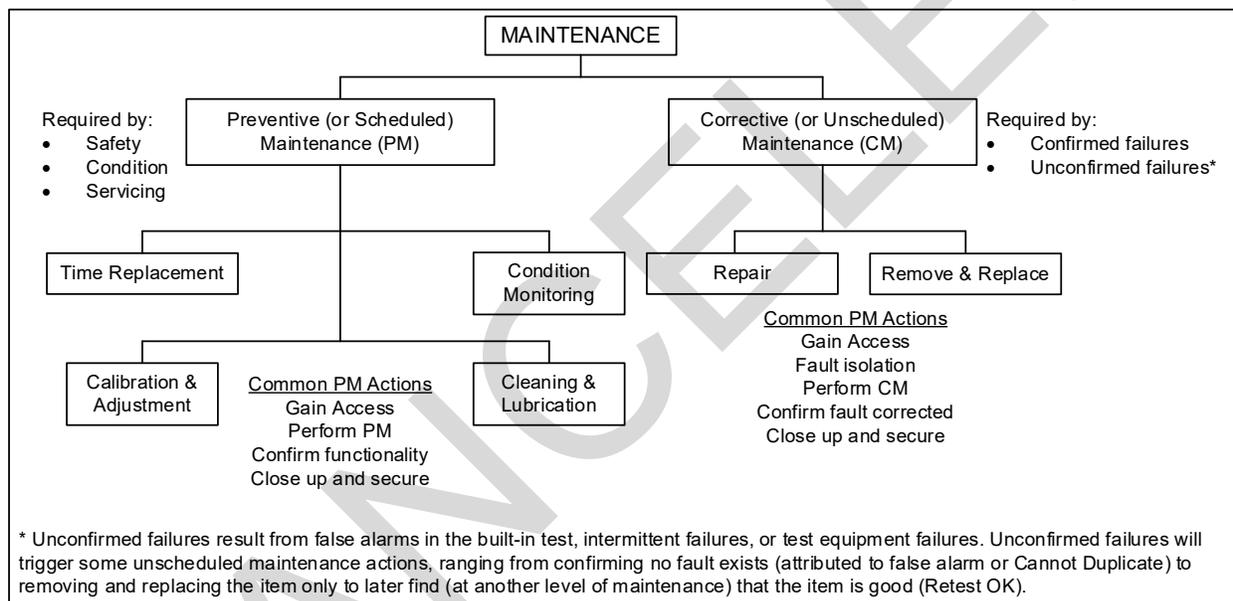
7-2.1 Categories of Maintenance.

Maintenance is usually categorized by either when the work is performed or where the work is performed.

7-2.1.1 Categorizing by when Maintenance is Performed.

In this case, maintenance is divided into two major categories: preventive and corrective. Figure 7-1 illustrates how these two categories are further broken down into specific tasks. These categories of maintenance, corrective and preventive, are further subdivided in some references into reactive, preventive, predictive, and proactive maintenance.

Figure 7-1 Major Categories of Maintenance by when Performed.



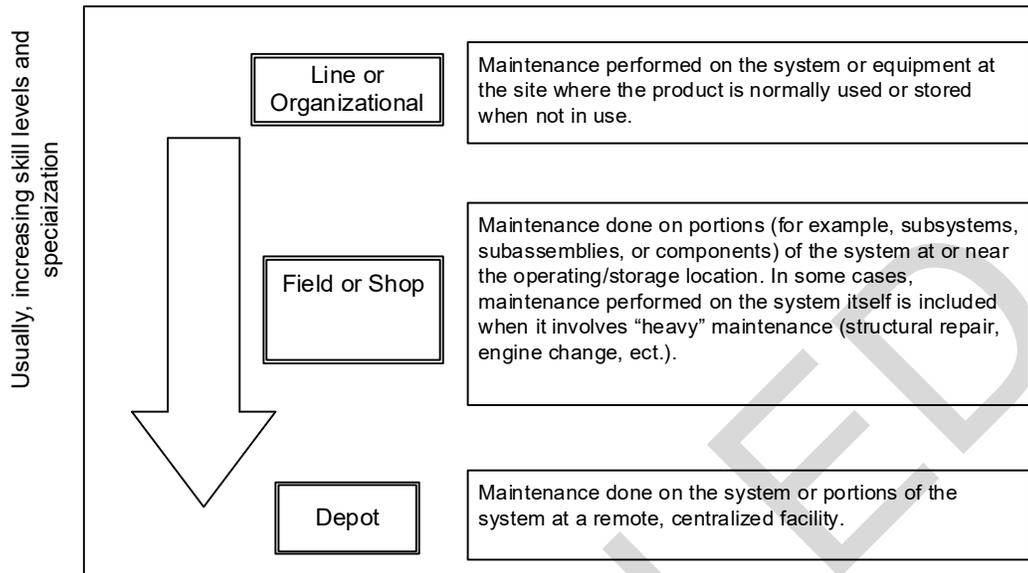
(1) Reactive maintenance. This term is equivalent to corrective maintenance, and both are also referred to as breakdown, repair, fix-when-fail, or run-to-failure maintenance.

(2) Proactive maintenance. Includes actions intended to extend useful life, such as root-cause failure analysis, continual improvement, and age exploration. Proactive and predictive are treated herein as categories of preventive maintenance, with proactive included under Scheduled, predictive under Condition-based, and age exploration as a separate step in the RCM process.

7-2.1.2 Categorizing by where Maintenance is Performed.

Maintenance can also be categorized by where the work is performed. These categories are referred to as levels of maintenance. The categories most often used are shown in Figure 7-2.

Figure 7-2 Typical Approach to Categorizing Maintenance by where it is Performed.



7-2.2 Categorization by when Maintenance is Performed.

7-2.2.1 Preventative Maintenance.

Preventive maintenance (PM) is usually self-imposed downtime (although it can be done while corrective maintenance is being performed and it may even be possible to perform some PM while the product is operating). PM consists of actions intended to prolong the operational life of the equipment and keep the product safe to operate. This UFC defines two types of PM: Scheduled and Condition-based. In both cases, the objectives of PM are to ensure safety, reduce the likelihood of operational failures, and obtain as much useful life as possible from an item. Table 7-2 has examples of each type of PM.

(1) Scheduled maintenance. When a specified interval between maintenance is required, the maintenance is referred to as scheduled preventive maintenance. The interval may be in terms of hours, cycles, rounds fired, or other measure meaningful to the way the item is operated. Note that with scheduled PM, no attempt is made to ascertain the condition of the item. Scheduled maintenance may also consist of recalibrations or adjustments made at regular intervals. Some texts categorize inspections as scheduled PM. Certainly, inspections are based on some periodic interval or event (for example, inspection of an aircraft prior to and after each flight). However, since the purpose of an inspection is to ascertain the condition of the item, it has been included under the next category of PM, Condition-based.

Table 7-2 Examples of Tasks under Two Categories of Preventive Maintenance

Category	Tasks	Examples	Notes
Scheduled ¹	Remove and replace (R&R)	R&R batteries in smoke alarm twice annually	Maintenance is performed without regard to actual condition of item. Interval based on useful life and other factors. Includes all lubrication and servicing.
		R&R gun barrel after 5,000 rounds have been fired	
		Change oil every 3,000 miles	
		Lubricate bearings every 25,000 shaft revolutions	
	Overhaul or recondition	Overhaul transmission every 100,000 miles	Item is overhauled or reconditioned without regard to actual condition. Interval based on useful life and other factors.
		Refinish blades every 2,000 operating hours	
	Recalibrate	Recalibrate depth setting on drill press daily	Compensate for changes in calibration due to vibration and other conditions of use.
Recalibrate gage against standard at beginning of each shift			
Condition ²	Inspect item or area	Visually inspect belts and pulleys for excessive wear prior to starting machine	Inspections can be performed using human senses (e.g., visually check belts for wear), using non-destructive inspection (NDI) techniques (e.g., inspect for corrosion using dye penetrant), or special measuring equipment (check tread depth using gage). Can also include functional check to determine proper operation.
		Inspect for corrosion every 2 weeks	
		Inspect for delamination or disbond weekly	
		Inspect tires for cuts and proper tread depth before and after each flight	
		Inspect for hidden failure of redundant item	
	Monitor condition	Continuously monitor vibration profile and R&R bearing when limits reached	Objective is to act before useful life has been reached or a functional failure has occurred. Parameter limits and profiles based on analysis, test, and field experience. Monitoring can but does not need to be continuous.
		Check sample of oil every 50 operating hours for presence of wear metals and overhaul engine when limits reached	

1. Based on time.
2. Based on observed or measured condition.

(2) Condition-based maintenance. Preventive maintenance performed to ascertain the condition of an item, detect, or forecast an impending failure, or performed because of such actions is referred to as Condition-based PM.

(a) A hidden failure of an item is one that has already occurred, has not affected performance of the end system, but will if another item fails. Ideally, through some form of warnings or monitoring device, no failure will be "hidden." It is impractical and not always feasible to detect every failure of every item in a system and alert the operator or maintainer that the failure has occurred. Inspections are therefore needed to detect such failures. See paragraph 7-4.3.1.3 for a more complete discussion of hidden failures. Maintenance that is required to correct a hidden failure condition is, of course, corrective maintenance.

(b) Some texts use terms such as predictive maintenance and on-condition. The definition of condition-based PM used herein includes these concepts. In summary, the objectives of condition-based PM are to first evaluate the condition of an item, then, based on the condition, either determine if a hidden failure has occurred or a failure is imminent, and then take appropriate action.

7-2.2.2 Corrective Maintenance and Run-to-Failure.

As already alluded to, corrective maintenance (CM) is required to restore a failed item to proper operation.

(1) Restoration. Restoration is accomplished by removing the failed item and replacing it with a new item, or by fixing the item by removing and replacing internal components or by some other repair action.

(2) When CM is required. CM can result from system failures or from condition based PM.

(a) When system operation is impaired by the failure of one or more items, the operator is usually and immediately alerted to the problem. This alert may come from obvious visual or sensory signals (such as, the operator can see, hear, or feel that a problem has occurred) or from monitoring equipment (indicators, built-in diagnostics, annunciator lights, etc.). When the alert comes from the latter, it is possible that a system failure has in fact not occurred. That is, the detecting equipment itself has failed or a transient condition has occurred resulting in an indication of system failure that is false or cannot be duplicated. Whether or not an actual system failure has occurred, any indication that one has will necessitate CM. The CM may result in a Cannot Duplicate (CND) or Retest OK (RTOK), in-place repair, or replacement. CNDs and RTOKs are serious problems in very complex systems for two reasons. First, they consume maintenance time and can cause unnecessary loss of system availability. Second, without in-depth test and analysis, one cannot be certain whether the detecting equipment failed, the system did fail, or transients caused the failure (and is not evident except under those transient conditions).

(b) When inspection or condition monitoring detects a hidden or failure, then some form of corrective maintenance is required.

(c) If the only concern were to obtain the greatest possible amount of life from an item, it would be allowed to run-to-failure. Under a run-to-failure approach, only CM would be required. No PM would be performed. However, the consequences on economics, safety, and mission requirements of some failures make a run-to-failure approach untenable. Consequently, most practical maintenance programs consist of a combination of PM and CM. Determining what combination is "right" for an item is one of the objectives of the RCM process.

7-2.3 Maintenance Concepts.

7-2.3.1 Level of Maintenance.

In considering how maintenance can be categorized, the idea of levels of maintenance was introduced. The term "levels of maintenance" has traditionally been used by the military services, although its use is not unknown in commercial industry. Within the services, the norm was once three levels of maintenance (line or organizational, field or shop, and depot). Under a 3-level concept, items are either repaired while installed on the end product or are removed and replaced. Various terms are used to refer to an item that is removed and replaced and include Line Replaceable Unit (LRU) and Weapon Replaceable Assembly (WRA). For convenience, LRU will be used in this document to refer to items that are normally removed from and replaced on the end product.

(1) The benefits of a 2-level maintenance concept. To reduce costs and increase availability, the services have been working for several years to implement a 2-level maintenance concept. Under this concept, repairs made on the system are kept to a minimum and, whenever possible, consist of remove and replace (R&R) actions. The idea is that by making R&R the preferred maintenance on the product, the downtime of the system can be kept to a minimum. Failed items are then sent back to the second level of maintenance, usually a depot or original equipment manufacturer (OEM).

(2) Making a 2-level concept work. A 2-level maintenance concept will only be affordable and practical if three criteria are met. First, each LRU's reliability must be "sufficiently high" given the item's cost. If not, availability will suffer, due to an excessive number of high-cost spares failing, and the supply "pipeline" will be expensive. Second, the integrated diagnostic capability (Built-in Test, Automatic Test Equipment, manual methods, etc.) must be very accurate and reliable. Otherwise, the supply pipeline to the second level of maintenance will be filled with good LRUs mistakenly being sent for repair – CNDs and RTOKs are a serious problem under any maintenance concept but spell disaster for a 2-level maintenance concept. Finally, a responsive and cost-effective means of transporting LRUs between the field and the depot must be available.

7-2.3.2 Centralized Versus De-Centralized.

When maintenance at a given level is performed at several locations located relatively close to the end user, a decentralized maintenance concept is being implemented. For example, suppose a 3-level maintenance concept is being used. When an LRU fails at an operating location, it is removed and replaced with a good LRU. The operating location sends the failed LRU to a co-located field repair activity (FRA) where it is repaired. Such repair can consist of either in-place repair or R&R of constituent components often called Shop Replaceable Units. Under a centralized concept, each operating location would not have a co-located FRA. Instead, one or more centralized FRAs would be strategically located throughout the geographic operating area (such as, country, continent, hemisphere, etc.). Each operating location would ship its failed LRUs to the nearest centralized FRA. Such a concept is most effective when the LRUs are

highly reliable. If the reliability is high, then few failures will occur at any given operating location making it difficult to keep the technicians proficient in repairing the LRUs. Also, with few failures, the technicians and any support equipment (for example, automatic test equipment) will be under utilized. Under such conditions, it is difficult to justify a co-located FRA.

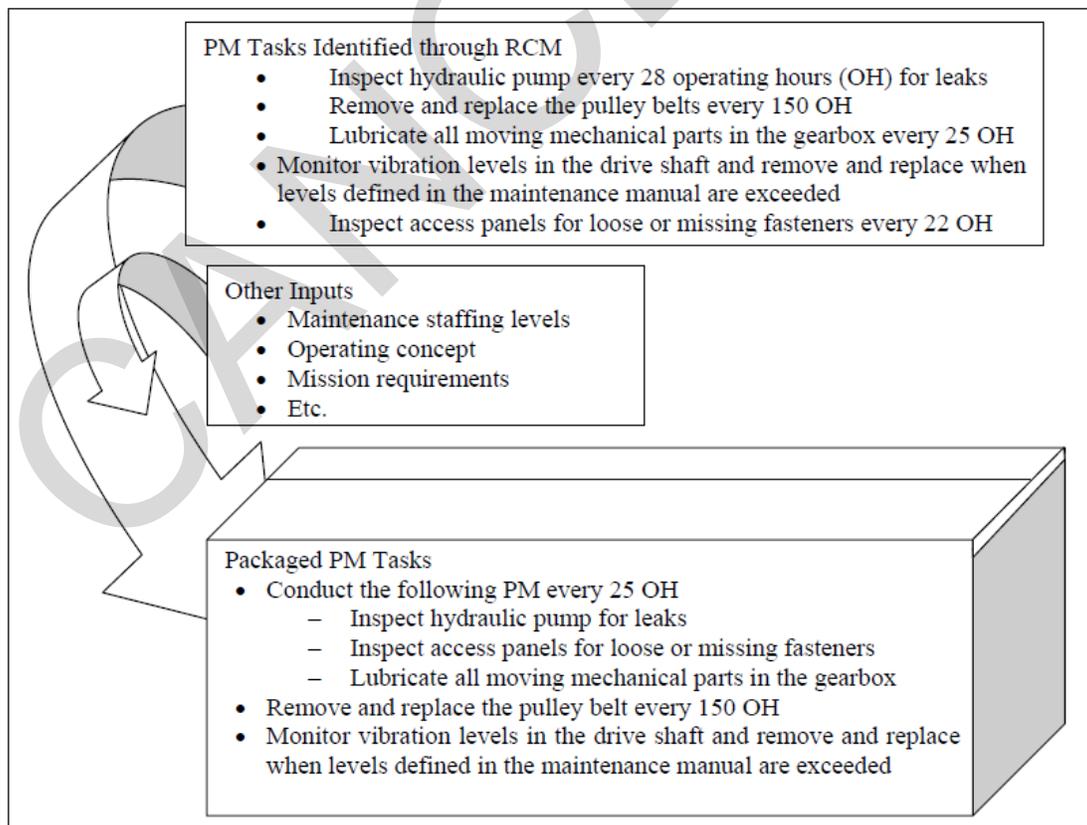
7-2.4 Packaging a Maintenance Program.

The total maintenance requirements for a product will dictate a set of preventive maintenance (PM) tasks and a set of corrective maintenance (CM) tasks. The latter tasks are essentially "maintenance on demand" and cannot be predicted. PM, as discussed previously, will consist of on-condition and scheduled maintenance. Once all PM tasks have been identified, they must be grouped, or packaged. By packaging PM tasks, maintenance resources can be used more effectively and minimize the number of times that the system will be out of service for PM.

7-2.4.1 Packaging Example.

An example is shown in Figure 7-3. The pump inspection could be conducted at 28 hours, the panel inspection at 22 hours, and lubricated the gearbox at 25 hours. But it is much more efficient to "package" the tasks as shown in the example.

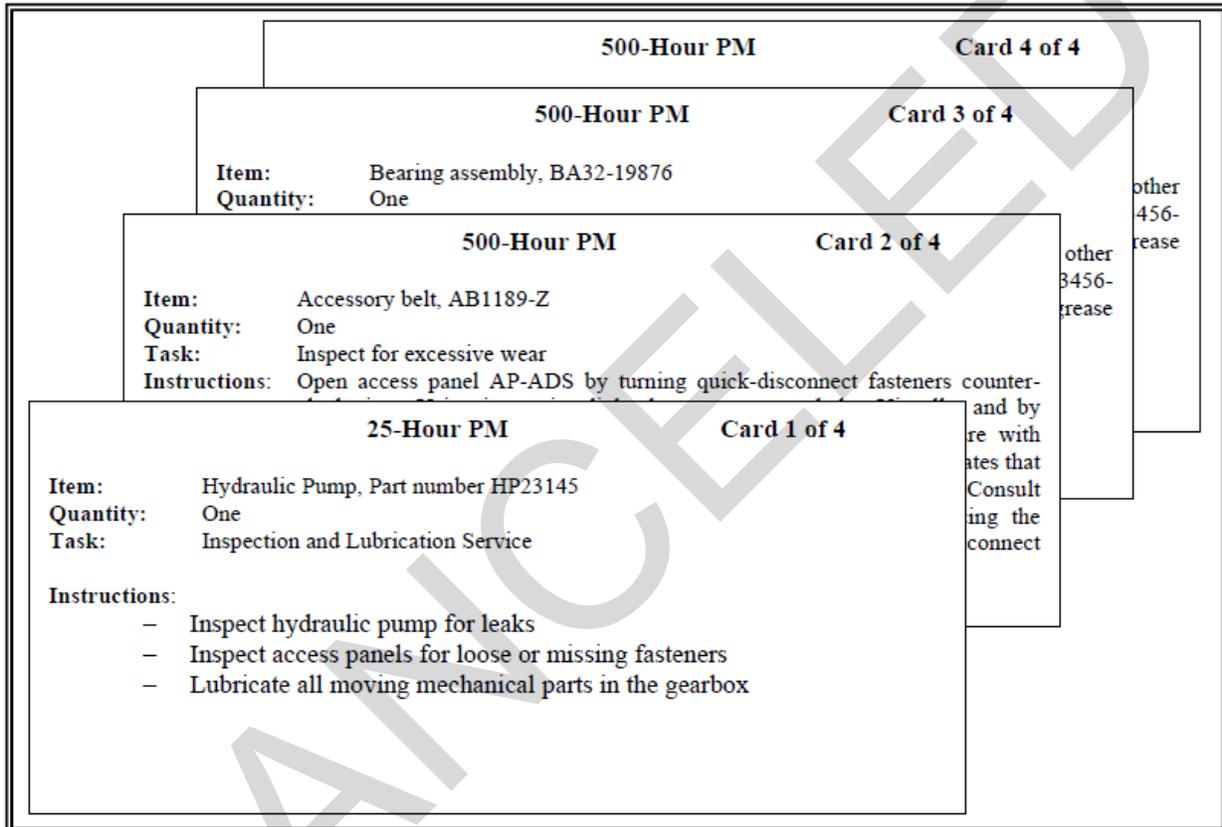
Figure 7-3 An Example of Packaging PM Tasks



7-2.4.2 Document the Packaging for Maintenance Personnel.

One method of documenting the packaging of PM tasks is to create inspection cards. For a given point in time (calendar time, number of operating hours, etc.), a set of cards defines the PM tasks to be performed. Figure 7-4 illustrates this approach.

Figure 7-4 Example of how PM Cards can be used to Document Required PM Tasks

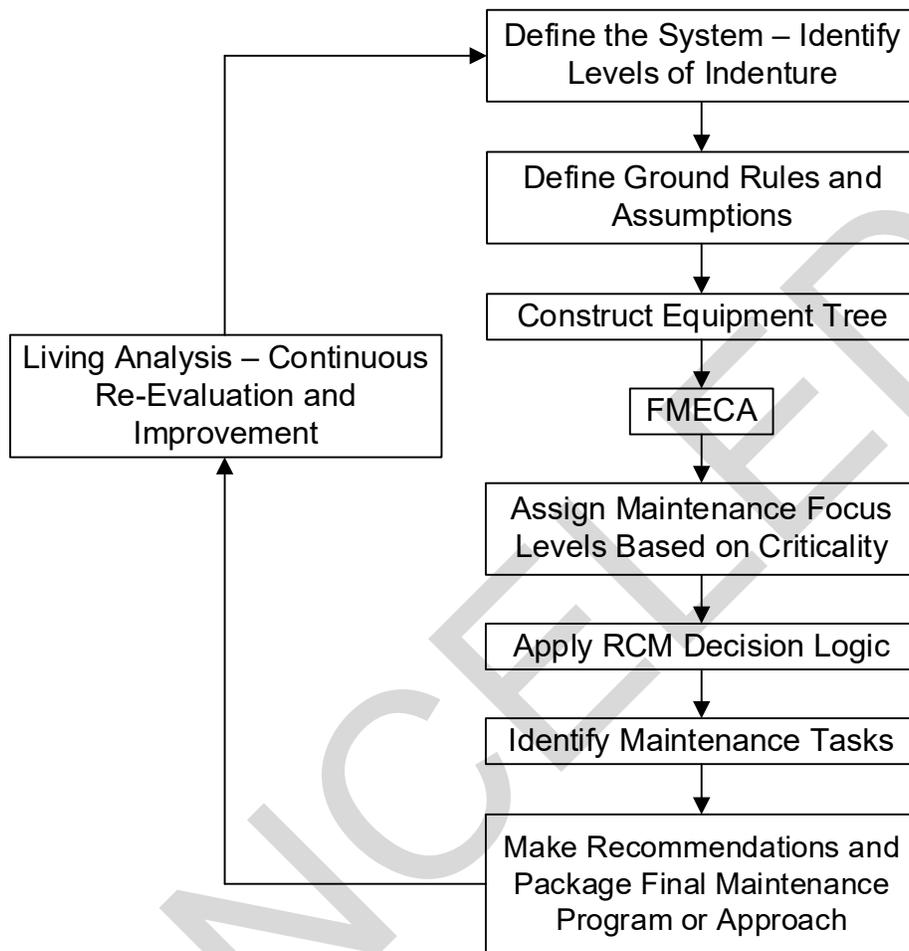


7-3 ELEMENTS OF RCM PROGRAM.

7-3.1 RCM Implementation Plan.

An overview of steps of the RCM process is shown in Figure 7-5.

Figure 7-5 The RCM Process Starts in the Design Phase and Continues for the Life of the System



7-3.1.1 Major Tasks.

As shown in Figure 7-5, several major tasks are required to implement the RCM concept.

- Define the System – Identify and document the boundaries of the analysis
 - Identify and document equipment included in the analysis
 - Identify and document the indenture level the analysis is intended to extend to
- Define Ground Rules and Assumptions – Identify and document ground rules and assumptions used to conduct the analysis

- Construct Equipment Tree – Construct equipment block diagrams to indicate equipment configuration, down to the lowest indenture level intended to be covered by the analysis
- Conduct FMECA – Analyze failure modes, effects and criticality
- Assign Maintenance Focus Levels – Classify maintenance focus levels based on criticality rankings
- Apply RCM Decision Logic – Apply RCM logic trees for items, especially those identified as being critical
- Identify Maintenance Tasks – Identify maintenance tasks to be performed on the given item
- Package Maintenance Program – Develop a maintenance tasking schedule for the analyzed equipment

Note: RCM Analysis is intended to be a living analysis. Effort should be made to continue to collect more complete information and add it to the analysis, to continue to provide a foundation for effective continuous improvement. Results and recommendations should be periodically reviewed and reevaluated, taking into consideration additional information of any kind.

(1) Conduct supporting analyses. RCM is a relatively information-intensive process. To provide the information needed to conduct the RCM analysis, several supporting analyses are either required, often as prerequisites to beginning the RCM analysis, or desirable. These supporting analyses include the FMEA, FTA, functional analysis, and others.

(2) Conduct the RCM analysis. The RCM analysis consists of using a logic tree to identify effective, economical, and, when safety is concerned, required PM. (As will be seen, PM is required when safety is involved; if no PM is effective, then redesign is mandatory).

7-3.1.2 The Implementation Plan.

Planning to implement an RCM approach to defining the PM for a system or product must address each of the tasks noted in the preceding paragraph. The plan must address the supporting design phase analyses needed to conduct an RCM analysis. Based on the analysis, an initial maintenance plan, consisting of the identified PM with all other maintenance being corrective, by default, is developed. This initial plan should be updated through Life Exploration during which initial analytical results concerning frequency of failure occurrence, effects of failure, costs of repair, etc. are modified based on actual operating and maintenance experience. Thus, the RCM process is iterative, with field experience being used to improve upon analytical projections.

7-3.2 Data Collection Requirements.

7-3.2.1 Required Data.

Since conducting an RCM analysis requires an extensive amount of information, and much of this information is not available early in the design phase, RCM analysis for a new product cannot be completed until just prior to production. The data falls into four categories: failure characteristics, failure effects, costs, and maintenance capabilities and procedures.

7-3.2.1.1 Failure Characteristics.

Studies conducted by the MSGs and confirmed by later studies showed that PM was effective only for certain underlying probability distributions. Components and items, for example, for which a constant failure rate applies (for example, the underlying probability distribution is the exponential) do not benefit from PM. Only when there is an increasing probability of failure should PM be considered.

7-3.2.1.2 Failure Effects.

The effects of failure of some items are minor or even insignificant. The decision whether to use PM for such items is based purely on costs. If it is less expensive to allow the item to fail, and to perform CM, than it is to perform PM, then the item is allowed to fail. As stated earlier, allowing an item to fail is called run to failure.

7-3.2.1.3 Costs.

The costs that must be considered are the costs of performing a PM task(s) for a given item, the cost of performing CM for that item, and the economic penalties, if any, when an operational failure occurs.

7-3.2.1.4 Maintenance Capabilities and Procedures.

Before selecting certain maintenance tasks, the analyst needs to understand what the capabilities are, or are planned, for the system. In other words, what is or will be the available skill levels, what maintenance tools are available or are planned, and what are the diagnostics being designed into or for the system.

7-3.2.2 Sources of Data.

Table 7-3 lists some of the sources of data for the RCM analysis. The data elements from the FMEA that are applicable to RCM analysis are highlighted in paragraph 7-5.4.2. Note that when RCM is being applied to a product already in use, or when a maintenance program is updated during Life Exploration, historical maintenance and failure data will be inputs for the analysis. An effective Failure Reporting and Corrective Action System (FRACAS) is an invaluable source of data. FRACAS is a closed-loop system for collecting, analyzing, and documenting failures and recording any corrective action taken to eliminate or reduce the probability of future such failures. FRACAS is

used when iterative tests or demonstrations are conducted on breadboard, or prototype products to identify mechanisms and trends for corrective action. FRACAS is used for existing systems to monitor performance.

Table 7-3 Data Sources for the RAM Analysis

Data Source	Comment
Lubrication requirements	Determined by designer. For off-the-shelf items being integrated into the product, lubrication requirements and instructions may be available.
Repair manuals	For off-the-shelf items being integrated into the product.
Engineering drawings	For new and off-the-shelf items being integrated into the product.
Repair parts list	
Quality deficiency reports	For off-the-shelf items being integrated into the product.
Other technical documentation	For new and off-the-shelf items being integrated into the product.
PREP Database	For new and off-the-shelf items being integrated into the product.
Recorded observations	From test of new items and field use of off-the-shelf items being integrated into the product.
Hardware block diagrams	For new and off-the-shelf items being integrated into the product.
Bill of Materials	For new and off-the-shelf items being integrated into the product.
Functional block diagrams	For new and off-the-shelf items being integrated into the product.
Existing maintenance plans	For off-the-shelf items being integrated into the product. Also, may be useful if the new product is a small evolutionary improvement of a previous product.
Maintenance technical orders/manuals	For off-the-shelf items being integrated into the product
Discussions with maintenance Personnel and field operators	For off-the-shelf items being integrated into the product. Also, may be useful if the new product is a small evolutionary improvement of a previous product.
Results of FMEA, FTA, and other reliability analyses	For new and off-the-shelf items being integrated into the product. Results may not be readily available for the latter.
Results of Maintenance task analysis	For new and off-the-shelf items being integrated into the product. Results may not be readily available for the latter.

7-3.3 Commitment to Life Cycle Support of the Program.

7-3.3.1 The Process Perspective.

As will be shown in this paragraph, RCM must be viewed as a continuing process, rather than an event that occurs once. Although a maintenance program based on RCM should be developed during design, it should be refined throughout the operational life of the system. In addition, RCM can be used to develop a maintenance program for an existing system for which the initial maintenance program was not based on RCM.

7-3.3.2 Learning from Experience.

Much of the information used to develop an RCM program, either during design for a new system or after fielding for an existing system will be based on estimates, may change over time, or be subject to some combination of these two factors. Consequently, it is essential to use experiential data to update the maintenance program.

7-3.3.3 Continuous PM Improvement.

RCM fundamentals established at design should be revisited on at least an annual interval. This process will maintain the efficiency intended for the facility at design. This takes into consideration changes in cost, Reliability degradation, changes in mission, changes in maintenance approach to name a few occurrences.

7-3.4 RCM as a Part of Design.

It is ideal to implement an RCM approach during the design and development of a new system to develop a maintenance program. The reasons will be briefly discussed here but will become clearer as the reader proceeds through the remaining paragraphs of this UFC.

7-3.4.1 Effective Use of Analyses.

During design and development, numerous analyses are performed. Many of these analyses directly support an RCM analysis. In turn, the results of going through the RCM process of developing a maintenance program can affect and contribute to these analyses. Obviously, implementing RCM during design and development makes very effective use of analyses that are usually performed.

7-3.4.2 Impact on Design.

As will be seen when the RCM logic diagrams are discussed, redesign is either mandatory or desirable in many cases. The cost and level of effort of design changes made during the design and development phase of a system are much less than if they were made after the system was fielded. Additionally, the effectiveness of design changes is higher when made during the design and development phase. Of course, RCM can and is used to develop maintenance programs for fielded systems, for which RCM was not applied during design and development. However, it is always best to implement RCM during design and development.

7-3.5 Focus on the Four Ws.

Discussion of the four Ws: what can fail, why does it fail, when will it fail, and what are the consequences of failures.

7-3.5.1 What can Fail?

In determining required maintenance, the first and most fundamental question that must be answered is what can fail. A variety of methods can be used to answer this question.

(1) Analytical methods. FMEA, FTA, and relayed analyses address, among other issues, what can fail that will prevent a system, subsystem, or component from performing its function(s).

(2) Test. Analytical methods are not infallible, and a particular failure may be overlooked or cannot be anticipated by analysis. Testing often reveals these failures. Testing can, of course, also be used to confirm or validate the results of analytical methods.

3) Field experience. Often, the same type of component, assembly, or even subsystem that is already used in one system may be used in a new system. If data is collected on field performance of these components, assemblies, and subsystems, it can be used to help answer the question, what can fail. Obviously, field experience is equally applicable to RCM when applied to an already fielded system.

7-3.5.2 Why Does an Item Fail?

To determine which, if any preventive maintenance tasks are appropriate, the reason for failure must be known. Insights into the modes and mechanisms of failure can be gained through analysis, test, and experience. Some of the analytical methods are the same as those used to determine What Can Fail. The methods include the FMEA and FTA. Others include root cause analysis, destructive physical analysis, and non-destructive inspection techniques. Table 7-4 lists some nondestructive inspection (NDI) techniques and Table 7-5 lists some of the modes and mechanisms of failure.

Table 7-4 Non-Destructive Inspection (NDI) Techniques, Briefly

Acoustic emission	Magnetic particle examination
Dye penetrant	Radiography
Eddy current	Spectrometric oil analysis
Emission spectroscopy	Stroboscopy
Ferrography	Thermography
Leak testing	Ultrasonics

Table 7-5 Examples of Failure Mechanisms and Modes

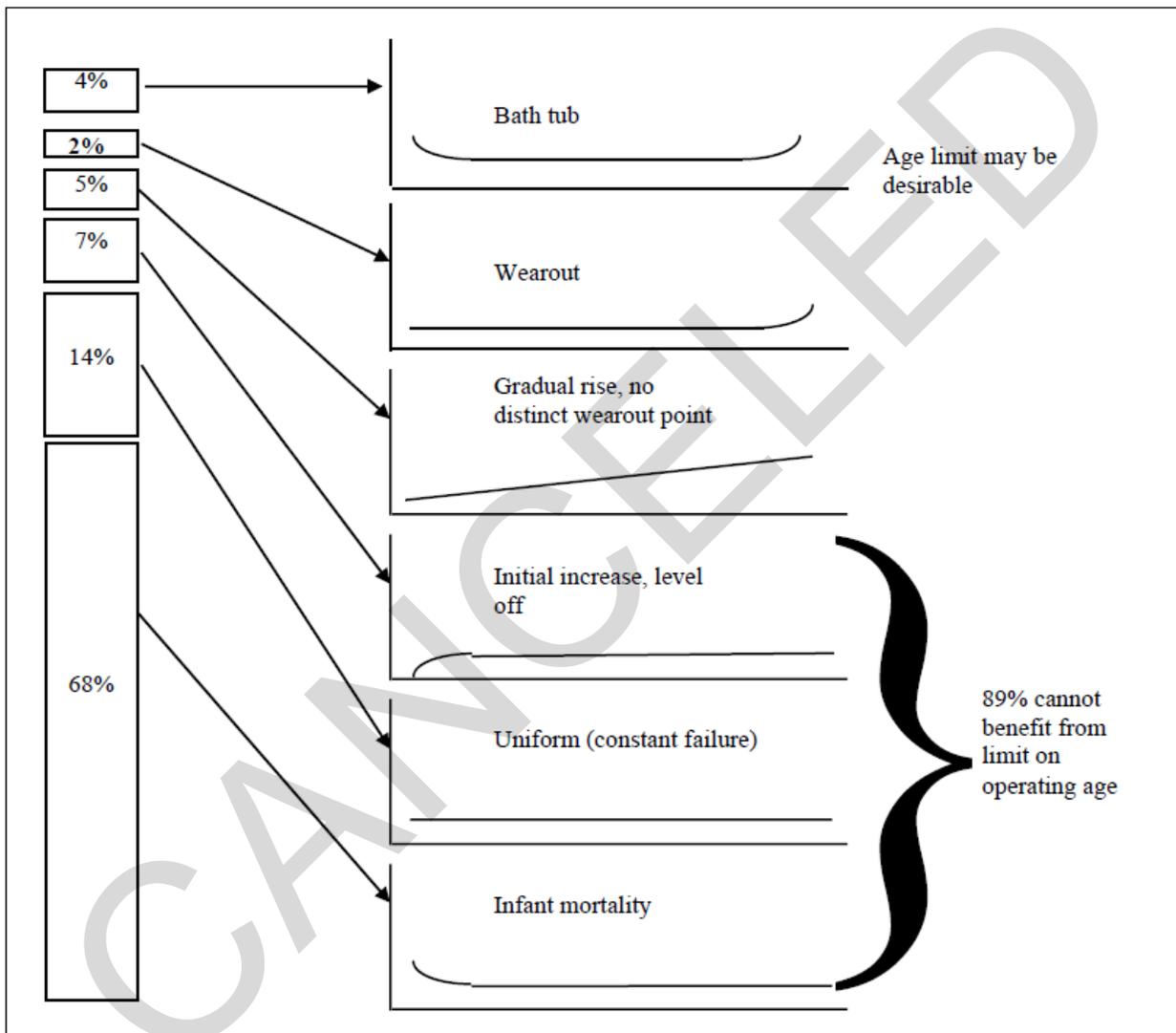
Modes		
Stuck open (valve)	Fractured (shaft)	Wear (bearing)
Shorted (connector)	Leakage (seal)	Slippage (belt drive)
Low torque (motor)	Excessive friction (shaft journal)	Short (resistor)
Mechanisms		
Brinelling (bearing ring)	Spalling (concrete)	Elongation/yielding (structure)
Fretting (pump shaft)	Condensation (circuit board)	Freezing (battery)
Ionization (microcircuit)	Glazing (clutch plate)	Fatigue (springs)
Plastic deformation (springs)	Wear (clutch plate)	Galvanic corrosion (structure)

7-3.5.3 When Will an Item Fail? (Occurrence).

If the underlying time to failure distribution is known for a part or assembly, then the probability of failure at any point in time can be predicted. For some items, the underlying distribution is exponential and the item exhibits a constant failure rate. In such cases, a new item used to replace an old item has the same probability of failing in the next instant of time as did the old item. Consequently, changing such an item at

some prescribed interval has no effect on the probability of failure. It makes more sense to run the item to failure. If that is not possible, if safety is involved for example, then redesign is necessary. As shown in Figure 7-6, only a small percentage of items can benefit from PM. Knowing the underlying distribution of times to failure is essential in determining if PM is applicable.

Figure 7-6 Applicability of Age Limit Depending on Failure Pattern



7-3.5.4 What are the Consequences of the Item Failing? (Severity).

Not all failures are equal in their effect on the system. Obviously, any failures that can cause death or injury to system operators or maintainers, or others who may be served by the system (for example, airline passengers) or are nearby the most serious. Very close in seriousness are failures that can result in compromised mission requirements, pollution to the environment, or a violation of government statutes. At the bottom of the list are failures such as cosmetic damage and other problems that have no effect on

system operation. Knowing the effect of a failure helps prioritize decisions. Serious failures usually demand some form of PM or redesign is necessary. Minor failures usually do not lead to redesign and PM is performed only if it is less expensive than running the item to failure. Table 7-6, on the following page, lists some examples of failure effect categorization used in FMEAs and in the RCM process. The way failure effects are categorized for C5ISR facilities should be based on the functions of the facility. Obviously, any failure that could kill or injure personnel or cause loss of the C5ISR mission would have to be categorized as the most serious. The criteria shown in Table 7-6, or some combination could be the basis for a C5ISR facility-specific categorization approach. Note that in using the RCM approach to developing a PM program, all failure must be put into one of three categories (Preventative Maintenance, Predictive Maintenance, Corrective Maintenance). These categories are used in the logic trees.

Table 7-6 Examples of Failure Effect Categorization

AIAG Standard (Automobile Industry Standard)		
Effect	Severity of Effect	Ranking
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe system operation and/or involves noncompliance with federal safety regulation without warning	10
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe system operation and/or involves noncompliance with federal safety regulation warning	9
Very High	System/item inoperable with loss of primary function	8
High	System/item operable, but at reduced performance level. User dissatisfied	7
Moderate	System/item operable, but comfort/convenience item inoperable	6
Low	System/item operable, but comfort/convenience item operate at reduced level	5
Very Low	Defect noticed by most customers	4
Minor	Defect noticed by average customers	3
Very Minor	Defect noticed by discriminating customers	2
None	No effect	1
Example of a Simplified Categorization		
Critical	Death, loss of system, violation of governmental statute	
High	Injury, loss of some system functions, very high economic loss	
Moderate	Damage to system requiring maintenance at first opportunity, economic loss	
Low	Minor damage to system, low economic loss	
Negligible	Cosmetic damage, no economic loss	
RCM Analysis		
Safety	Directly and adversely effects on operating safety	
Operational	Prevents the end system from completing a mission	
Economic	Does not adversely affect safety and does not adversely affect operations - the only effect is the cost to repair the failure	

7-4 FUNDAMENTALS OF RCM.

7-4.1 Objectives of RCM.

This chapter provides a discussion of the two primary objectives of RCM: Ensure safety through preventive maintenance actions, and, when safety is not a concern, preserve functionality in the most economical manner. For C5ISR facilities, mission should be considered at the same level as safety.

7-4.2 Applicability of Preventive Maintenance.

7-4.2.1 Effectiveness.

PM can be effective only when there is a quantitative indication of an impending functional failure or indication of a hidden failure. That is, if reduced resistance to failure can be detected (potential failure) and there is a consistent or predictable interval between potential failure and functional failure, then PM is applicable. Condition monitoring has long been used to monitor operating parameters that have been shown to be dependable predictors of an impending failure. Age limit information can also be utilized to determine effectiveness of preventative maintenance efforts (see Figure 7-6). Preventive maintenance (PM) is effective if a potential failure condition is definable or there is a quantitative indication of an impending failure. PM is generally effective only for items that wear out. It has no benefit for items that have a purely random pattern of failure (such as, failures are exponentially distributed, and the failure rate is constant – see Appendix B for a discussion of statistical distributions). Consequently, performing a PM action for electronics is rare, if ever, since electronics exhibit a random pattern of failures. Mechanical items, on the other hand, usually have a limited useful period of life and then begin to wear out.

7-4.2.2 Economic Viability.

The costs incurred with any PM being considered for an item must be less than for running the item to failure. The failure may have operational or non-operational consequences. The costs to be included in such a comparison for these two failure consequences are Operational and Nonoperational.

7-4.2.2.1 Operational.

The operational cost is defined as the indirect economic loss because of failure plus the direct cost of repair. An example of an operational cost is the revenue lost by an airline when a flight must be canceled and passengers booked another airline. For military organizations where profit is not an objective, an operational cost might be the cost of a second flight or mission. Sometimes, it may be difficult for a military organization to quantify an operational cost in terms of dollars and a subjective evaluation may be needed.

7-4.2.2.2 Non-Operational.

The non-operational cost is defined as the direct cost of repair. The direct cost of repair is the cost of labor, spare parts, and any other direct costs incurred because of repairing the failure (by removing and replacing the failed item or performing in-place repair of the item).

7-4.2.3 Preservation of Function.

The purpose of RCM is not to prevent failures but to preserve functions. Many maintenance people who are unfamiliar with RCM initially find this idea difficult to accept. For many years prior to and following World War II, the "modern" view within the maintenance community was that every effort should be made to prevent all failures. Preventing failure was the focus of every maintenance technician. But products became increasingly complex and maintenance costs increased both in absolute terms and as a percentage of a product's total life cycle costs. It was soon clear that preventing all failures was technically and economically impractical. Instead, attention was turned to preserving all the essential functions of a product. This shift from preventing failures to preserving function was fundamental to the development of the RCM approach to defining a maintenance program.

7-4.2.4 Opportunity Cost.

From time to time manufactures of equipment improve existing equipment maintenance capabilities by providing an improved part of a more effective maintenance process. Both can contribute to a cost-effective improvement of the overall RCM plan. Manufactures in general desire to improve their equipment and track performance and maintenance issues for continuous improvement and to keep ahead of competition.

7-4.3 Failure.

For RCM purposes, three types of failures are defined: functional, evident, and hidden.

7-4.3.1 Types of Failures.

7-4.3.1.1 Functional Failure.

A functional failure is one in which a function of the item is lost. A functional failure directly affects the mission of the system. To be able to determine that a functional failure has occurred, the required function(s) must be fully understood. As part of a FMEA, all functions have been defined. This definition can be very complex for products that have varying levels of performance (for example, full, degraded, and loss of function).

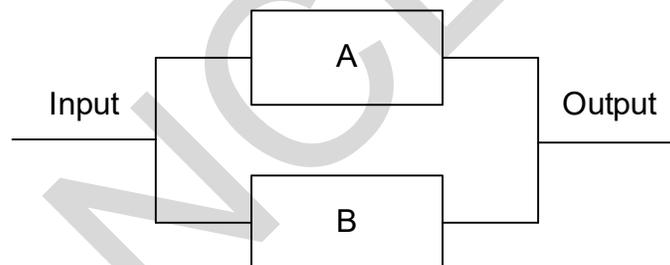
7-4.3.1.2 Evident Failures.

When the loss of a function can be observed or is made evident to the operator, the failure is said to be evident. In the latter case, dials or displays, audible or visual alarms, or other forms of instrumentation alert the operator to the failure.

7-4.3.1.3 Hidden Failures.

A hidden failure is a functional failure of an item that has occurred, has not affected performance of the end system, and is not evident to the operator, but will cause a functional failure of the end system if another item fails. In other words, because of redundancy or the nature of the item's function in the system, no single-point failure of the end system has occurred. If, on the other hand, multiple failures occur, then the system will fail to perform its function. A simple example is the system shown in Figure 7-7. Either of the two redundant items, A and B, can perform a critical function. Redundancy was used because the function is critical and a single point failure was unacceptable. If either item A or B can fail without the knowledge of the operator, it is considered a hidden failure. The system would now be subject to a single point failure (such as, the function can be lost by one more failure – the failure of the other redundant component). Hidden failures must be found by maintenance personnel.

Figure 7-7 Block Diagram of A simple Redundant System



7-4.3.2 Consequences of Failure.

A basic objective of the RCM analysis is to make decisions regarding the selection of a maintenance action for a specific functional failure of a specific item based on the consequence of the failure. Three categories of failure consequences are generally used. They are safety, operational (mission), and economic.

7-4.3.2.1 Safety.

If a functional failure directly has an adverse effect on operating safety, the failure effect is categorized as Safety. The functional failure must cause the effect by itself and not in combination with other failures. That is, the failure must be a single-point failure. (Note that a hidden failure for which no preventive maintenance is effective and which, in combination with another failure, would adversely affect safety must be treated as a safety-related failure. The methodology is designed to address this situation).

7-4.3.2.2 Operational.

When the failure does not adversely affect safety but prevents the end system from completing a mission, the failure is categorized as an Operational failure. For many end systems, operational failure results in loss of revenue. In other cases, a critical objective cannot be met. See Table 7-7 for examples.

(a) An adverse effect on safety means that the result of the failure is extremely serious or catastrophic. Results can include property damage, injury to operators or other personnel, death, or some combination of these.

(b) In some industries, this category is expanded to include failures that result in a federal statute being violated. An industry such as the petroleum or power industry often includes failures that would result in violations of the Environmental Protection Act. Other industries may include failures with other effects in this category.

Table 7-7 Examples of Effects of Operational Failures

End System	Effect of Operational Failure
Airliner	Airline must cancel flight and either send passengers to another airline or add a flight. In either case, revenue is adversely affected.
Manufacturing equipment	Production must be halted until repairs are made adversely affecting sales. Some orders may be canceled because delivery dates cannot be met (unless no other sources can provide the product to the customers – in that case, loss of customer confidence may result affecting future sales).
Military aircraft	Prolonged or lost conflict, inability to respond to a political crisis in a timely manner, or exposure to a period of vulnerability
Financial information system	Loss of revenue due to an inability to make investments, penalties due to late payments, etc.
C5ISR Facility	Facility cannot provide necessary electrical power to support an assigned mission.

7-4.3.2.3 Economic.

When a functional failure does not adversely affect safety and does not adversely affect operations, then the failure is said to have an Economic effect. The only penalty of such a failure is the cost to repair the failure.

7-5 RCM PROCESS.

7-5.1 C5ISR Candidates for RCM Analysis.

It is important to note from the onset that an RCM analysis is not beneficial for all products. The criteria listed in Table 7-8 will help the analyst determine if an RCM analysis is potentially of value. There are three major systems comprising C5ISR facilities that are candidates for RCM analysis, mechanical systems, electrical systems, and control systems. All three combine to support the facilities mission and

provide the necessary environmental conditions to maintain operation of critical equipment and personnel. All the components shown in paragraph 7-5.1 are candidates for RCM optimization and require a maintenance program geared toward the mission requirement of the facility.

Table 7-8 Criteria for Applying RCM to Products

Criteria	Comment
Product has or is projected to have a large number of PM tasks.	Existing product already in service or new system for which the PM tasks were identified using an approach other than RCM.
Product maintenance costs are or are projected to be very high.	Existing product already in service. PM tasks identified using an approach other than RCM or RCM requires updating. New system for which maintenance tasks were identified using approach other than RCM
Product requires or is projected to require frequent corrective maintenance.	Existing product already in service. PM tasks either identified using an approach other than RCM or RCM requires updating. New System for which maintenance tasks were identified using an approach other than RCM.
Hazardous conditions could result from failure	New product, or existing product for which the PM tasks were identified using an approach other than RCM.

7-5.1.1 Mechanical Systems.

The types of mechanical systems typical for a C5ISR facility include those listed below.

- Chillers
- Boilers
- Cooling Towers
- HVAC distribution equipment including Fan Coil Units
- Valves
- Piping

7-5.1.1.1 Other Systems.

Mechanical systems also include generators, fuel oil delivery systems and storage and pumping components. These are critical to the mission of the facility but are frequently neglected.

7-5.1.1.2 Temperatures.

Mechanical systems not only maintain a comfortable environment for the occupants but are also designed to maintain optimal equipment operating temperatures.

7-5.1.2 Electrical Systems.

Electrical systems begin at the transformer feeding the building or the 13.8kV feeder and continue through the entire distribution system generally to the panels containing the 220 or 208/120-volt distribution. Some facility mission requirements require solutions all the way to the operating equipment at the wall outlet. Typical components comprising the electrical system include those listed below.

- Transformer, liquid filled and air cooled
- Connections
- Cables
- Switch Gear
- Circuit Breakers
- Motor Control Centers
- Motors
- Cable Connections
- UPS systems including Gel and Wet Cell Lead Acid Batteries

7-5.1.3 System Controls.

Control systems are the third major component making a C5ISR facility as reliable as possible. Control systems are the brains behind the operational characteristics during normal and abnormal conditions. Control systems are commonly identified as SCADA systems and are designed to monitor conditions and react in a manner to maintain a set point. Typical SCADA systems are comprised of a series of sensors sending signals to a central command center where the signals are interpreted. Signals are sent from the command center to actuators to throttle input conditions and provide the necessary environmental condition required for the mission operations. Typical components for a SCADA system are listed below.

- Computer access panel
- Digital drivers
- Power Supplies
- PLC
- Interface devices such as control panels or circuit breakers

7-5.2 RCM Data Sources.

Conducting an RCM analysis requires an extensive amount of information. Since much of this information is not available early in the design phase, RCM analysis for a new product cannot be completed until just prior to production. Table 7-9 lists some general sources of data for the RCM analysis. The data elements from the FMEA that are applicable to RCM analysis are highlighted in paragraph 7-5.4.2. Note that when RCM is being applied to a product already in use, or when a maintenance program is updated during Life Exploration, historical maintenance and failure data will be inputs for the analysis.

Table 7-9 General Data Sources for the RCM Analysis

Data Source	Comment
Lubrication requirements	Determined by designer. For off-the-shelf items being integrated into the product, lubrication requirements and instructions may be available.
Repair manuals	For off-the-shelf items being integrated into the product.
Engineering drawings	For new and off-the-shelf items being integrated into the product.
Repair parts list	
Quality deficiency reports	For off-the-shelf items being integrated into the product.
Other technical documentation	For new and off-the-shelf items being integrated into the product.
PREP Database	For new and off-the-shelf items being integrated into the product.
Recorded observations	From test of new items and field use of off-the-shelf items being integrated into the product.
Hardware block diagrams	For new and off-the-shelf items being integrated into the product.
Bill of Materials	For new and off-the-shelf items being integrated into the product.
Functional block diagrams	For new and off-the-shelf items being integrated into the product.
Existing maintenance plans	For off-the-shelf items being integrated into the product. Also, may be useful if the new product is a small evolutionary improvement of a previous product.
Maintenance technical orders/manuals	For off-the-shelf items being integrated into the product
Discussions with maintenance Personnel and field operators	For off-the-shelf items being integrated into the product. Also, may be useful if the new product is a small evolutionary improvement of a previous product.
Results of FMEA, FTA, and other reliability analyses	For new and off-the-shelf items being integrated into the product. Results may not be readily available for the latter.
Results of Maintenance task analysis	For new and off-the-shelf items being integrated into the product. Results may not be readily available for the latter.

7-5.2.1 C5ISR Data Sources.

RCM related data may be obtained from several different types of sources. Some potential sources of maintainability data include those listed below.

- Historical data from similar products used in similar conditions (PREP Database, IEEE Gold Book)
- Product design or manufacturing data
- Test data recoded during demonstration testing

- Field data

7-5.2.1.1 Expressing Data.

The data maybe expressed in a variety of terms. These include observed values or modified values (true, predicted, estimated, extrapolated, etc.) of the various maintainability measures. Some precautions are therefore necessary regarding the understanding and use of such data as listed below.

- Historical – Used primarily during the concept definition phase to generate specifications requirements. In later phases historical data may be compared with actual data obtained for the product. They can also serve as additional sources of information for maintainability verification.
- Product Design and Manufacturing – Data obtained using design analysis or prediction, or from data generated during the design phase or the manufacturing phase. Design data may be used as the basis for product qualification and acceptance, review and assessment of historical data relevancy and the validity of previous assessments. Before this type of data is used in an analysis the analyst must understand the data collection and analysis methodology, why the specific method was chosen, and any possible limitations.
- Product Demonstration and Field – These data are essential for sustaining engineering activities during the in-service phase of the system life cycle. They include maintainability related data obtained from formal or informal demonstration test on mock-ups, prototypes, or production equipment in either a true or simulated environment or data generated during actual item use.

7-5.2.1.2 Other Data Categories.

Other categories of data that would be beneficial to collect include information on the maintenance support conditions. Operational maintainability may not be determined solely by inherent maintainability, but by logistical factors. Therefore, information to be collected should include shortages in spares (due to inadequate initial provisioning, long pipeline times, etc.), test resources, and human resources. Such data are important to determine why a system's maintainability as measured in the field, may not be meeting the values expected based on the design data.

7-5.2.1.3 SCADA Systems.

SCADA systems are excellent data collection mechanisms, providing the system is initially designed to capture critical information. It can also be utilized to monitor trends of component operational conditions to provide information on proactive logistics supplies.

7-5.3 PM Tasks Under RCM.

7-5.3.1 Lubrication and Servicing Task.

Many mechanical items in which movement occurs require lubrication. Examples include internal combustion engines that require oil and periodic replacement of that oil (and associated filters). Lubrication and servicing tasks are sometimes overlooked due their relative simplicity and because they are "obvious." Prior to the latest version of the airline's RCM approach, lubrication and servicing tasks were often omitted from the decision logic tree, with the understanding that such tasks cannot be ignored. In the current MSG-3, these tasks are explicitly included in the decision logic, as they are in this document.

7-5.3.2 Inspection or Functional Check Task.

Inspections normally refer to examinations of items to ensure that no damage, failure, or other anomalies exist. Inspections can be made of an entire area (for example, the body or "under the hood"), a subsystem (for example, the engine, controls, or feed mechanism), and a specific item, installation, or assembly (for example, the battery, shaft, or flywheel).

7-5.3.2.1 Visual Inspections or Checks.

These are checks conducted to determine that an item is performing its intended function. The check may be performed by physically operating the item and observing parameters on displays or gauges, or by visually looking to see if the function is being performed properly. In neither case are quantitative tolerances required. A functional check consists of operating an item and comparing its operation with some pre-established standard. Functional checks often involve checking the output of an item (for example, pressure, torque, voltage, or power) and checking to determine if the output is acceptable (such as, within a pre-established range, greater than a pre-established minimum value, or less than a pre-established maximum value). These checks are conducted as failure finding tasks.

7-5.3.2.2 Use of NDI.

Inspections may consist of purely visual examinations or be made using special techniques or equipment. Many inspections require the special capability of non-destructive inspection (NDI) techniques. Table 7-10 lists some of the NDI methods available to maintenance personnel.

Table 7-10 NDI Techniques

Main Application NDE Method	C	W	F	CR	E	L	MA	MC	S	D	MT	DT	PR	OTHER	Restrictions	Remarks
	Legend: C = Cracks; W = Wear; F = Fractures; CR = Corrosion; E = Erosion; L = Leaks; MA = Material Analysis; MC = Material Conditions; S = Stress; D = Deformation; MT = Material Thickness; DT = Deposit Thickness; PR = Physical															
1 Acoustic cross correlation						X										Locating buried pipes
2 Acoustic emission	X		X			X		X		X				X		Internal structural noise
3 Coating thickness												X		X		Magnetic methods and eddy currents. Ferrite content of ferritic-austenitic steels
4 Dye penetrant	X		X			X										Including the chalk, water, alcohol methods
5 Eddy current testing	X	X	X	X	X	X				X	X			X		Heat exchanger tubes, wire rope, surface checks, sorting
6 Emission spectroscopy (Metascope)							X									Low and high alloy steels. Including X-ray fluorescence
7 Endoscopy	X	X	X	X	X	X						X	X			Inspection of internal surface
8 ER-probe				X												Average corrosion rates
9 Ferrography		X														Lubricated mechanical systems
10 Hardness testing								X								Brinell, Vickers, Rockwell B, C&N, Rockwell superficial, Knoop, Shore, Scleroscope, Equotip, UCI
11 Hydrogen cell				X												Average corrosion rates
12 Isotope techniques		X				X		X			X	X	X	X		Tracer tech., ball test, radiometry, collim. Photon
13 Laser distance measurements (optocator)		X									X			X		Topography, symmetry
14 Leak testing resistance						X								X		Liquid penetrant, ultrasonics, pressure change, foam, tracers, sulphur diffusion, ozalide paper, halogen
15 LPR-probe, polarization				X												Instantaneous corrosion rate
16 Magnetic plugs		X														Lubricated mechanical systems
17 Magnetic particle examination	X													X		Weld defects, laminations – only ferromagnetic materials
18 Mechanical calibration		X		X	X						X	X		X		Physical dimensions
19 NDE method combination	X	X	X	X	X	X	X	X	X	X	X	X	X	X		Check of entire component condition. Predictive programs
20 NDE meth. under. dev.	(X)							(X)	(X)	(X)				(X)		
20.1 SPAT									X							Stress pattern analysis by thermal emission
20.2 Pulsed video thermography (PVT)								X						X		Composite materials. Glued metals, delamination, and coatings.
20.3 Moire contour										X				X		Topography

Table 7-10 NDI Techniques (cont'd)

Main Application NDE Method	C	W	F	CR	E	L	MA	MC	S	D	MT	DT	PR	OTHER	Legend: C = Cracks; W = Wear; F = Fractures; CR = Corrosion; E = Erosion; L = Leaks; MA = Material Analysis; MC = Material Conditions; S = Stress; D = Deformation; MT = Material Thickness; DT = Deposit Thickness; PR = Physical
	Restrictions														Remarks
20.4 Holographic interferometry (HI)									X					X	Lack of adhesion, material defects, thin samples
20.5 Computerized tomography (CT)	X													X	Annual rings, knots, moisture, concrete column cross sections
20.6 Positron annihilation								X						X	Voids in metals. Fatigue in titanium
21 Noise measurements														X	Noise level, bearing checks
22 Pattern recognition	X	X	X	X	X					X	X	X	X		
23 P-scan	X	X	X	X	X						X			X	Weld inspection, stress corrosion, corrosion topography, creep defects. Full documentation
24 Pinhole														X	Coatings, high/low voltage
25 Pressure testing	X		X			X				X					Including vacuum testing. See also leak
26 Radiography	X	X	X	X	X	X					X	X	X	X	Check of joints, geometry, laminations, reinforced concrete, and corrosion/erosion
27 Replica technique	X	X	X					X		X				X	Surface microstructure, crack type, wear grooves, topography
28 Spectrometric oil analysis programs		X													Lubricated mechanical systems
29 Strain gauge technique									X	X					Weight, pressure, oscillation
30 Stroboscopy	X	X	X											X	Visual condition monitoring, rotation direction and rate
31 Test coupons				X	X										Average corrosion rate
32 Thermography	X			X		X						X		X	Surface temp., bearing pressure, moisture, energy loss
33 Ultrasonic leak, detection						X								X	Electrical discharge, flow
34 Ultrasonics	X	X	X	X	X	X		X	X	X	X				Including sound attenuation
35 Vibration monitoring	X	X	X											X	Machinery includes bearings, gears, turbines, centrifuges, etc.
36 Visual inspection	X	X	X	X	X	X	X			X		X	X		Spark pattern & chemical analysis
37 X-ray crawlers														X	Checking welds inside pipes
38 X-ray diffraction									X						Measurement residual stresses

7-5.3.3 Restoration Task.

Many items, primarily mechanical, wear out as they are used. At some point, it may be necessary, and possible, to restore the item to "like new" condition. Examples include internal combustion engines, electric motors, and pumps.

7-5.3.4 Discard Task.

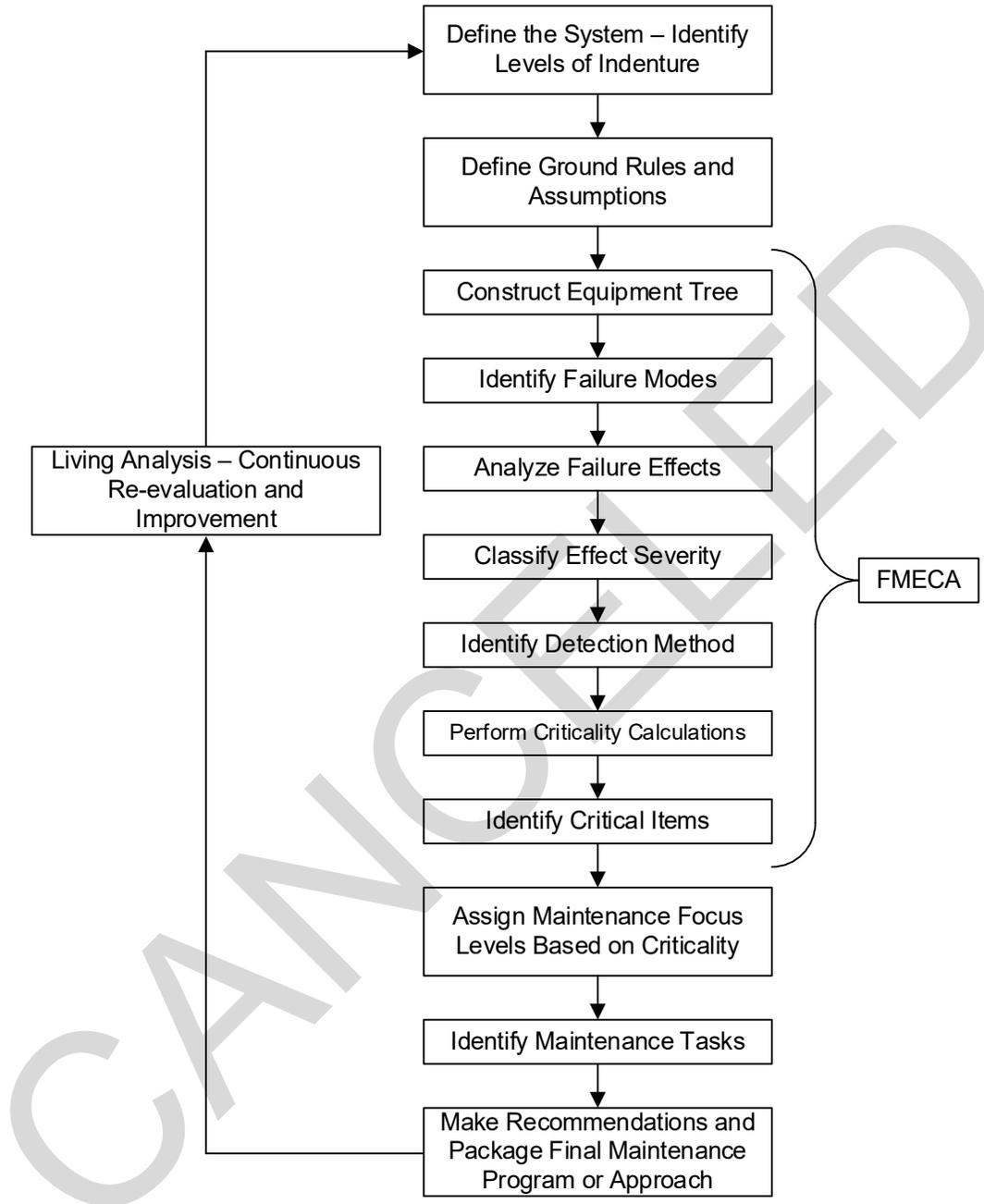
Some items upon failure or after their useful life has been reached (such as, they are worn out), cannot be repaired or restored. These items must be discarded and replaced with a new item identical in function. Examples include seals, fan belts, gaskets, screws (stripped threads), and oil filters.

7-5.4 The RCM Process.

The objective of conducting an RCM analysis is to rank all included equipment and systems by their relative importance, and risk, to the overall facility mission, and to prescribe PM tasks based on subsystem and system ranking. The RCM process is outlined below, by an expanded Figure 7-8, and following text.

- Define the System – Identify and document the boundaries of the analysis
 - Identify and document equipment included in the analysis
 - Identify and document the indenture level the analysis is intended to extend to
- Define Ground Rules and Assumptions – Identify and document ground rules and assumptions used to conduct the analysis
- Construct Equipment Tree – Construct equipment block diagrams to indicate equipment configuration, down to the lowest indenture level intended to be covered by the analysis
- Identify Failure Modes – Identify the potential failure modes for the analyzed equipment at the indenture levels covered by the analysis
- Analyze Failure Effects – Analyze the effects of the identified failure modes on the lowest levels of indenture and above
- Classify Effect Severity – Classify the effects of the identified failure modes on the lowest levels of indenture and above
- Identify Detection Method – Identify and classify the methods, in place, by which potential failures may be detected or avoided
- Perform Criticality Calculations – Perform Criticality Analysis

Figure 7-8 The RCM Process



- Identify Critical Items – Identify items within the analysis that ranked highly critical
- Assign Maintenance Focus Levels – Classify maintenance focus levels based on criticality rankings
- Apply RCM Decision Logic – Apply RCM logic trees for items, especially those identified as being critical

- Identify Maintenance Tasks – Identify maintenance tasks to be performed on the given item
- Package Maintenance Program – Develop a maintenance tasking schedule for the analyzed equipment

7-5.4.1 Identify the System Configuration.

Since the RCM analysis usually begins before the final design has been completed, the system configuration is changing. Even when the design is complete, model changes can be made. The configuration, of course, determines how functions are performed, the relationship of items within a product, and so forth. Consequently, it is important that the precise configuration of the product or system for which the RCM analysis is being conducted be documented as part of the analysis. It is also important that the analysis be updated to account for any changes in the configuration (some of which may be required as a direct result of the RCM analysis itself).

7-5.4.2 Perform a FMEA and Other Analyses.

To perform the RCM analysis, many pieces of information are needed. These include the information listed below.

- The types of failures that can occur in the product
- The failure characteristics of the items that make up the product being analyzed
- The nature of the failures (hidden, evident, safety, operational, ect.)
- The capabilities of the maintenance organization
- The maintenance concepts
- A thorough understanding of operation

Obviously, such information will probably not be known or be very shaky early in design. For that reason, the RCM analysis should not be started until sufficient and reasonably stable information is available. Of course, the objective is to develop and complete the initial maintenance program prior to the product being transferred to the customer.

RCM Analysis can be conducted using a traditional quantitative, qualitative, or flexible approach.

- Traditional quantitative approach can be used when there is sufficient failure rate data available to calculate criticality numbers. A quantitative approach is the preferred analysis method. However, to be effective, high levels of failure specific data must be available. When specific failure rates for specific failure modes and failure mechanisms are unavailable, analysis must be conducted qualitatively.

- Qualitative analysis must be used when specific part or item failure rates are not available. Therefore, failure mode ratio and failure mode probability are not used in this analysis. Instead, the equipment is ranked in terms of discrete occurrence levels. Under traditional qualitative analysis severity, occurrence, and detection method levels are determined subjectively and utilized to produce a component risk assessment.
- The flexible technique is born of traditional qualitative analysis. Under this approach, RPN calculations will be generated by the same formulas as given by traditional qualitative approach. However, the arguments of the component level RPN calculation (O , S , D) will be defined differently. See Equation 6-11.

7-5.4.2.1 Other Inputs.

When FTAs are needed to understand the effects of, for example, multiple failures, the information derived from these analyses can also be valuable inputs to the RCM analysis.

7-5.4.2.2 Other Information.

Other important sources of information for the RCM analysis include RBDs, Functional Block Diagrams, system requirements documents, descriptions of system applications, technical manuals/drawings/layouts, and indenture level identification system.

7-5.4.2.3 Sources.

To provide the needed information, various sources must be exploited. One of the most obvious sources is the body of analyses conducted as part of the design process. These include the Failure Mode and Effects Analysis (FMEA) or Failure Modes, Effects, and Criticality Analysis (FMECA), FTA, maintainability analysis, and so forth.

7-5.4.2.4 FMEA.

The FMEA can be a primary source of much of the information needed for the RCM analysis. Table 7-11 shows excerpts of the form prescribed in the Automotive Industry Group standard on FMEA/FMECA. Table 7-12 indicates the data in many of the columns can be directly used for the RCM analysis. The columns having data most applicable for the RCM analysis are shaded. In addition to those shown, columns can be added for functions, functional failure, compensating provisions, and three columns for failure effects: local effects, next higher level, and end effects. Other chart examples for recording FMECA data can be used as shown in Table 7-12. Further information is available in TM 5-698-4, Failure Modes, Effects and Criticality Analysis (FMECA) for C4ISR Facilities.

Table 7-11 Data Elements from FMEA that are Applicable to RCM Analysis

(Form from the Automotive Industry Group Standard on FMEA)

Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	S E V	C L A S S	Potential Cause(s)/ Mechanisms of Failure	O C C	Current Design Controls	D E T	R P N	Recommended Action(s)	Responsibility & Target Completion Date	Action Results				
												Action Taken	New Sev	New Occ	New Det	New RPN

Legend: SEV – Severity of failure effect

OCC – Probability of occurrence

DET – Method of detection

RPN – Risk Priority Number

A completed chart may be similar to the following example:

Table 7-12 Example of Failure Modes and Effects Analysis Worksheet; DA Form 7610

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	FAILURE RATE λ_p (SOURCE)	DETECTION METHOD	CRITICALITY NUMBER (C_M)
130.2	Cooling Tower #1/ maintain a water temp of 75°F.	Fan failure	Motor winding open, Loss of power to motor	3	10.0518x10 ⁻⁶	3	99.05X10 ⁻⁵
310.1	Air Handler/ Provide 3200cfm of air to room, maintain room at 72°F,	Provide airflow at a rate less than 3200cfm	Reduced motor output –winding degradation, belt slippage-belt too loose, loose sheave, Dirty intake filter	3	1.7657x10 ⁻⁶	2	1.06x10 ⁻⁵
310.0	Air Handler/ Provide 3200cfm of air to room, maintain room at 72°F,	Maintain air at a temp higher than 72°F	Dirty coils	3	1.7657x10 ⁻⁶	7	3.7x10 ⁻⁵

DA FORM 7610 AUG 2006

Where:

- Failure modes are the generic way an item failed
- Failure mechanisms are the specific circumstances that allowed the given failure mode to occur
- Severity is the assessment of the consequence of a given failure
- Occurrence is the probability of the failure occurring (failure rate)

7-5.4.3 Applying RCM Decision Logic.

The overall decision logic for applying the RCM methodology is depicted in Figure 7-9. The decision logic represented in this figure is adapted from that used in the Reliability Analysis Center's Master Steering Group –3 (MSG-3). The most significant difference is in the portions of the tree labeled ②, ④, ⑦, and ⑧. MSG-1 through MSG-3 used the term "safety" for these portions of the tree.

7-5.4.3.1 Safety.

Safety is of paramount importance to the airline industry, as it is in other industries, such as the nuclear power industry.

7-5.4.3.2 Other Critical Considerations.

Many industries have concerns that are as important, or nearly so, as safety considerations. The petroleum and chemical industries, for example, are subject to severe economic and even criminal penalties under Federal statutes for events in which the environment is polluted. For other industries, failures that result in the violation of other Federal, state, or local statutes, or in other unacceptable consequences may be treated as seriously as safety-related failures are in the airline industry. For that reason, in the portions of the tree labeled ②, ④, ⑦, and ⑧, the term "hazardous effects" is used rather than "safety effects". (The circled numbers in this and following discussions refer to a corresponding numbered portion of the referenced figures.) When applying RCM decision logic, it is important to consider the criticality of the current item. Highly critical items have the direct potential to compromise mission goals, and risk should be heavily mitigated. It is important to recognize single point failures, as well as their functional contribution to critical and non-critical systems, and to prescribe maintenance approaches accordingly. Conversely, some items recognized as being very non-critical may be allowed to run to failure, especially non-critical items that are inherently very reliable. This viewpoint should also be incorporated into the use of RCM decision logic to build an intelligent, and cost effective, maintenance strategy.

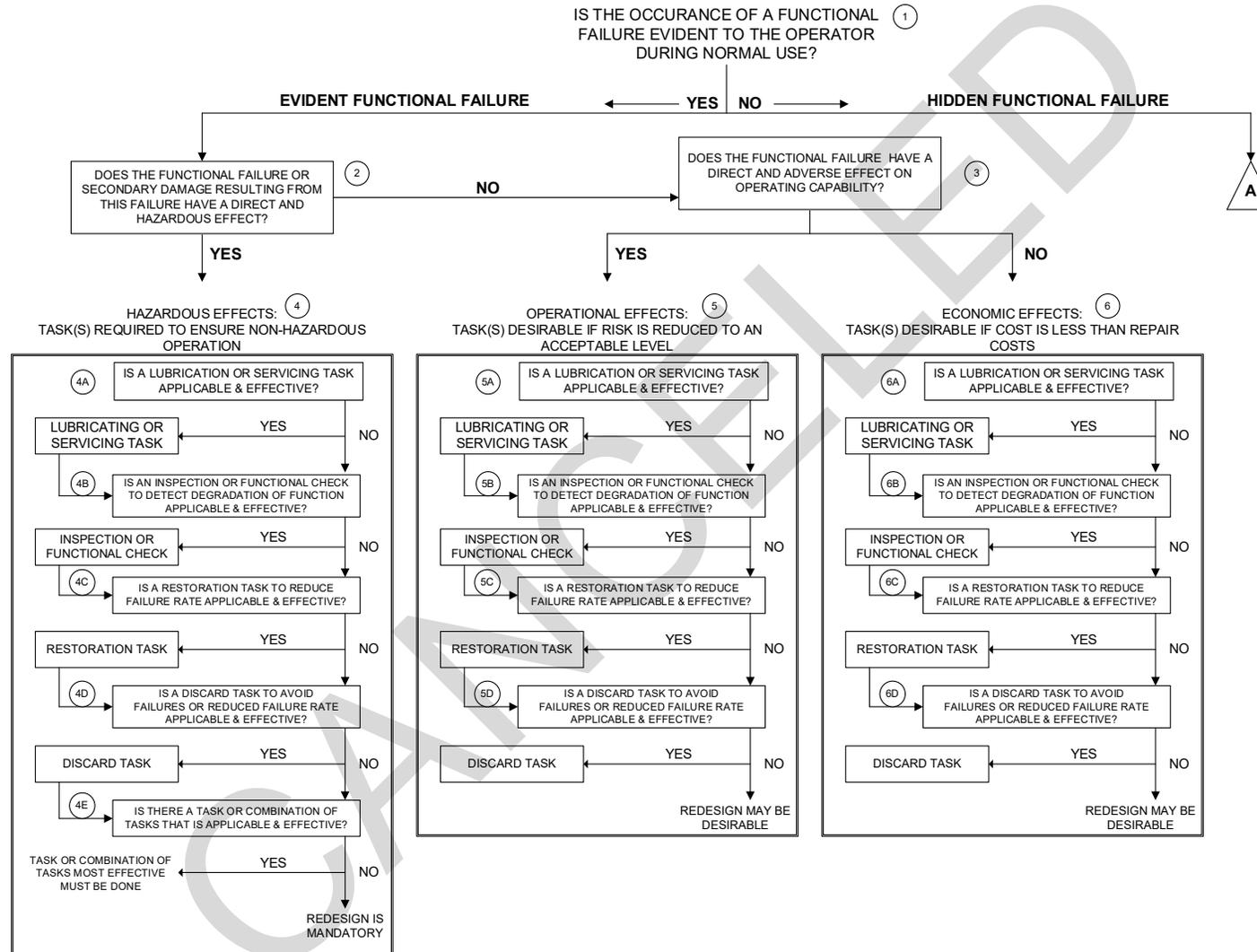
7-5.4.4 Use of Logic Tree.

As can be seen from Figure 7-9, the decision logic tree consists of a series of Yes-No questions. The answers to these questions lead to a specific path through the tree. The questions are structured to meet the objectives of the RCM analysis: ensure the safe (non-hazardous) and economical operation and support of a product while maximizing the availability of that product. This objective is met by selecting preventive maintenance (PM) tasks when appropriate, redesign, some combination of PM and redesign, and by corrective maintenance (CM) when PM is either applicable or effective.

(1) The first question asked is "Is the occurrence of a functional failure evident to the operator or (or user) during normal use?" A "No" answer means that the failure is hidden, and the analyst is directed to ⑦ in the tree. The portion of the tree below ⑦ is discussed under paragraphs 7-5.4.8 and 7-5.4.9. A "Yes" answer means that the failure can be observed or is made known to the operator/user, in which case, the analyst is directed to ②.

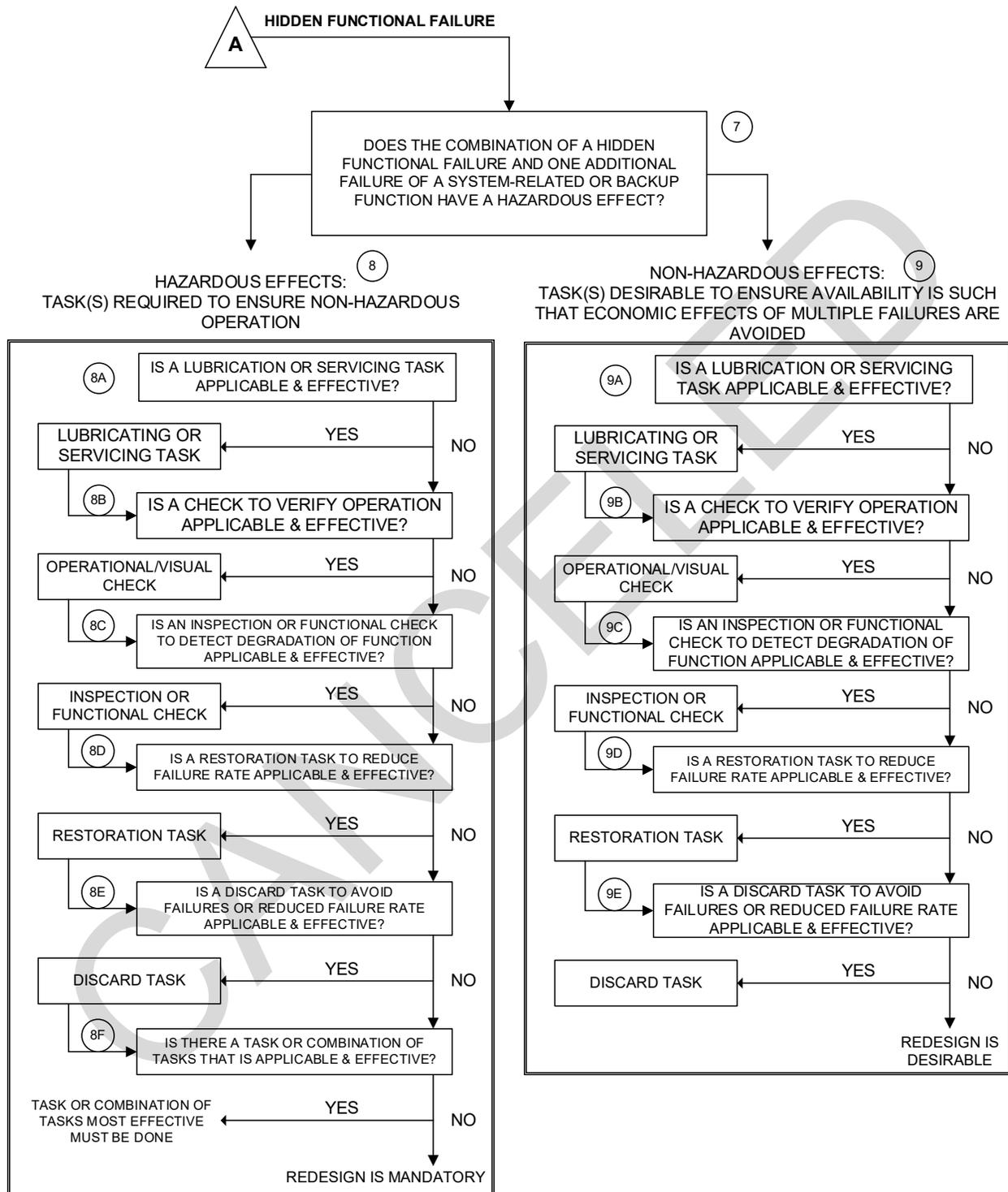
(2) At ②, the question is "Does the (evident) functional failure or secondary damage resulting from the functional failure have a direct and hazardous effect?" A "Yes" answer directs the analyst to ④. The portion of the tree below ④ is discussed under paragraph 7-5.4.5. A "No" answer directs the analyst to ③. The portion of the tree below ③ is discussed under paragraphs 7-5.4.6 and 7-5.4.7.

Figure 7-9 RCM Decision Logic Tree (Adapted from MSG-3)



* Hazardous effects include property damage, injury or death to operators or other people, violation of Federal environmental or health statutes, and other effects determined by the company or industry to be serious or catastrophic.

Figure 7-9 RCM Decision Logic Tree (Adapted from MSG-3) (cont'd)



* Hazardous effects include property damage, injury or death to operators or other people, violation of Federal environmental or health statutes, and other effects determined by the company or industry to be serious or catastrophic.

7-5.4.5 Evident Failure – Hazardous Effects.

The portion of the decision logic tree that deals with situations where an evident functional failure has hazardous effects is shown in Figure 7-10.

(1) This portion of the tree steps the analyst through a series of questions intended to identify all PM tasks that will reduce to an acceptable level the probability of occurrence of the functional failure that results in the effects, reduce the effects to purely operational or economic effects, or result in a combination of these two improvements.

(2) If none of the PM tasks listed is either applicable or effective, then redesign is mandatory. The reason for making redesign mandatory is obvious. The effects categorized as "hazardous" are unacceptable. Consequently, when PM cannot fulfill any of the objectives listed, a redesign the product must be performed to eliminate the mode of failure that causes the hazardous effects, reduce to an acceptable level the probability of occurrence of the functional failure that results in the effects, or result in a combination of these two improvements.

7-5.4.6 Evident Failure – Operational Effects.

The portion of the decision logic tree that deals with situations where an evident functional failure has a direct and adverse effect on operating capability is shown in Figure 7-11. This portion of the tree steps the analyst through a series of questions intended to identify all PM tasks that will reduce the risk of failure to an acceptable level. If none of the PM tasks listed is either applicable or effective, then redesign may be desirable. The cost of a functional failure that results in operational effects includes both the cost of the PM and the economic cost incurred because of the end system not completing a mission or being able to perform its function(s).

(1) If the costs exceed the cost to redesign the product, redesign is economically justified. The purpose of the redesign would be to eliminate the mode of failure that causes the operational effects, reduce to an acceptable level the probability of occurrence of the functional failure that results in the effects, or some combination of these.

(2) Even if redesign is economically justified, other considerations, such as schedule, may outweigh the advantages gained.

Figure 7-10 Evident Failure – Hazardous Effects

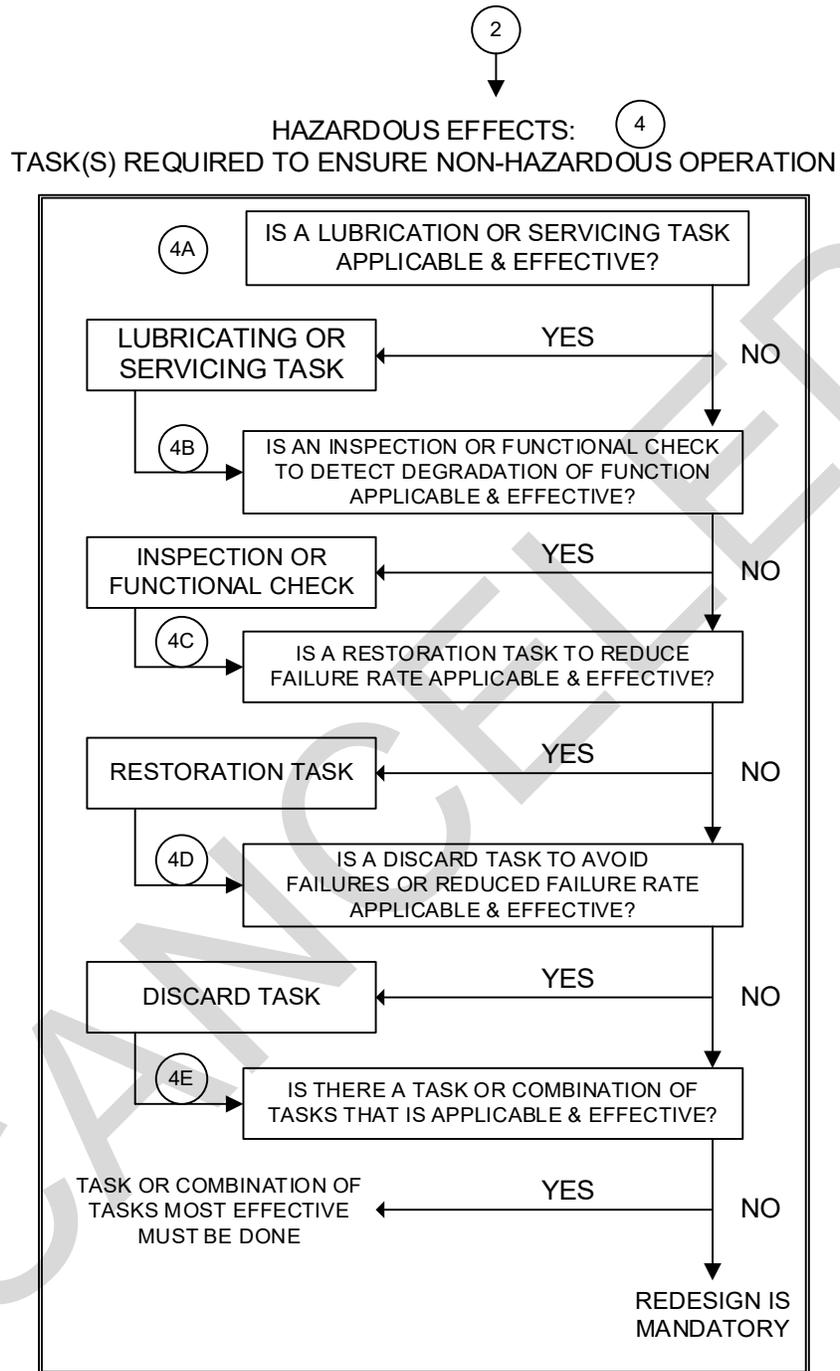
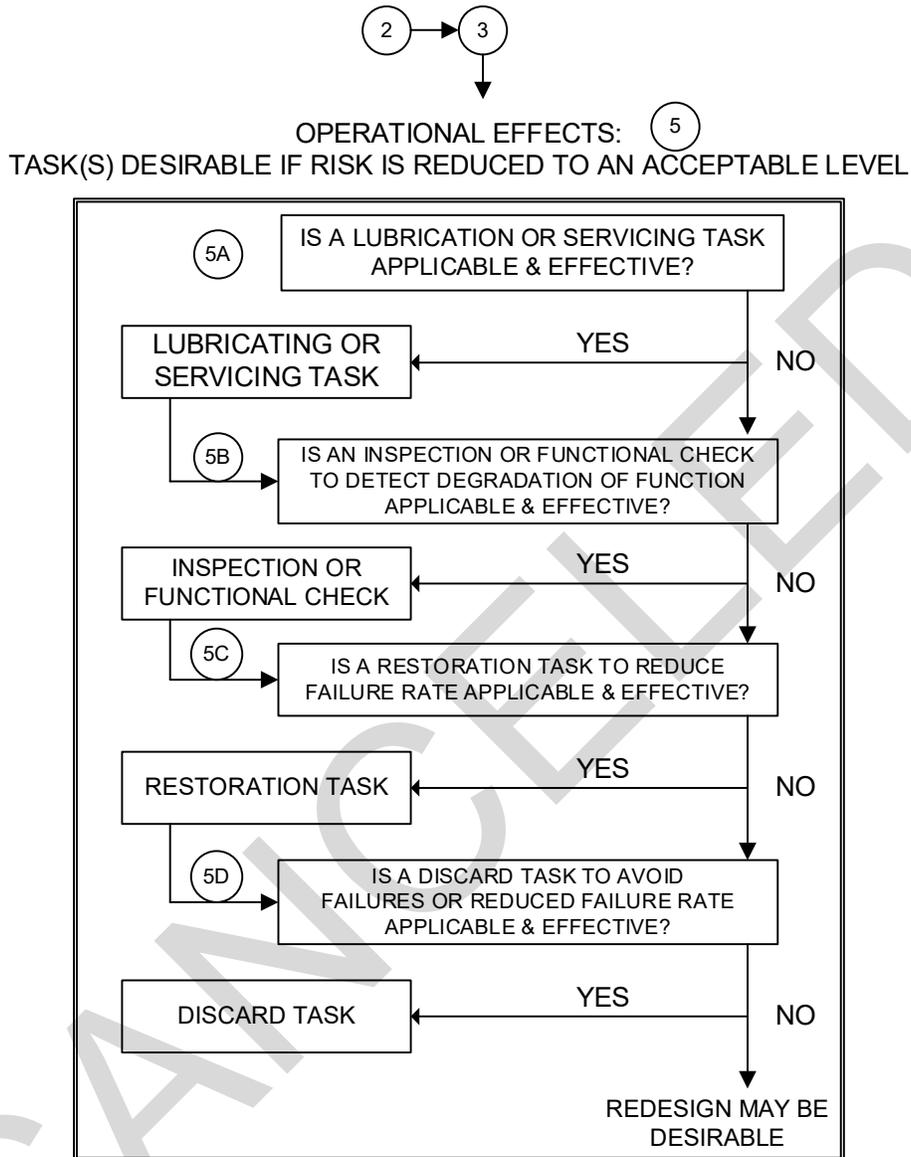


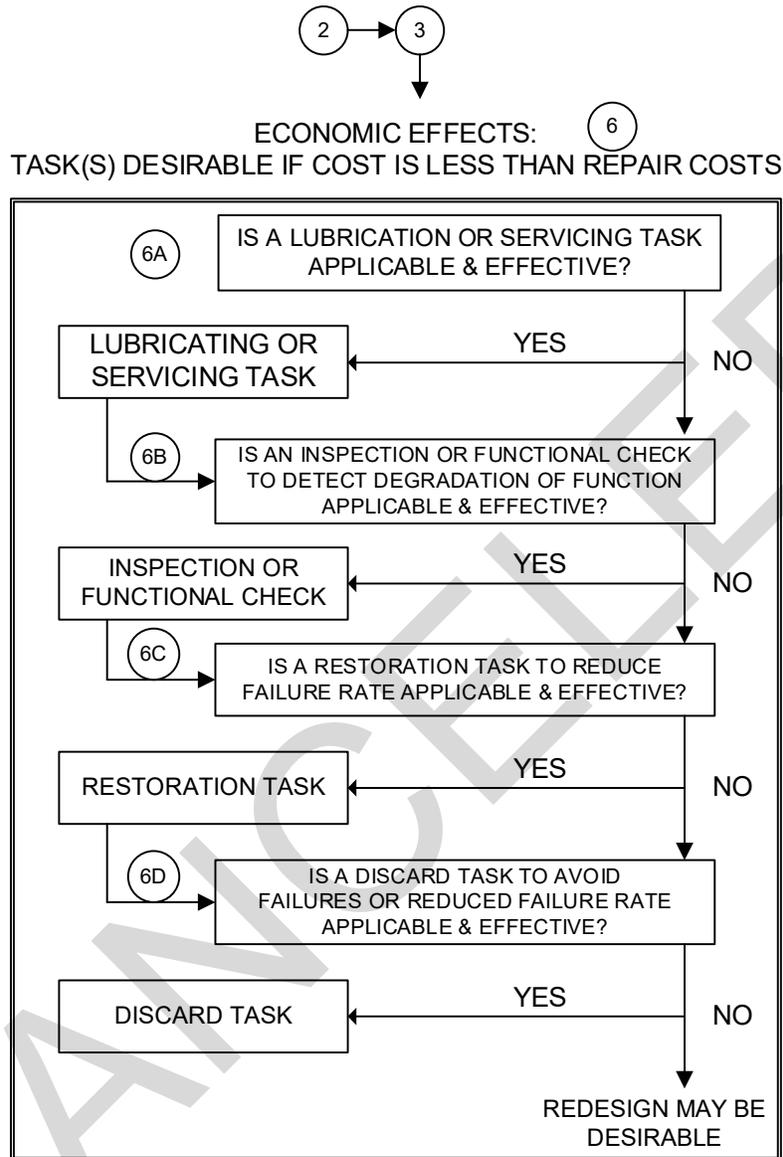
Figure 7-11 Evident Failure – Operational Effects



7-5.4.7 Evident Failure – Economic Effects.

The portion of the decision logic tree that deals with situations where an evident functional failure has only an economic effect is shown in Figure 7-12. This portion of the tree steps the analyst through a series of questions intended to identify all PM tasks that are desirable if their costs are less than the cost of repair. If none of the PM tasks listed is either applicable or effective, then redesign may be desirable. Again, the decision to redesign or not redesign is one of economics. If redesign is less than the economic effects of the failure, then it may be desirable. Otherwise, redesign is not justified.

Figure 7-12 Evident Failure – Economic Effects



7-5.4.8 Hidden Failure – Hazardous Effects.

The portion of the decision logic tree that deals with situations where a hidden functional failure has a hazardous effect in combination with another failure is shown in Figure 7-13. This portion of the tree steps the analyst through a series of questions intended to identify all PM tasks that are required to ensure non-hazardous operation. The tasks are effective if they reduce to an acceptable level the probability of occurrence of the functional failure that results in the effects, reduce the effects to purely operational or economic effects, or result in a combination of these.

(1) If none of the PM tasks listed is either applicable or effective, then redesign is mandatory. The reason for making redesign mandatory is obvious. The effects categorized as "hazardous" are unacceptable. Consequently, when PM cannot fulfill any of the objectives listed, a redesign must be performed the product to eliminate the mode of failure that causes the hazardous effects, reduce to an acceptable level the probability of occurrence of the functional failure that results in the effects, or result in a combination of these.

(2) Note that by redesigning to make the failure evident, the effects might be reduced to purely economic or operational.

7-5.4.9 Hidden Failure – Non-Hazardous Effects.

The portion of the decision logic tree that deals with situations where a hidden functional failure has a non-hazardous effect is shown in Figure 7-14. This portion of the tree steps the analyst through a series of questions intended to identify all PM tasks that are desirable to ensure availability is sufficiently high to avoid the economic effects of multiple failures. If none of the PM tasks listed is either applicable or effective, then redesign is desirable.

Figure 7-13 Hidden Failure – Hazardous Effects

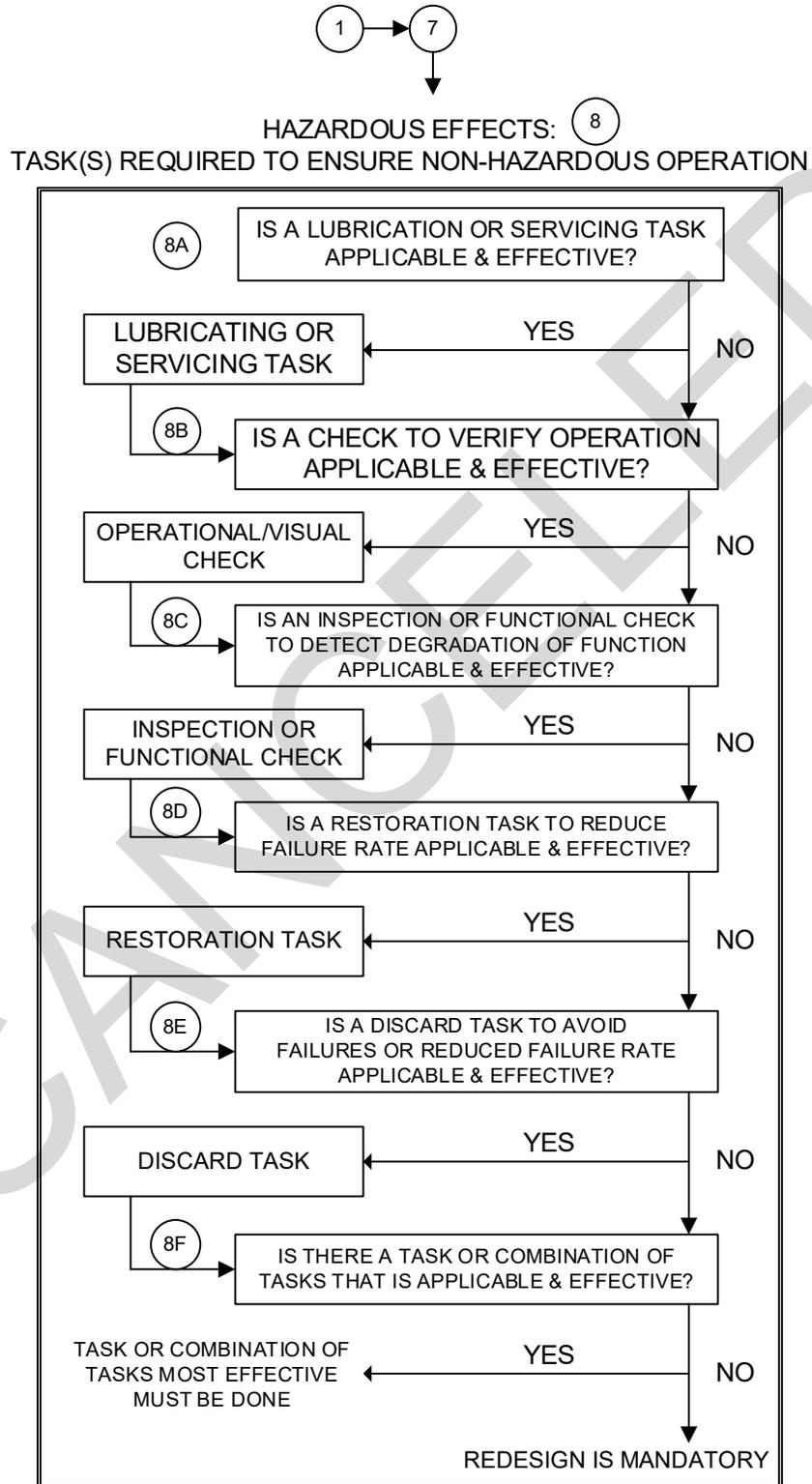
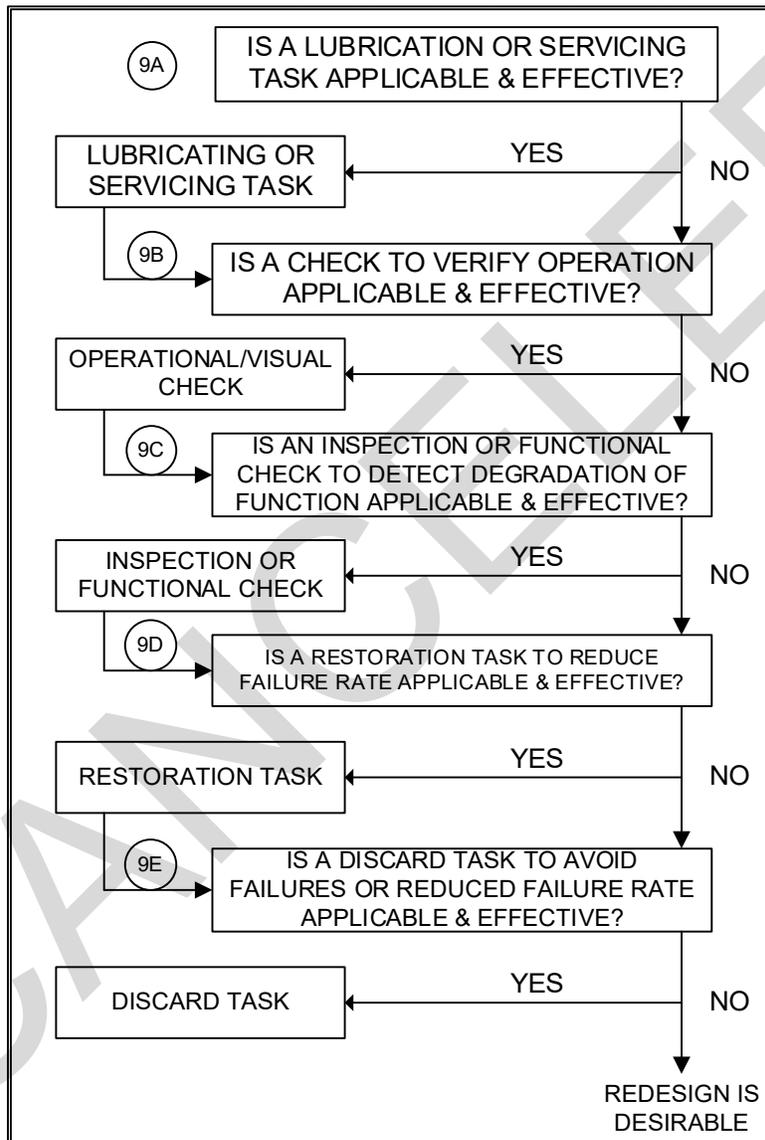


Figure 7-14 Hidden Failure – Non-Hazardous Effects

1 → 7
 ↓
 NON-HAZARDOUS EFFECTS: 9
 TASK(S) DESIRABLE TO ENSURE AVAILABILITY IS SUCH THAT ECONOMIC EFFECTS OF MULTIPLE FAILURES ARE AVOIDED



7-5.4.10 Package Final Maintenance Program.

The result of the RCM analysis will be a set of preventive maintenance (PM) tasks and, by default, a set of corrective maintenance (CM) tasks. PM will consist of on-condition and scheduled maintenance.

(1) Frequency of tasks. The frequency with which each of the scheduled PM tasks must be performed will no doubt vary from item to item. It is also probable that many of these tasks may be grouped and performed together at some calendar or operating time interval. The process of grouping the scheduled tasks into sets of tasks to be performed at some prescribed time is called "packaging" the maintenance program.

(2) Example of packaging. For example, it may be that for a given product that the scheduled tasks listed below were identified.

- Three visual inspections: A to be conducted every 45 hours of operation, B to be conducted every 52 hours of operation, and C to be conducted every 105 hours of operation.
- A lubrication performed every 55 hours of operation
- A non-destructive inspection every 100 hours of operation
- An overall task performed when a stated operating characteristic is out of limits
- A hard-time replacement task every 60 hours of operation

One way to package these tasks is listed below.

- Conduct the following PM every 50 operating hours (such as, at 50, 100, 150, 200, ect.)
 - Visual Inspections A and B
 - Lubrication
 - Hard-time replacement
- Conduct the following PM every 100 operating hours (such as, at 100, 200, 300, ect.)
 - Visual inspection C
- Perform overhaul task whenever the operating characteristic goes out of limits

Note that at the 100, 200, 300, etc. hour points, all the tasks except the overhaul task are performed. This example is purposely over-simplified, and many other factors may (and probably will) have to be considered when packaging the tasks. The point is that by packaging PM tasks, maintenance resources are used as effectively as possible and minimize the downtime of the product for PM.

7-5.4.11 Continuously Improve the Maintenance Program.

Given the possibility for errors in the initial maintenance program, it is prudent to implement the RCM process as an on-going effort, one requiring perpetual evaluation and adjustment, as depicted in Figure 7-8. The process for continuously improving the RCM-based maintenance program consists of Maintenance Audit, Trend Analysis, and Life Exploration. The purpose of this process is to continuously improve the initial maintenance program developed using the RCM concept.

7-5.4.11.1 The Initial Maintenance Program.

The maintenance program that is developed based on the RCM analysis done prior to the first product being delivered to the customer is the initial maintenance program. This initial program will have been based on the best information that was available at the time the analysis was performed. One of the critical pieces of information is the underlying failure distribution for each item. The information used in the initial RCM analysis was based on a mix of analysis and test results. When off-the-shelf items are used in the product, the information can include actual field experience. It must be recognized, however, that some of the information will not be 100% accurate.

7-5.4.11.2 Maintenance Audit.

Auditing the maintenance performed in actual service provides the data needed to refine and improve the maintenance program. In analyzing the data, the maintenance analysts and planners attempt to address the technical content of the program, intervals for performing tasks, packaging of tasks, training, the maintenance concept, and the support infrastructure.

(a) In addressing technical content, analysts and planners must determine if the current maintenance tasks cover all identified failure modes and result in the desired/required level of reliability. Failure modes may have been missed or the current maintenance tasks may not be effectively addressing identified failure modes. The latter may result from incorrectly identifying the underlying failure probability distribution function. Much of this information can be confirmed or updated through a reliability assessment. Listed below are the type of questions that can be answered by such an assessment.

- Were assessments of useful life too conservative?
- Have replacement intervals been made too short?
- Is wearout occurring later or earlier than anticipated?
- Have the operating conditions or concept changed?
- Has the reliability performance been as expected?
- Have any new failure modes been uncovered?

- Are failure modes identified in development occurring with the expected frequency and pattern (such as, underlying pdf of failures)?
- Have any modifications to the product been made or are any planned that would add or delete failure modes, change the effects of a given failure mode, or require additional or different PM tasks?
- Were the consequences of failures forecast during development adequately identified?

(b) In addressing performance interval, analysts and planners must determine if the intervals for PM tasks result in decreased resistance to failure. Most often, the objective is to extend the interval as much as possible, without compromising safety, when doing so will reduce costs. Initial intervals are frequently set at conservative levels.

(c) In addressing task packaging, analysts and planners must determine if like tasks with similar periodicity are or can be grouped together to minimize downtime and maximize effectiveness. Lessons learned during actual operation and maintenance may make it necessary to revise the initial packaging.

(d) The analysts and planners should evaluate if available personnel, as currently being trained and using available tools and data, are effectively performing the identified PM tasks. If not, changes to training, procedures, tools, and so forth should be considered.

(e) The analysts and planners should determine if the maintenance concept for the product is effective or should be revised.

(f) The analysts and planners should address the adequacy and responsiveness of the support infrastructure. If the performance of the infrastructure is not as anticipated, recommendations regarding policy, spares levels, and other factors should be considered.

7-5.4.11.3 Trend Analysis.

By collecting data on failures, time to failure, effectiveness of maintenance tasks, and costs of maintenance, trends can be identified. The objective of trend analysis is to anticipate problems and adjust the maintenance program to prevent their occurrence. For the RCM effort, two factors typically addressed by trend analysis are the rate of occurrence of failures and maintenance costs.

(a) For trending purposes, at least three data points are needed. The first two establish the trend (positive or negative) and the third serves as confirmation. In control charting used for quality control, a trend is said to exist when 7 consecutive points continue to rise or fall. However, when measurements are based upon sample surveys over time, data at different points in time may vary because the underlying phenomenon has changed (such as, a trend exists) or due to sampling error (such as, the underlying

phenomenon has not changed at all). It is not an easy task to seek out the one from the other.

(b) Statistical methods can be used to determine if a trend exists. For example, if a system failure rate is changing (such as, it is not constant), the Laplace Statistic will show that a trend exists at a certain level of confidence. The Laplace transform is an integral transform perhaps second only to the Fourier transform in its utility in solving physical problems. The Laplace transform is particularly useful in solving linear ordinary differential equations such as those arising in the analysis of electronic circuits (Wolfram MathWorld).

(c) In addition to trend analysis, impending failures can be detected using pattern recognition, data comparison, tests against limits and ranges, correlation, and statistical process analysis.

7-5.4.11.4 Life Exploration.

The process of collecting and analyzing in-service or operational reliability data to update the maintenance program is called Life (or Age) Exploration. The data that should be collected during Life Exploration includes historical field service data. Historical field service data typically describes three kinds of maintenance activities: corrective maintenance actions, preventive maintenance action, and service maintenance action.

(a) Historical corrective maintenance data. Corrective maintenance actions occur in response to an operational failure of the system. Corrective maintenance actions are always unscheduled, unwanted, inconvenient, and random.

(b) Historical preventive maintenance data. Preventive maintenance actions occur in accordance with a schedule and are intended to minimize the need for corrective maintenance actions.

(c) Historical service maintenance data. Service maintenance actions are those tasks performed to replenish expended parts and supplies required to operate a system. Many assets require adjustment, replenishment of supplies, lubrication, and cleaning.

7-5.5 Specific Considerations for Implementing RCM for C5ISR Facilities.

7-5.5.1 Current Versus New Facilities.

Many C5ISR facilities were built, and the mechanical and electrical equipment developed and installed without an RCM analysis having been conducted. Implementing RCM for an existing C5ISR facility, when the current PM program was not based on RCM, is different from implementing it on a facility, new or old, for which the PM program was based on RCM.

7-5.5.1.1 Current PM Program in Place.

Of course, a program of preventive maintenance will already be in place for an existing facility. Without an RCM analysis, the PM program was probably based on past programs. Indications that the PM program is inefficient or ineffective are an excessive number of corrective maintenance actions (with an associated low facility availability), or an extremely large number of required PM actions that are imposing a very heavy economical penalty. Attempts to change the existing PM program may meet with some resistance (see paragraph 7-5.5.3.3).

7-5.5.1.2 Need for Supporting Analyses.

If an RCM analysis was not originally performed for the facility, its systems and equipment, much of the supporting analysis may also have been omitted. If such analyses, such as an FMEA, were not conducted, they must be conducted before an RCM-based PM program can be developed. For many of the installed systems and equipment, performing an FMEA or other analysis may be quite difficult because much of the data may not be available. Either the data was not acquired with the systems and equipment (such as, data rights were not procured), or the data is missing. In such cases, engineers will have to use engineering judgment and require more time to adequately analyze the systems and equipment.

7-5.5.1.3 Feasibility of Redesign.

If following the RCM logic, it is possible that the path may lead to a "Redesign is mandatory" or "redesign may be desirable" outcome. Redesign during initial development is a sometimes-difficult task. Once a system or piece of equipment is in operation, redesign is even more difficult. However, an advantage of a facility is that adding redundancy is less constrained, in terms of space and weight, than for other systems.

7-5.5.2 Training.

The RCM process is very disciplined and logical. It involves the integration of many different analytical tools, data, experience, and a decision logic tree. Without proper training, those assigned the responsibility of implementing RCM will find it difficult to succeed. Training in the RCM methodology and the related disciplines must be an essential element of an organization's plan for implementing RCM. For C5ISR facilities, especially when maintenance is outsourced, funding must be provided for training to ensure that an RCM analysis is properly performed. Of course, training to ensure maintenance is properly performed is also essential.

7-5.5.3 Pitfalls.

In implementing an RCM program in organizations where the concept is new, pitfalls can make implementation ineffective.

7-5.5.3.1 Run to Failure Shock.

For many maintenance managers and technicians, allowing an item to run to failure runs counter to conventional wisdom. It is important that they understand the concepts of reliability and turn their focus from preventing failures to preserving function.

7-5.5.3.2 Failure to Accept the “Preserve Function” Principle.

Most maintenance personnel traditionally have viewed their role as one of preventing failures. To effectively implement an RCM program, it is essential that maintenance personnel focus on preserving the function or functions of an item, not preventing failures.

7-5.5.3.3 Challenging the Past.

Tradition and conventional wisdom remain the principal guidance for many maintenance organizations. Challenging past practices almost always invokes strong resistance, especially if the new practices are not fully understood. Education is the best way to deal with cultural resistance.

7-5.5.3.4 Organization Structure.

The RCM process requires close coordination and cooperation among several groups of people, including but not limited to designers, maintainers, and logistic planners. Organizational structures can impede or even prevent the level of cooperation and coordination needed to make RCM a success. The concept of integrated process/product teams is one that facilitates and encourages cross-discipline cooperation.

7-5.5.3.5 Threat of Reduction in Staff.

When RCM was first implemented within the airline industry, drastic reductions in scheduled maintenance tasks were made possible. Consequently, the number labor hours and people required to, for example, conduct structural inspections of an aircraft were significantly reduced. When a segment of an organization perceives that a new policy or procedure will eliminate their jobs, the natural reaction is to fight against the new policy or procedure. However, with vision and planning, management can find ways to effectively use the resources freed up by implementing RCM and minimize the impact on jobs by using normal attrition, cross training, etc.

7-5.5.3.6 Inadequate Buy-in.

All too often, management implements a new policy or procedure without fully supporting that policy or procedure. If either resources or management interest is insufficient, the new policy or procedure will probably fall short of expectations. This is especially true for RCM, an approach that is often met with skepticism and resistance by the very same people who must help implement it.

7-5.5.3.7 Informal Procedures.

RCM is a very structured, disciplined method of developing a comprehensive and effective maintenance program. It cannot be effectively implemented on an informal or ad hoc basis. The procedures for implementing an RCM approach within an organization must be formal, documented, and managed.

7-5.5.3.8 Inadequate Data Collection.

If the underlying pattern of failures for a given item is unknown, one cannot objectively determine if PM should be considered. Without adequate information regarding the frequency of failure or the parameters of the failure PDF, one cannot objectively determine when a PM task should be performed. Data that is adequate in both quantity and type (for example, time to failure) is essential to the RCM process.

7-5.6 Evaluation of Alternatives.

As a result of performing an RCM analysis, alternatives will present themselves. These alternatives fall into two categories: Maintenance Tasks and Designs. Both categories are a natural result of the RCM analysis. Examining the logic trees in paragraph 7.5-4 indicates more than one type of maintenance task may be applicable and effective for a given failure. In some cases, for example where the effects of a failure are hazardous or a hidden failure can occur, redesign is mandatory or desirable. How is it determined which tasks to perform? How are the "best" design changes (for example, in the case of failures with hazardous effects) selected? How is it determined if a design change is cost-effective (for example, in the case of a hidden failure). These questions are addressed using Trade-off Studies, Operational Analysis, and Cost-Benefit Analysis.

7-5.6.1 Trade-off Studies.

Designing a new system or a change to an existing one, even a moderately complex one, requires a series of compromises. These compromises are inevitable, given the fact that requirements often conflict. Design decisions necessary to meet one requirement may result in another requirement not being met. For example, strength and fatigue life requirements drive the selection of materials and the size (bulk) of structures in one direction. The maximum weight requirement drives these same factors in the opposite direction. Systems engineering is the process of selecting design solutions that balance the requirements and provide an optimized system. Usually, this balance means that some requirements may not be fully met. The process of selecting one design solution over another is often referred to as design trade-offs. Trade-off studies consist of the steps listed below.

- Compare two or more design solutions
- Determine which provides the best results given cost and schedule constraints

- Determine if the system requirements can be met with the selected design solution
- If the system requirements cannot be met, determine the budget and schedule required to support a design solution that does allow the system requirements to be met, or re-evaluate the requirements

7-5.6.1.1 RCM and Desired Design Changes.

An RCM analysis may indicate that a change to the design is required or desirable. In such cases, trade-off studies will probably be needed to determine if a solution can be found that is effective (affordability is addressed in a cost-benefit analysis – see paragraph 7.5.6.2).

7-5.6.1.2 RCM and Mandatory Design Changes.

When the RCM analysis shows that two or more PM tasks are applicable, trade-off studies will be needed to determine which task(s) is (are) most effective. Of course, when a specific failure has hazardous effects, redesign is mandatory if no PM tasks are effective and applicable.

7-5.6.1.3 Operational Analysis.

To determine if a specific failure has operational effects (but no hazardous effects), an analysis of the operational concept is necessary. This analysis addresses the impact of a given failure on measures of operational performance. The measures are a function of the type of product and how that product is used. For the airline industry, for example, the cost of an operational failure includes lost revenue, potential penalties (in the form of compensation to passengers), loss of customer confidence and loyalty, and the cost of fixing the failure. For a military organization that operates aircraft, the costs might include a decrease in readiness, the inability to fulfill a mission, the cost of reassigning another aircraft to replace the original aircraft, and the cost to fix the failure. For a commercial company, the cost of an operational failure of a product could include the loss of customer confidence and loyalty, the cost of repair under warranty, and possible claims by the customer for lost revenue or other non-hazardous effects of the failure.

7-5.6.2 Cost-benefit Analysis.

Another type of analysis frequently used whenever one of two or more alternatives (design A vs. design B, task 1 vs. task 2, process I vs. process II, etc.) must be selected is a cost-benefit analysis (CBA).

7-5.6.2.1 Potential Benefits.

In a CBA, the potential life-cycle benefits of and life-cycle costs to implement a given alternative are compared with those of the other alternatives. One of the most difficult steps in a CBA is finding a common basis for comparison. That basis is almost always

dollars, since the costs of implementing a choice can almost always be directly measured in terms of dollars. Some of the benefits of an alternative may be intangible. However, it may be possible to attach a dollar value to even these benefits. Benefits to which a dollar value cannot be assigned should be evaluated and assigned relative numeric values for comparison purposes. For example, a maximum benefit could be assigned a value of 5, an average benefit a value of 3, and a minimum benefit a value of 1. Evaluating and comparing benefits that have both dollar values and relative numeric values requires extra effort, but it allows all benefits to be considered in the analysis.

7-5.6.2.2 Costs.

In a simple CBA, the annual costs of implementing each alternative design change, for example, are estimated. For this purpose, the analyst would sum up the estimates of the costs listed below. The analyst would estimate the annual benefits of the first alternative and then repeat this process for each of the other alternative design.

- The cost of the labor hours needed to develop the design
- The cost of any additional testing required
- Any differences in material costs
- Changes in manufacturing costs
- Additional costs due to changes in schedule
- Other costs

7-5.6.2.3 Conversion.

The analyst must convert the annual estimates to a common unit of measurement to properly compare competing alternatives. This conversion is done by discounting future dollar values, which transforms future benefits and costs to their "present value." The present value (also referred to as the discounted value) of a future amount is calculated using Equation 7-1.

Equation 7-1. Present Value

$$PV = \frac{FV}{(1 + i)^n}$$

Where:

PV = Present Value

FV = Future Value

i = Interest rate per period

n = Number of compounding periods

7-5.6.2.4 Comparison.

When the costs and benefits for each competing alternative have been discounted, the analyst compares and ranks the discounted net value (discounted benefit minus discounted cost) of the competing alternatives. In the ideal case one alternative will have the lowest discounted cost and provide the highest discounted benefits – it clearly would be the best alternative. More often, however, the choice is not so clear-cut, and other techniques must be used to determine which alternative is best.

7-5.6.2.5 Dollar Values.

Earlier, it was mentioned that some benefits may not be quantifiable in terms of dollars and may have relative numeric values assigned for comparison purposes. In those cases, these numeric values can be used as tie breakers if the cost figures do not show a clear winner among the competing alternatives, and if the non-quantifiable benefits are not key factors. If they are key factors, the quantified benefits can be converted to scaled numeric values consistent with the non-quantifiable benefits. The evaluation then consists of comparing the discounted costs and the relative values of the benefits for each alternative. When the alternative with the lowest discounted cost provides the highest relative benefits, it is clearly the best alternative (the same basic rule used when there are discounted benefits). If that is not the case, the evaluation is more complex.

7-5.6.2.6 Numerical Values.

Finally, if no benefits have dollar values, numerical values can be assigned (using some relative scale) to each benefit for each competing alternative. The evaluation and ranking are then completed in the manner described in the previous paragraph.

7-5.6.2.7 Sensitivity Analysis.

Sensitivity analysis can be used to test the sensitivity and reliability of the results obtained from a CBA. For more information on conducting a CBA and related analysis, see the references in TM 5-698-2 Appendix A.

This Page Intentionally Left Blank

CANCELLED

APPENDIX A FACTORS INFLUENCING FIELD MEASURES OF RELIABILITY

A-1 INHERENT RELIABILITY VERSUS OPERATIONAL RELIABILITY.

The reliability achieved by diligent attention to failure modes and mechanisms during design and manufacture is defined as inherent reliability. The reliability observed during operation of the system in its intended environment is defined as operational reliability.

A-1.1 Inherent Reliability.

Inherent reliability is the level of reliability inherent in the system as designed and manufactured. All failures are due to inherent weaknesses in the design, flaws in the materials, or defects from the manufacturing processes. The level of inherent reliability achieved is determined through analysis and test. Although in applying analytical methods and in testing the system (the "actual" system or prototypes), the design and development team attempts to simulate the actual operating environment, it is difficult if not impossible to account for some aspects of operation.

A-1.2 Operational Reliability.

Operational reliability is the measure a customer or user of a system uses. Whenever a system fails to perform its function(s) or requires maintenance, the customer will count such events as failures, regardless of the cause. Inherent weaknesses in the design, flaws in the materials, and defects from the manufacturing processes will cause such failures, but so will maintenance errors, improper operation, and changes in operating concept. In addition, if the operating environment is substantively different from that defined during design, more failures or failure modes may occur than were addressed during design and manufacturing. Consequently, operational reliability can never be higher than inherent reliability and is usually lower.

A-2 ACCOUNTING FOR THE DIFFERENCES.

The differences between design and operational reliability can be accounted for. This can be done in two ways: the way procedures are designed and developed, and the way in which design requirements are developed.

A-2.1 Design of Procedure.

Recognizing that humans make mistakes, design techniques that minimize the chance of human error can be applied. For example, parts can be designed to mate in only one way, preventing maintenance personnel from making an incorrect connection. Displays can be designed so they are easy to read and use conventional symbols. Controls can be designed using standard orientation (for example, turn right to shut off a valve). In a similar manner, procedures can be written in a clear, concise, and logical manner. Such attention to the human element during design can minimize the opportunity for human error.

A-2.2 Design Requirements.

If the customer needs an operational reliability of 1000 hours Mean Time Between Failures (MTBF) for a system, 1000 hours cannot be used as the design requirement. If it was used and missed one failure mode due to the inexact understanding of the operating environment, the operational reliability requirement would not be met. The system must be designed to a higher level. An arbitrarily high inherent reliability requirement should not be set. To do so would drive up costs unnecessarily. A commonly used approach for setting the inherent reliability requirement is to use past experience. If experience with previous systems indicates that the operational reliability runs 10%-15% lower than what was measured during design and manufacture, then, as a rule of thumb, the inherent reliability requirement for new systems should be 12% higher than the operational reliability requirement. For example, if the inherent reliability for past systems was 1,000 hours MTBF and the observed operational reliability was only 850 hours (15% less), and the operational reliability requirement for a new system is 1,000 hours, the inherent reliability requirement must be about 11.8% higher or 1,180 hours. If this level of inherent reliability is achieved, then it is expected the operational reliability to be $1180 - (15\% \times 1180) = 1,003$ hours.

APPENDIX B STATISTICAL DISTRIBUTION USED IN RELIABILITY AND MAINTAINABILITY

B-1 INTRODUCTION TO STATISTICAL DISTRIBUTION.

Many statistical distributions are used to model various reliability and maintainability parameters. The distribution used depends on the nature of the data being analyzed.

B-1.1 Exponential and Weibull.

These two distributions are commonly used for reliability modeling – the exponential is used because of its simplicity and because it has been shown in many cases to fit electronic equipment failure data, and the Weibull because it consists of a family of different distributions that can be used to fit a wide variety of data and it models wear out (such as, an increasing hazard function).

B-1.2 Normal and Lognormal.

Although also used to model reliability, the normal and lognormal distributions are more often used to model repair times. In this application, the normal is most applicable to simple maintenance tasks that consistently require a fixed amount of time to complete with little variation. The lognormal is applicable to maintenance tasks where the task time and frequency vary, which is often the case for complex systems and products.

B-2 THE EXPONENTIAL DISTRIBUTION.

The exponential distribution is widely used to model electronic reliability failures in the operating domain that tend to exhibit a constant failure rate. To fail exponentially means that the distribution of failure times fits the exponential distribution as shown in Table B-1. The characteristics of the exponential distribution are listed below.

- It has a single parameter, λ , which is the mean. For reliability applications, λ called the failure rate.
- λ , the failure rate, is a constant. If an item has survived for t hours, the chance of it failing during the next hour is the same as if it had just been placed into service.
- The mean-time-between-failure (MTBF) = $1/\lambda$.
- The mean of the distribution occurs at about the 63rd percentile. Thus, if an item with a 1000-hour MTBF had to operate continuously for 1000 hours, the probability of success (survival) would be only 37%.

Figure B-1 shows the exponential Probability Density Function for varying values of λ .

Table B-1 Summary of the Exponential Distribution

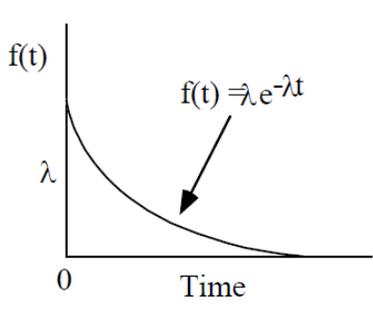
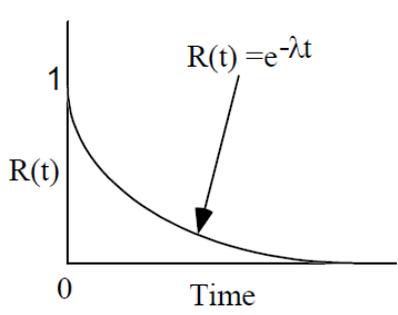
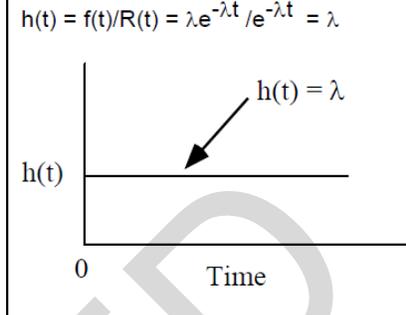
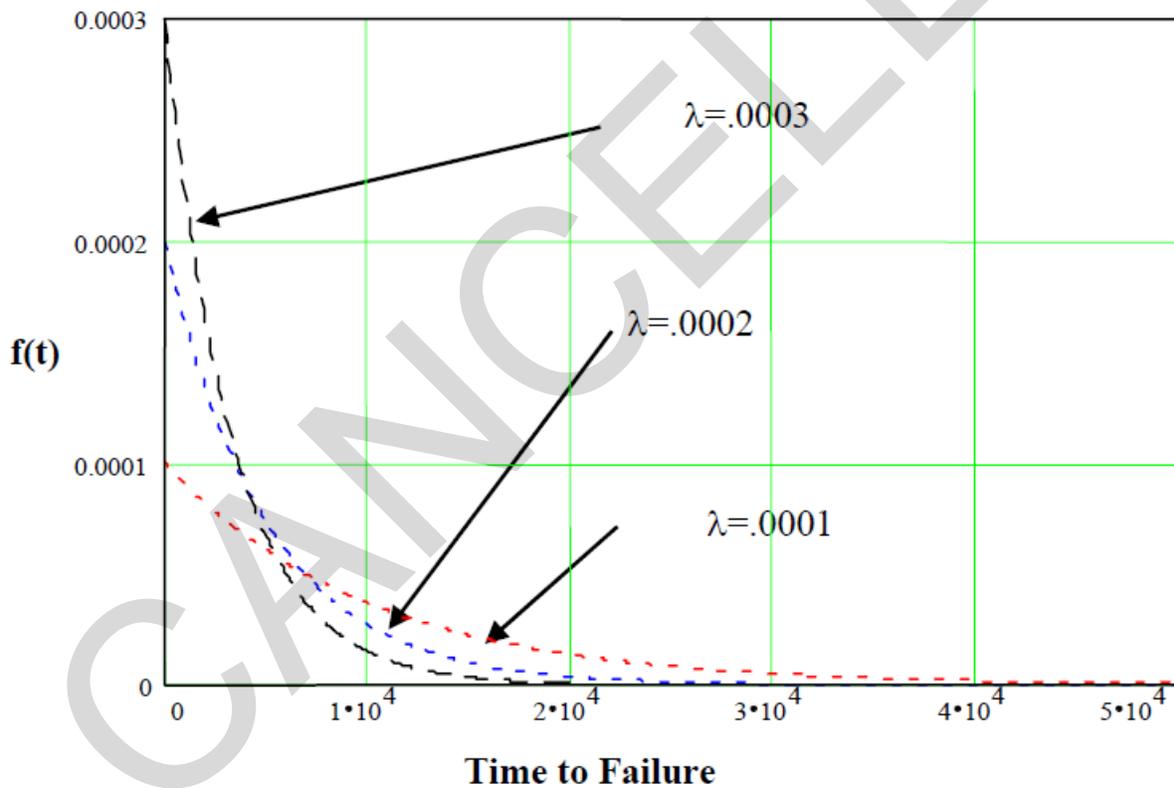
Probability Density Function	Reliability Function	Hazard Function
		

Figure B-1 The Exponential PDF for Varying Values of λ



B-3 THE WEIBULL DISTRIBUTION.

The Weibull distribution is an important distribution because it can be used to represent many different pdfs; therefore, it has many applications. The characteristics of the Weibull are listed below.

- It has 2 (β , η , and γ) parameters.

- The shape parameter, β , describes the shape of the Probability Density Function.
 - The scale parameter, η , is the 63rd percentile value of the distribution and is called the characteristic life. In some texts, Θ , is used as the symbol for the characteristic life.
 - The location parameter, γ , is the value that represents a failure-free or prior use period for the item. If there is no prior use or period where the probability of failure is zero, then $\gamma = 0$ and the Weibull distribution becomes 2-parameter distribution.
- β , η , and γ can be estimated using Weibull probability paper or software programs.
 - When $\beta = 1$ and $\gamma = 0$, the Weibull probability is exactly equivalent to the exponential distribution.
 - When $\beta = 3.44$, the Weibull closely approximates the normal distribution.

The distribution is described in Table B-2. Figure B-2 shows the 2-parameter Weibull pdf for different values of β , and a given value of η .

Table B-2 Summary of the Weibull Distribution

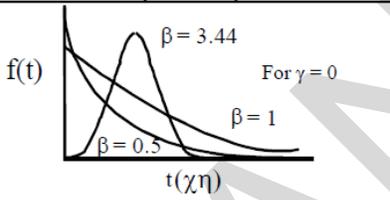
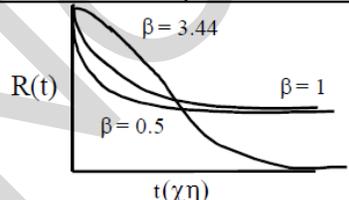
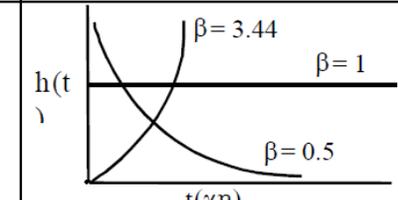
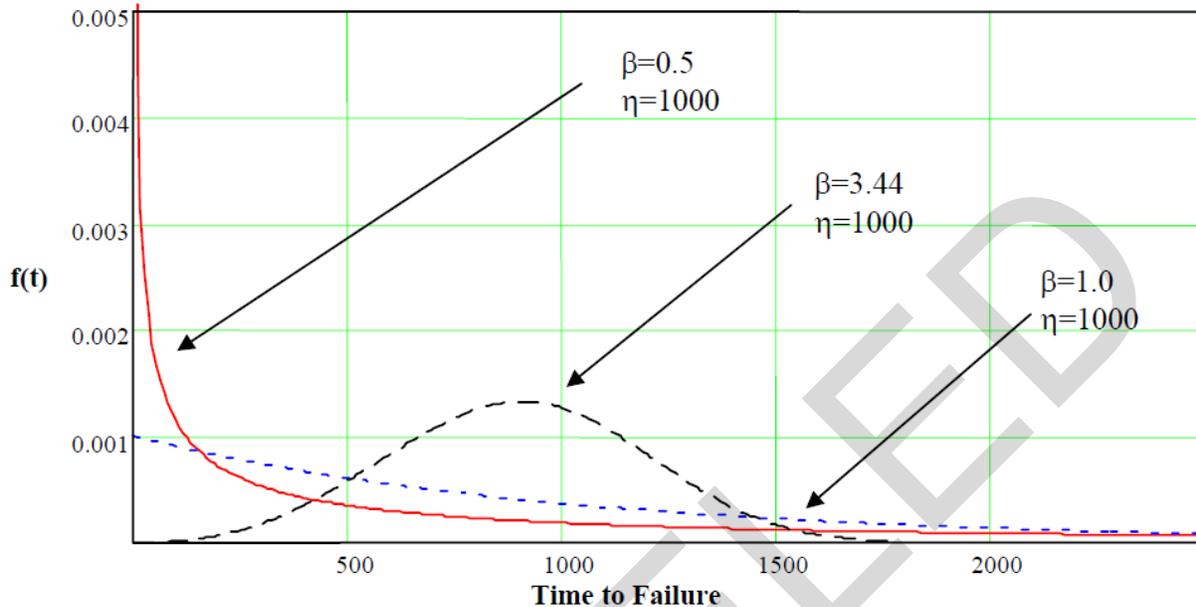
Probability Density Function	Reliability Function	Hazard Function
 <p style="text-align: center;">For $\gamma = 0$</p> $f(t) = \frac{\beta}{\eta} \left(\frac{t - \gamma}{\eta} \right)^{\beta-1} \exp \left[- \frac{(t - \gamma)^\beta}{\eta} \right]$	 $R(t) = \exp \left[- \frac{(t - \gamma)^\beta}{\eta} \right]$	 $h(t) = \frac{\beta}{\eta} \left(\frac{t - \gamma}{\eta} \right)^{\beta - 1}$

Figure B-2 The Two-Parameter Weibull PDF for Different Values of β and a Given Value of η



B-4 THE NORMAL DISTRIBUTION.

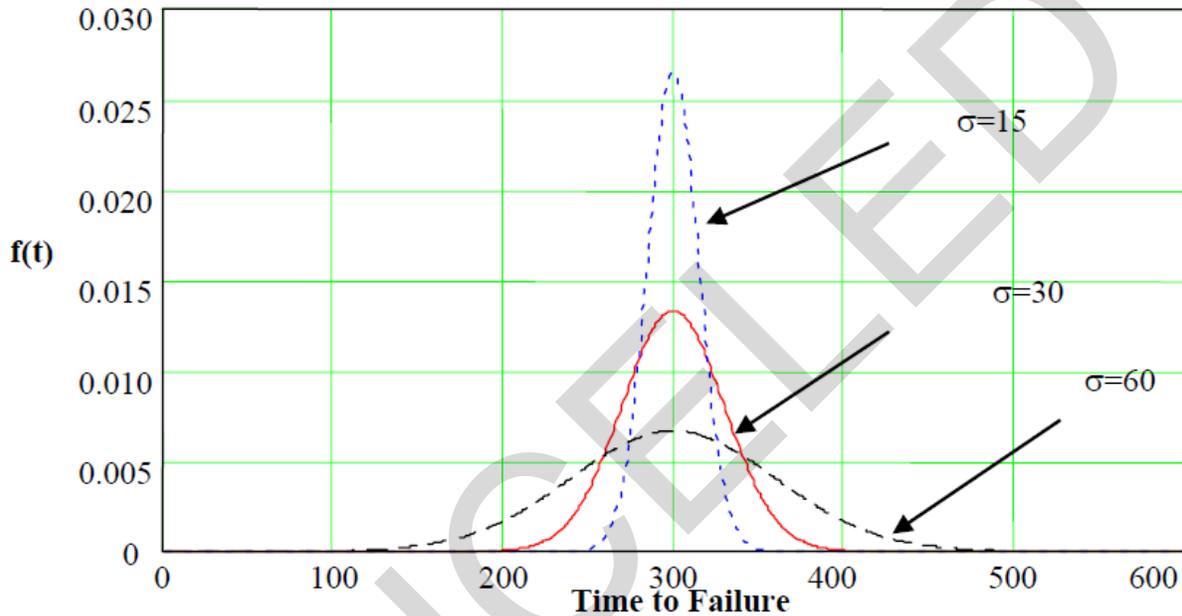
The pdf of the Normal distribution is often called the bell curve because of its distinctive shape. The Normal distribution is described in Table B-3. The characteristics of the Normal distribution are listed below.

- It has two parameters:
 - The mean, μ , is the 50th percentile of the distribution. The distribution is symmetrical around the mean.
 - The standard deviation, σ , is a measure of the amount of spread in the distribution.
- If t has the pdf defined in Figure B-3 and $\mu = 0$ and $\sigma = 1$, then t is said to have a standardized normal distribution.
- The integral of a distribution's pdf is its cumulative distribution function, used to derive the reliability function. The integral of the normal pdf cannot be evaluated using the Fundamental Theorem of Calculus because a function for which the derivative equals $\exp(-x/2)$ cannot be found. However, numerical integration methods have been used to evaluate the integral and tabulate values for the standard normal distribution.

Table B-3 Summary of the Normal Distribution

Probability Density Function	Reliability Function	Hazard Function
$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-\mu)^2}{2\sigma^2}}$	$R(t) = \int_t^{\infty} f(t)dt$	$h(t) = \frac{f(t)}{R(t)}$

Figure B-3 The Normal PDF for Varying Values of σ and Fixed μ .



B-5 THE LOGNORMAL DISTRIBUTION.

The lognormal distribution is summarized in Table B-4. The characteristics of the lognormal distribution are listed below.

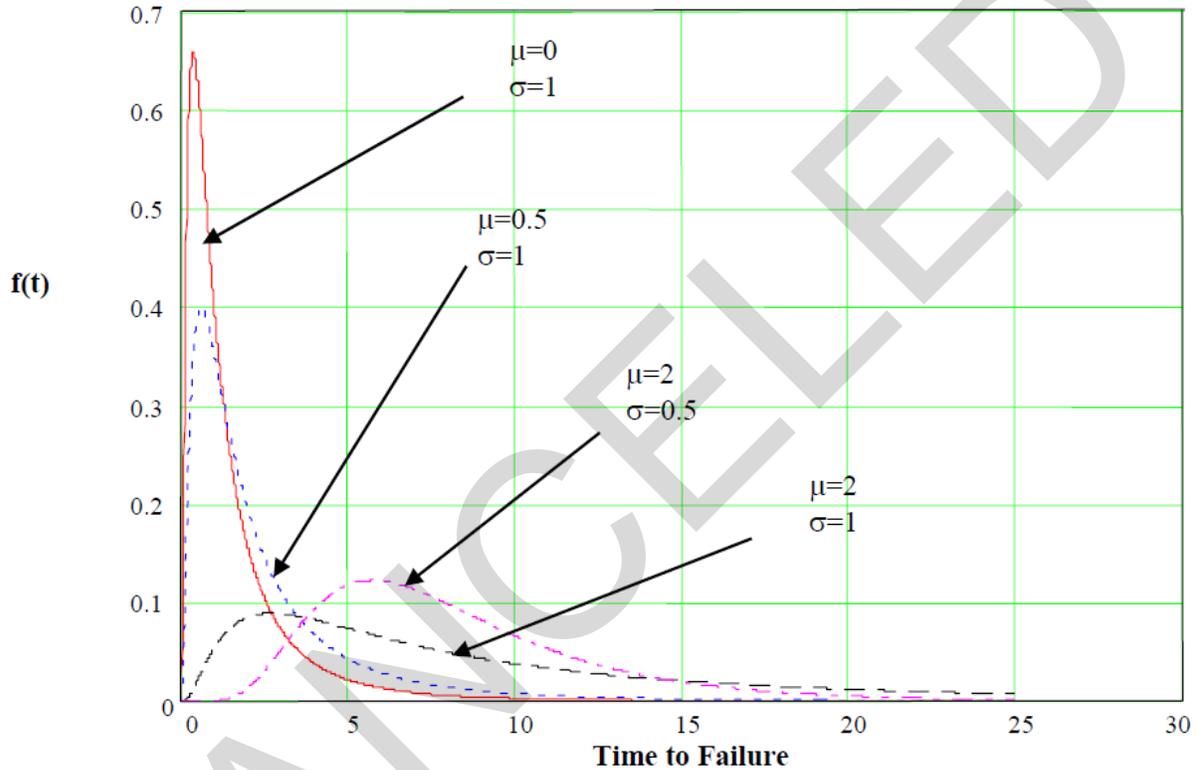
- It has two parameters:
 - The mean, μ . Unlike the mean of the Normal distribution, the mean of the lognormal is not the 50th percentile of the distribution and the distribution is not symmetrical around the mean.
 - The standard deviation, σ .
- The logarithms of the measurements of the parameter of interest (for example, time to failure, time to repair) are normally distributed.

Figure B-4 shows the distribution for different values of μ and σ .

Table B-4 Summary of the Lognormal Distribution

Probability Density Function	Reliability Function	Hazard Function
$f(t) = \frac{1}{\sigma t \sqrt{2\pi}} e^{-\frac{(\ln(t)-\mu)^2}{2\sigma^2}}$	$R(t) = \int_t^{\infty} f(t) dt$	$h(t) = \frac{f(t)}{R(t)}$

Figure B-4 The Lognormal PDF for Different Values of μ and a Fixed σ



APPENDIX C AVAILABILITY AND OPERATIONAL READINESS

C-1 AVAILABILITY.

In general, availability is the ability of a product or service to be ready for use when a customer wants to use it. That is, it is available if it is in the customer's possession and works when it's turned on or used. A product that's "in the shop" or is in the customer's possession but doesn't work is not available. Measures of availability are shown in Table C-1.

Table C-1 Quantitative Measures of Availability

Measure	Equation	Description
Inherent Availability: A_i	$\frac{MTBF}{MTBF + MTTR}$	<ul style="list-style-type: none"> Where MTBF is the mean time between failure and MTTR is the mean time to repair A probabilistic measure Reflects the instantaneous probability that a component will be up. A_i considers only downtime for repair due to failures. No logistics delay time, preventative maintenance, etc. is included.
Operational Availability: A_o	$\frac{MTBM}{MTBM + MDT}$	<ul style="list-style-type: none"> Where MTBM is the mean time between maintenance (preventative and corrective) and MDT is the mean downtime, which includes MTTR, and all other time involved with downtime such as logistic delays A probabilistic measure Similar to inherent availability but includes ALL downtime. Included is downtime for corrective maintenance and preventative maintenance, including any logistics delay time.

MTBF = Mean Time Between Failure MTBM = Mean Time Between Maintenance
MDT = Mean Downtime MTTR = Mean Time to Repair (corrective only)

C-1.1 Nature of the Equations.

Note that the equations are time independent and probabilistic in nature. The value of availability yielded by each equation is the same whether the period of performance being considered is 1 hour or a year.

C-1.2 Derivation of Steady State Equation for Availability.

The equations in Table C-1 are steady state equations. The equation for inherent availability (Equation C-1) is the steady state equation derived from Equation C-2, as time approaches infinity:

Equation C-1. Inherent Availability

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Equation C-2. Inherent Availability

$$A_i = \frac{MTBF}{MTBF + MTTR} + \frac{MTTR}{MTBF + MTTR} e^{-\left(\frac{1}{MTBF} + \frac{1}{MTTR}\right)t}$$

1. Equation C-1 represents a limit for inherent availability. It represents the long-term proportion of time that a system will be operational.

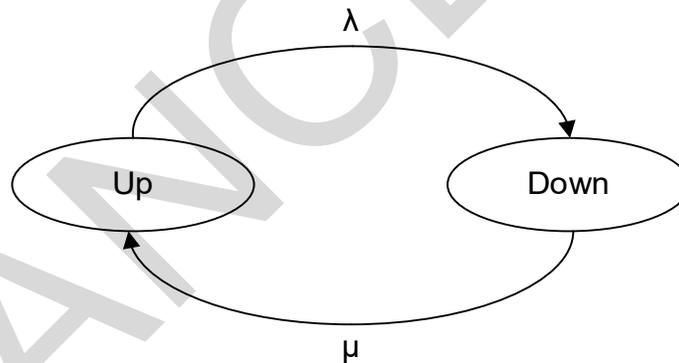
2. Assuming that the times to failure and time to repair are both exponentially distributed, with rates λ and μ , respectively, Equation C-1 can be expressed as:

Equation C-3. Inherent Availability

$$A_i = \frac{\frac{1}{\lambda}}{\frac{1}{\lambda} + \frac{1}{\mu}} = \frac{\mu}{\mu + \lambda}$$

3. The derivation of Equation C-1 now follows. A simple Markov model is used to evaluate availability. The probabilities of being in either the up state or the down state are determined using the Laplace transform. The model and equations are:

Figure C-1 Simple Markov Model



Equation C-4.

$$\frac{dP_{Up}(t)}{dt} = -\lambda P_{Up}(t) + \mu P_{Down}(t)$$

Equation C-5.

$$sL_{Up}(s) - P_{Up}(0) = sL_{Up}(s) - 1 = -\lambda L_{Up}(s) + \mu L_{Down}(s)$$

Equation C-6.

$$1 - sL_{Up}(s) = sL_{Down}(s) = \lambda L_{Up}(s) - \mu L_{Down}(s)$$

Equation C-7.

$$\text{From Equation C-4, } L_{Up}(s) = \frac{1+\mu L_{Down}(s)}{s+\lambda}$$

Equation C-8.

$$\text{From Equation C-5, } L_{Down}(s) = \frac{\lambda L_{Up}(s)}{s+\mu}$$

4. Substituting the expression for $L_{Down}(s)$ into Equation C- 7,

Equation C-9.

$$L_{Up}(s) = \frac{1}{s + \mu + \lambda} + \frac{\mu}{s(s + \mu + \lambda)}$$

5. Then, availability equals the inverse of the Laplace transform for $L_{Up}(s)$. To obtain the inverse,

Equation C-10.

$$\begin{aligned} \frac{1}{s + \mu + \lambda} + \frac{\mu}{s(s + \mu + \lambda)} &= \frac{1}{\lambda + \mu} \left(\frac{\mu(s + \mu + \lambda) + \lambda s}{s(s + \mu + \lambda)} \right) \\ &= \frac{1}{\lambda + \mu} \left(\frac{\mu}{s} + \frac{\lambda}{s + \mu + \lambda} \right) \\ &= \frac{\mu}{\lambda + \mu} * \frac{1}{s} + \frac{\lambda}{\mu + \lambda} * \frac{1}{s + \mu + \lambda} \\ &= \frac{1}{\lambda + \mu} \left(\frac{\mu}{s} + \frac{\lambda}{s + \mu + \lambda} \right) \\ &= \frac{\mu}{\lambda + \mu} * \frac{1}{s} + \frac{\lambda}{\mu + \lambda} * \frac{1}{s + \mu + \lambda} \\ &= \frac{\mu}{\lambda + \mu} \int_0^{\infty} e^{-st} dt + \frac{\lambda}{\lambda + \mu} \int_0^{\infty} e^{-(s+\mu+\lambda)t} dt \\ &= \int_0^{\infty} \frac{\mu}{\lambda + \mu} e^{-st} dt + \frac{\lambda}{\lambda + \mu} e^{-(s+\mu+\lambda)t} dt \\ &= \int_0^{\infty} \frac{\mu}{\lambda + \mu} e^{-st} dt + \frac{\lambda}{\lambda + \mu} e^{-(s+\mu+\lambda)t} dt \end{aligned}$$

$$= L \left[\frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\mu+\lambda)t} \right]$$

$$A = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\mu+\lambda)t}$$

6. Taking the limit of Equation C-10 as t approaches infinity,

Equation C-11.

$$A_i = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} * 0 = \frac{\mu}{\lambda + \mu}$$

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Q.E.D

C-2 OPERATIONAL READINESS.

Closely related to the concept of operational availability but broader in scope is operational readiness. Operational readiness is defined as the ability of a military unit to respond to its operational plans upon receipt of an operations order. It is, therefore, a function not only of the product availability, but also of assigned numbers of operating and maintenance personnel, the supply, the adequacy of training, and so forth.

C-2.1 Readiness in the Commercial World.

Although operational readiness has traditionally been a military term, it is equally applicable in the commercial world. For example, a manufacturer may have designed and can make very reliable, maintainable products. What if he has a poor distribution and transportation system or does not provide the service or stock the parts needed by customers to effectively use the product? Then, the readiness of this manufacturer to go to market with the product is low.

C-2.2 Relationship of Availability and Operational Readiness.

The concepts of availability and operational readiness are obviously related. Important to note, however, is that while the inherent design characteristics of a product totally determine inherent availability, other factors influence operational availability and operational readiness. The reliability and maintainability engineers directly influence the design of the product. Together, they can affect other factors by providing logistics planners with the information needed to identify required personnel, spares, and other resources. This information includes the identification of maintenance tasks, repair procedures, and needed support equipment.

APPENDIX D PREP DATABASE IEEE DOT STANDARD 3006.8

The header below represents the header in the database. Each column heading is explained in the text boxes. The formulas, representing the column heading, are contained in the Table E-1 below.

Category	Class	Unit-Years	Failures	Failure Rate (Failures/Year)	MTBF	MTTR	MTTM	MDT
Name of the Category (Example: Boiler) of the item.	Name of the Class (Example: Boiler, Hot Water) of the item.	The number of calendar hours collected for each item divided by 8760.	The number of failures recorded for each item during the data collection.	Failure Rate based on a year.	Average time between failures in hours.	Mean time to replace or repair a failed component. Logistics delay time associated with the repair, such as parts acquisitions, crew mobilization, are not included	Average downtime for preventative maintenance. This includes any logistics delay time.	Average downtime caused by preventative and corrective maintenance, including any logistics delay time.

Table D-1 Reliability and Maintainability Calculations

Calculated Data	Formula for Calculation
A_i , Inherent Availability	$A_i = \text{MTBF} / (\text{MTBF} + \text{MTTR})$
A_o , Operational Availability	$A_o = \text{MTBM} / (\text{MTBM} + \text{MDT})$
λ , Failure Rate (failures/hour(h))	$\lambda = T_f / T_p$
λ_y , Failure Rate (failures/year(y))	$\lambda_y = T_f / (T_p / 8760)$
MDT, Mean Down Time (h)	$\text{MDT} = (\text{Rdt} + \text{Rlt} + \text{Mdt}) / \text{Tde}$
MTBF, Mean Time Between Failures (h)	$\text{MTBF} = T_p / T_f$
MTBM, Mean Time Between Maintenance (h)	$\text{MTBM} = T_p / \text{Tde}$
MTTM, Mean Time To Maintain (h)	$\text{MTTM} = \text{Mdt} / \text{Tma}$
MTTR, Mean Time To Repair (h)	$\text{MTTR} = \text{Rdt} / T_f$
$R(t)$, Reliability (for time interval t)	$R(t) = e^{-\lambda t}$
Hrdt/Year, Hours Downtime per Year	$\text{Hrdt/Year} = (1 - A_o) \times 8760$

Table D-2 USACE-PREP Equipment Reliability Database

Category			Class	Unit-years	Failures	Failure rate (failures/year)	MTBF (hours)	MTTR (hours)	MTTM (hours)	MDT (hours)
Accumulator				1463.2	10	0.006 834 233	1 281 782	7.80	0.94	0.98
	Pressurized	H01-100	Accumulator, pressurized	1072.8	7	0.006 525 131	1 342 502	10.29	0.96	1.01
	Unpressurized	H01-200	Accumulator, unpressurized	390.4	3	0.007 683 510	1 140 104	2.00	0.33	0.42
Air compressor				5124.5	1592	0.310 662 877	28 198	12.20	1.55	4.24
	Electric	H02-100	Air compressor, electric	4534.6	1492	0.329 029 093	26 624	11.80	1.48	4.16
	Fuel	H02-200	Air compressor, fuel	590.0	100	0.169 499 396	51 682	17.45	2.72	5.71
Air conditioner	All types	H03-000	Air conditioner	4947.4	781	0.157 860 257	55 492	5.95	1.59	2.63
Air dryer	All types	H04-000	Air dryer, all types	2307.2	170	0.073 681 948	118 889	9.11	1.44	5.36
Air handling unit				12 173.7	2650	0.217 681 964	40 242	5.06	1.99	3.27
	Humid			379.1	68	0.179 375 438	48 836	2.55	2.53	3.21
		H05-110 ^a	Air handling unit, humid, pan humid, w/o drive	25.0	0	0.027 695 536	429 882	0.00	0.00	0.00
		H05-130	Air handling unit, humid, pan humid, with drive	212.8	30	0.140 975 629	62 138	3.02	2.73	2.94
		H05-120 ^a	Air handling unit, humid, spray humid, w/o drive	38.1	0	0.018205276	653 976	0.00	0.00	0.00
		H05-140	Air handling unit, humid, spray humid, with drive	103.2	38	0.368 256 160	23 788	2.27	1.59	4.31
	Multizone system	H05-310	Air handling unit, multizone system, packaged	1103.7	448	0.405 891 785	21 582	6.18	4.34	9.97
	Non-humid			10 690.9	2134	0.199 609 243	43 886	4.75	1.67	2.38
		H05-210	Air handling unit, non-humid, without drive	7821.1	1734	0.221 709 225	39 511	4.95	1.88	2.40
		H05-220	Air handling unit, non-humid, with drive	2869.8	400	0.139 380 939	62 849	4.18	1.51	2.36
Air separator	All types	H06-000	Air separator, all types	84.7	9	0.106 272 848	82 429	6.31	0.88	3.35
Surge arrester	Surge and lightning	E01-000	Surge arrester, surge and lightning	1863.4	12	0.006 439 803	1 360 290	9.50	12.28	11.66
Battery	Rechargeable			13 228.7	121	0.009 146 782	957 714	13.40	0.16	0.45
		E02-110	Battery, gel cell-sealed	3106.8	53	0.017 059 514	513 496	2.00	0.13	0.15
		E02-120	Battery, lead acid	5022.6	65	0.012 941 467	676 894	24.08	0.25	4.31
		E02-130	Battery, nickel-cadmium	5099.3	3	0.000 588 315	14 889 985	10.33	0.16	0.16

Blower				4307.0	239	0.055 490 708	157 864	9.44	0.17	0.63
	Without drive	H07-100	Blower, without drive	3947.4	189	0.047 880 115	182 957	10.75	0.17	0.32
	With drive	H07-200	Blower with drive	359.7	50	0.139 016 903	63 014	3.79	1.04	24.95
Boiler				5125.6	2190	0.427 265 681	20 502	17.69	6.61	8.72
	Hot water	H08-100	Boiler, hot water	2566.6	688	0.268 055 191	32 680	3.94	6.35	6.89
	Steam			2559.0	1502	0.586 952 425	14 925	24.40	6.70	9.37
		H08-210	Boiler, steam, high pressure, > 103.4 kPa (15 psig)	942.7	781	0.828 434 093	10 574	39.77	5.52	6.84
		H08-220	Boiler, steam, low pressure, ≤ 103.4 kPa (15 psig)	1616.2	721	0.446 097 568	19 637	13.25	48.03	40.86
Bus duct or busway	All types	E03-000	Bus duct or busway, all types, per 30.5 m (100 ft)	2462.3	143	0.058 075 621	150 838	1.65	1.08	1.26
Cabinet heaters	Forced air flow			14 053.8	64	0.004 553 920	1 923 618	3.10	1.23	1.56
		E04-100	Cabinet heaters, forced air flow, steam or hot water	13 931.1	64	0.004 594 025	1 906 825	3.10	1.23	1.56
		E04-200 ^a	Cabinet heaters, forced air flow, electric	122.7	0	0.005 649 689	2 107 341	0.00	0.67	0.67
Cable				736 799.6	1366	0.001 853 964	4 725 011	5.59	4.34	4.43
	AC			698 824.2	924	0.001 322 221	6 625 216	7.29	4.35	4.50
		E06-111	Cable, ac, 0 V to 600 V, above ground, in conduit, per 305 m (1000 ft)	29 442.9	2	0.000 067 928	28 959 932	8.00	13.06	13.01
		E06-112 ^a	Cable, ac, 0 V to 600 V, above ground, in trays, per 305 m (1000 ft)	15.9	0	0.043 545 391	273 412			
		E06-113	Cable, ac, 0 V to 600 V, above ground, no conduit, per 305 m (1000 ft)	33 286.3	4	0.000 120 170	72 896 904	2.50	0.05	0.08
		E06-121	Cable, ac, 0 V to 600 V, below ground, in duct, per 305 m (1000 ft)	40 000.4	5	0.000 124 999	70 080 730	16.40	0.73	2.79
		E06-122	Cable, ac, 0 V to 600 V, below ground, in conduit, per 305 m (1000 ft)	24 426.8	49	0.002 005 991	4 366 919	11.22	87.71	28.22
		E06-123	Cable, ac, 0 V to 600 V, below ground, insulated, per 305 m (1000 ft)	3095.3	80	0.025 845 534	338 937	7.60		7.60

		E06-211	Cable, ac, 601 kV to 15 kV, above ground, in conduit, per 305 m (1000 ft)	523 356.6	281	0.000 536 919	16 315 315	8.56	40.51	16.11
		E06-212 ^a	Cable, ac, 601 kV to 15 kV, Above ground, in trays, per 305 m (1000 ft)	180.1	0	0.003 849 060	3 093 176			
		E06-214	Cable, ac, 601 kV to 15 kV, above ground, in trays, in conduit, per 305 m (1000 ft)	2646.0	2	0.000 755 852	11 589 564	4.00		4.00
		E06-221	Cable, ac, 601 kV to 15 kV, below ground, in conduit, per 305 m (1000 ft)	19 525.5	46	0.002 355 896	3 718 331	15.70	211.43	41.55
		E06-222	Cable, ac, 601 kV to 15 kV, below ground, in duct, per 305 m (1000 ft)	78.1	1	0.012 799 383	684 408			
		E06-223	Cable, ac, 601 kV to 15 kV, below ground, insulated, per 305 m (1000 ft)	22 770.3	454	0.019 938 292	439 356	5.13	3.97	4.01
	Aerial			37 500.3	439	0.011 706 565	748 298	2.03	0.35	1.91
		E07-200	Cable, aerial, > 15 kV, per 1.6 km (1 mile)	30 884.9	127	0.004 112 048	2 130 325	2.54	0.35	2.08
		E07-100	Cable, aerial, 0 kV to 15 kV, per 1.6 km (1 mile)	6615.5	312	0.047 162 173	185 742	1.82		1.82
	DC	E08-100	Cable, dc, insulated, per 305 m (1000 ft)	475.1	3	0.006 313 969	1 387 400	2.00		2.00
Cable connection	Underground	E05-100	Cable connection, underground, duct, ≤ 600 V	21 574.5	8	0.000 370 808	23 624 073	0.75		0.75
Capacitor bank	All types	E10-000	Capacitor/capacitor bank, all types	2041.1	104	0.050 951 857	171 927	2.37	4.27	3.13
Charger	Battery	E11-000	Charger, battery	666.0	26	0.039 040 966	224 380	7.46	0.72	2.29
Chiller				3607.7	1283	0.355 626 726	24 633	8.57	1.86	3.33
	Absorption	H10-100	Chiller, absorption	587.7	93	0.158 231 093	55 362	11.40	0.68	0.72
	Centrifugal			1054.5	529	0.501 674 408	17 462	7.73	11.29	24.68
		H10-210	Chiller, centrifugal, ≤ 600 tons (2110 kW)	152.1	298	1.959 149 120	4471	5.75	29.58	140.30
		H10-230	Chiller, centrifugal, > 1000 tons (3517 kW)	242.9	152	0.625 733 105	14 000	9.23	35.17	35.44

		H10-220	Chiller, centrifugal, 600 tons to 1000 tons (2110 kW to 3517 kW)	659.4	79	0.119 797 371	73 123	11.81	5.28	5.51
	Reciprocating			1193.5	192	0.160 868 248	54 455	10.77	1.65	2.21
		H10-321	Chiller, reciprocating, closed, with drive, 50 tons to 200 tons (176 kW to 703 kW)	881.8	139	0.157 633 096	55 572	11.11	1.53	2.06
		H10-331	Chiller, reciprocating, open, w/o drive, 50 tons to 200 tons (176 kW to 703 kW)	285.7	53	0.185 495 934	47 225	10.02	2.98	3.80
		H10-311 ^a	Chiller, reciprocating, with drive, < 50 tons (176 kW)	26.0	0	0.026 651 082	446 729		1.00	1.00
	Rotary			122.5	15	0.122 477 741	71 523	7.33	8.47	9.47
		H10-420	Chiller, rotary, < 600 tons (2110 kW)	32.0	1	0.031 244 650	280 368	1.00	1.63	1.60
		H10-410	Chiller, rotary, 600 tons to 1000 tons (2110 kW to 3517 kW)	90.5	14	0.154 754 694	56 606	8.60	8.74	9.79
	Screw			649.5	454	0.698 994 807	12 532	7.83	8.12	10.69
		H10-510	Chiller, screw, ≤ 300 tons (1055 kW)	499.0	380	0.761 497 960	11 504	5.37	27.44	15.71
		H10-520	Chiller, screw, > 300 tons (1055 kW)	150.5	74	0.491 734 634	17 814	23.24	6.37	7.97
Circuit breaker				180 935.2	1437	0.007 942 070	1 102 987	15.11	7.99	11.33
	Air			9012.4	93	0.010 319 132	848 909	11.65	73.27	60.16
		E12-111	Circuit breaker, air, 3-phase, > 600 V, > 600 A, normally closed (NC)	8885.8	90	0.010 128 467	864 889	11.65	73.27	60.16
		E12-112	Circuit breaker, air, 3-phase, > 600 V, > 600 A, normally open (NO)	126.5	3	0.023 707 970	369 496			
	Fixed (includes molded case)			150 305.9	10	0.000 066 531	31 667 972	25.36	8.29	9.74
		E12-211	Circuit breaker, fixed (includes molded case), 3-phase, ≤ 600 V, ≤ 600 A, normally closed (NC)	34 569.2	4	0.000 115 710	75 706 529	23.25	3.09	9.64

		E12-212	Circuit breaker, fixed (includes molded case), 3-phase, ≤ 600 V, ≤ 600 A, normally open (NO)	26 607.0	3	0.000 112 752	77 692 576	18.67	8.61	8.73
		E12-221	Circuit breaker, fixed (includes molded case), 3-phase, ≤ 600 V, > 600 A, normally closed (NC)	88 546.5	1	0.000 011 294	75 667 016		13.62	13.62
		E12-222	Circuit breaker, fixed (includes molded case), 3-phase, ≤ 600 V, > 600 A, normally open (NO)	583.2	2	0.003 429 339	2 554 428	37.50	2.69	3.03
	Fixed (molded case)	E12-311	Circuit breaker, fixed (molded case), 600 V, single phase, normally closed (NC)	7027.5	1	0.000 142 299	61 560 528	1.00		1.00
	Metal clad (drawout)			9529.8	179	0.018 783 250	466 373	9.58	2.12	4.33
		E12-411	Circuit breaker, metal clad (drawout), ≤ 600 V, ≤ 600 A, normally closed (NC)	5705.6	18	0.003 154 788	2 776 732	6.50	2.02	2.02
		E12-412	Circuit breaker, metal clad (drawout), ≤ 600 V, ≤ 600 A, normally open (NO)	911.2	4	0.004 389 750	1 995 558	6.00	2.93	2.94
		E12-421	Circuit breaker, metal clad (drawout), ≤ 600 V, > 600 A, normally closed (NC)	2290.1	153	0.066 809 897	131 118	9.90	2.56	26.74
		E12-422	Circuit breaker, metal clad (drawout), ≤ 600 V, > 600 A, normally open (NO)	622.9	4	0.006 421 989	1 364 063	2.00	2.38	2.37
	Oil filled			1573.9	640	0.406 641 344	21 542	19.01	28.83	30.54
		E12-512	Circuit breaker, oil filled, > 5 kV, normally closed (NC)	1392.3	631	0.453 204 694	19 329	18.98	28.84	30.56
		E12-511	Circuit breaker, oil filled, > 5 kV, Normally open (NO)	181.6	9	0.049 569 941	176 720	23.75	8.00	20.60
	SF6 filled	E12-610	Circuit breaker, SF6 filled, normally closed (NC)	315.2	418	1.326 315 057	6605	12.81	51.03	42.52
	Vacuum			3170.7	96	0.030 277 684	289 322	10.71	0.61	2.91
		E12-711	Circuit breaker, vacuum, < 15 kV, < 600 A, normally closed (NC)	514.4	3	0.005 832 348	1 501 968	5.33	0.05	0.06

		E12-712 ^a	Circuit breaker, vacuum, < 15 kV, < 600 A, normally closed (NC)	458.2	0	0.001 512 626	7 870 965		1.84	1.84
		E12-721	Circuit breaker, vacuum, < 15 kV, > 600 A, normally closed (NC)	1476.2	65	0.044 031 239	198 950	11.58	2.60	14.89
		E12-722	Circuit breaker, vacuum, < 15 kV, > 600 A, normally closed (NC)	716.8	28	0.039 061 903	224 259	9.39	0.35	0.49
		E12-730 ^a	Circuit breaker, vacuum, > 15 kV	5.0	0	0.138 553 516	85 929			
Compressor	Refrigerant			1344.2	19	0.014 134 513	619 760	8.69	0.93	1.02
		H11-010	Compressor, refrigerant, ≤ 1 ton (3.52 kW)	74.7	2	0.026 780 146	327 108	9.00	1.31	1.53
		H11-020	Compressor, refrigerant, > 1 ton (3.52 kW)	1052.0	5	0.004 752 765	1 843 138	3.50	0.91	0.93
		H11-100	Compressor, refrigerant, screw	217.5	12	0.055 165 812	158 794	10.83	0.94	1.15
Computer				406.3	100	0.246 142 641	35 589	4.30	4.82	23.48
	Control system server	C02-200	Computer, control system server	156.9	94	0.598 997 888	14 624	4.52	4.65	27.62
	Personal computer (PC) workstation	C02-100	Computer, PC workstation	249.3	6	0.024 063 554	364 036	1.90	5.09	4.09
Condenser				3972.6	305	0.076 775 438	114 099	8.10	2.83	4.91
	Double tube	H12-100	Condensers, double tube	298.7	8	0.026 781 865	327 087	2.50	2.63	2.63
	Propeller type fans/coils	H12-200	Condensers, propeller type fans with coils, direct expansion (DX)	2097.2	267	0.127 309 780	68 809	8.18	1.98	4.91
	Shell and tube	H12-300	Condenser, shell and tube	1576.7	30	0.019 027 462	460 387	9.50	6.86	7.06
Control center	Motor/load center	C03-100	Control center, motor/load center	1109.4	12	0.010 816 417	809 880	5.03	6.40	6.38
Control panel				6247.8	73	0.011 684 020	749 742	2.86	4.29	4.36
	Generator	C04-100	Control panel, generator, w/o switchgear	1808.4	30	0.016 589 350	528 050	4.38	0.62	1.45
	Heating, ventilation, and air conditioning (HVAC)/chillers/air-handling unit (AHU)	C04-200	Control panel, HVAC/chillers/AHU, w/o switchgear	3841.9	32	0.008 329 286	1 051 711	2.07	1.41	1.45
	Switchgear controls	C04-300	Control panel, switchgear controls	597.6	11	0.018 407 130	475 903	1.27	7.01	6.96

Control system				605.1	385	0.636 294 482	13 767	5.35	0.92	1.68
	≤ 1000 acquisition points	C12-100	Control system, ≤ 1000 acquisition points	384.7	99	0.257 318 645	34 043	1.73	1.26	1.43
	> 1000 acquisition points	C12-200	Control system, > 1000 acquisition points	220.3	286	1.298 060 184	6749	6.75	0.88	1.72
Convector	Fin tube baseboard			6387.9	8	0.001 252 62	6 994 782	2.44	0.13	0.15
		H13-110	Convector, fin tube baseboard, electric	1519.8	8	0.005 263 936	1 664 154	2.44	0.33	0.43
		H13-120 ^a	Convector, fin tube baseboard, steam or hot water	4868.2	0	0.000 142 384	83617694		0.08	0.08
Cooling tower				2063.7	556	0.269 418 665	32514	13.56	1.50	2.24
	Atmospheric type (w/o fans)	H14-100	Cooling tower, atmospheric type (w/o fans, motors, and internal lift pump)	323.7	24	0.074 137 736	118158	88.92	0.99	1.14
	Atmospheric type (with fans)	H14-300	Cooling tower, atmospheric type (with fans, motors, and internal lift pump)	1037.4	502	0.483 905 897	18103	8.77	4.34	8.28
	Evaporative type (w/o fans)	H14-200	Cooling tower, evaporative type (w/o fans, motors, and internal lift pump)	515.3	3	0.005 821 372	1 504 800	16.67	1.44	1.46
	Evaporative type (with fans)	H14-400	Cooling tower, evaporative type (with fans, motors, and internal lift pump)	187.2	27	0.144 194 894	60 751	6.25	3.83	4.78
Damper assembly				18 711.9	74	0.003 954 699	2 215 086	23.10	0.07	0.65
	Motor operated	H15-100	Damper assembly, motor operated	15 793.2	48	0.003 039 287	2 882 255	28.73	0.07	0.54
	Pneumatically operated	H15-200	Damper assembly pneumatically operated	2918.7	26	0.008 907 946	983 392	11.83	4.00	59.87
Dehumidifier	> 10 lb/h (4.54 kg/h)	H16-100	Dehumidifier, > 4.54 kg/h (10 lb/h)	98.3	68	0.691 808 122	12 662	16.26	17.27	32.31
Direct fired furnace				1301.1	404	0.310 517 283	28 211	3.64	13.86	23.35
	≤ 500 MB/h	H17-100	Direct fired furnace, ≤ 500 MBH (147 kW)	161.4	6	0.037 173 459	235 652	0.83	3.33	3.82
	> 500 MB/h	H17-200	Direct fired furnace, >500 MBH (147 kW)	1139.6	398	0.349 230 237	25 084	3.67	15.69	24.90
Distribution panel				7939.1	31	0.003 904 724	2 243 436	20.86	3.4	11.70

	≤ 225 A	E13-100	Distribution panel, ≤ 225 A, circuit breakers, not included (wall mount unit)	6552.6	25	0.003 815 271	2 296 036	22.69	1.41	10.90
	> 225 A	E13-200	Distribution panel, > 225 A, circuit breakers, not included (wall mount unit)	1386.5	6	0.004 327 482	2 024 272	16.00	10.06	14.34
Drive				4534.9	169	0.037 266 634	235 063	13.08	2.15	14.04
	Adjustable speed	E14-100	Drive, adjustable speed	3158.4	96	0.030 395 480	288 201	15.51	3.45	22.10
	Variable frequency	E14-200	Drive, variable frequency	1376.5	73	0.053 032 158	165 183	9.07	1.28	7.59
Engine				1245.6	2007	1.611 246 868	5437	1.36	2.87	2.71
	Diesel	E15-100	Engine, diesel	207.2	134	0.646 760 906	13 544	9.64	3.27	4.11
	Gas	E15-200	Engine, gas	1038.4	1873	1.803 679 412	4857	1.00	0.75	0.94
Evaporator	Coil			8150.2	40	0.004 907 850	1 784 896	13.03	0.27	0.29
		H18-100	Evaporator, direct expansion, coil	7114.1	31	0.004 357 533	2 010 312	14.55	0.27	0.29
		H18-120	Evaporator, direct expansion, shell tube	1036.1	9	0.008 686 501	1 008 461	5.17	0.28	0.30
Fan				19 708.4	1549	0.078 595 830	111 456	10.70	2.09	3.71
	Centrifugal	H19-100	Fan, centrifugal	11 895.7	577	0.048 504 894	180 600	10.51	1.71	3.57
	Propeller/disc	H19-200	Fan, propeller/disc	3857.7	649	0.168 236 811	52 069	10.88	2.09	4.37
	Tubeaxial	H19-300	Fan, tubeaxial	2244.8	69	0.030 737 667	284 992	5.51	4.04	4.09
	Vaneaxial	H19-400	Fan, vaneaxial	1710.3	254	0.148 515 645	58 984	14.24	1.10	1.61
Filter				5796.7	33	0.005 692 936	1 538 749	11.66	0.30	0.36
	Electrical	E16-200 ^a	Filter, electrical, tempest	342.1	0	0.002 026 405	5 875 341			
	Mechanical			5454.6	33	0.006 049 940	1 447 948	11.66	0.30	0.36
		H20-100	Filter, mechanical, air regulator set	3314.5	22	0.006 637 450	1 319 784	15.33	0.05	0.08
		H20-200 ^a	Filter, mechanical, fuel oil	743.2	0	0.000 932 659	12 765 459		0.49	0.49
		H20-300	Filter, mechanical, lube oil	1396.9	11	0.007 874 695	1 112 424	3.95	1.47	1.72
Fuse				10 226.0	483	0.047 232 405	185 466	4.00		4.00
	> 15 kV	E17-300	Fuse, > 15 kV	4756.7	483	0.101 541 423	86 270	4.00		4.00
	> 5 kV ≤ 15 kV	E17-200 ^a	Fuse, > 5 kV ≤ 15 kV	3590.5	0	0.000 193 050	61 672 329			
	0 kV to 5 kV	E17-100 ^a	Fuse, 0 kV to 5 kV	1878.8	0	0.000 368 923	32 271 812			
Gauge	Fluid level	C05-100	Gauge, fluid level	830.2	4	0.004 817 989	1 818 186	3.31	7.13	6.04
Generator				4538.6	2283	0.503 018 519	17 415	23.24	2.93	3.93

	Diesel engine			3045.1	1305	0.428 550 581	20 441	19.29	2.02	3.08
		E18-111	Generator, diesel engine, packaged, < 250 kW, continuous	15.0	16	1.063 558 550	8 237			
		E18-112	Generator, diesel engine, packaged, < 250 kW, standby	857.8	281	0.327 590 557	26 741	12.24	1.69	4.88
		E18-121	Generator, diesel engine, packaged, 250 kW to 1.5 MW, continuous	266.0	155	0.582 686 262	15 034	25.74	0.52	1.15
		E18-122	Generator, diesel engine, packaged, 250 kW to 1.5 MW, standby	1439.8	358	0.248 652 553	35 230	12.95	1.72	2.63
		E18-211	Generator, diesel engine, unpackaged, 750 kW to 7 MW, continuous	180.6	328	1.815 727 611	4825	25.08	3.86	5.00
		E18-212	Generator, diesel engine, unpackaged, 750 kW to 7 MW, standby	285.9	167	0.584 093 735	14 998	23.91	2.57	3.11
	Gas turbine			983.7	485	0.493 016 528	17 768	25.05	2.39	2.72
		E19-111	Generator, gas turbine, packaged, 750 kW to 7 MW, continuous	185.5	295	1.590 684 138	5507	27.31	0.83	1.23
		E19-112	Generator, gas turbine, packaged, 750 kW to 7 MW, standby	612.4	113	0.184 526 491	47 473	6.05	4.40	4.42
		E19-211	Generator, gas turbine, unpackaged, 750 kW to 7 MW, continuous	185.9	77	0.414 185 923	21 150	50.33	13.26	15.87
	Hydro turbine	E20-000	Generator, hydro turbine	90.4	27	0.298 790 286	29 318	78.36	238.44	310.21
	Natural gas			281.4	250	0.888 285 342	9862	5.87	139.75	64.13
		E21-110	Generator, natural gas, < 250 kW, continuous	7.4	5	0.674 926 036	12 979	1.50		1.50
		E21-120	Generator, natural gas, < 250 kW, standby	222.4	31	0.139 419 404	62 832	6.33	32.87	34.60
		e21-210	generator, natural gas, ≥ 250 kW, continuous	51.7	214	4.140 691 264	2116		191.73	71.13
	Steam	E23-000	Generator, steam, heat recovery	20.5	86	4.185 891 452	2093	162.40		45.84
	Steam turbine	E22-000	Generator, steam turbine	117.4	130	1.107 687 280	7908	100.59	288.24	263.61
	Heat exchanger			4858.5	272	0.055 984 436	156 472	10.81	1.11	1.74

	Boiler system	H21-100	Heat exchanger, boiler system, steam	964.0	164	0.170 129 316	51 490	7.22	18.15	19.15
	Lube oil	H21-200	Heat exchanger, lube oil	546.2	15	0.027 462 330	318 982	12.21	6.52	14.46
	Radiator	H21-310	Heat exchanger, radiator, small tube	1801.7	65	0.036 076 572	242 817	12.55	0.23	0.60
	Water to water	H21-400	Heat exchanger, water to water	1546.6	28	0.018 104 293	483 863	10.10	0.38	0.86
Heat pump	All types	H22-000	Heat pump	1330.4	82	0.061 635 471	142 126	3.26	0.76	6.37
Heater	Lube/fuel oil or jacket water	E24-110	Heater, lube/fuel oil or jacket water, electric	768.1	62	0.080 713 618	108 532	3.13	1.21	1.28
Humidifier	All types	H23-000	Humidifier	1569.1	38	0.024 217 472	361 722	4.11	1.86	2.00
Humistat assembly	All types	H24-000	Humistat assembly	643.3	10	0.015 544 284	563 551	1.00		1.00
Inverter	All types	E25-000	Inverter, all types	612.1	38	0.062 079 275	141 110	17.45	3.93	7.59
Line conditioner	All types	E26-000 ^a	Line conditioner, all types	10.7	0	0.064 971 423	183 247			
Meter				18 288.1	26	0.001 421 689	6 161 684	38.78	0.38	1.80
	Electric	C06-100	Meter, electric	15 067.2	7	0.000 464 587	18 855 470	1.29	3.29	3.10
	Fuel	C06-200	Meter, fuel	238.2	13	0.054 567 200	160 536	72.00		72.00
	Water	C06-300	Meter, water	2982.7	6	0.002 011 594	4 354 756	4.75	0.01	0.04
Motor	Electric			33 939.9	567	0.016 705 988	524 363	29.11	1.09	3.59
		E29-100	Motor, electric, dc	1513.9	119	0.078 605 141	111 443	67.60	0.42	0.97
		E29-210	Motor, electric, induction, ≤ 600 V	3195.9	340	0.106 385 715	82 342	21.50	14.55	53.01
		E29-220	Motor, electric, induction, > 600 V	429.9	11	0.025 584 819	342 391	4.44	3.29	3.31
		E29-310 ^a	Motor, electric, single phase, ≤ 5 A	25 377.5	0	0.000 027 314	435 895 106		0.49	0.49
		E29-320	Motor, electric, single phase, > 5 A	1455.1	1	0.000 687 237	12 746 688	3.00	0.71	0.72
		E29-410	Motor, electric, synchronous, ≤ 600 V	1726.6	94	0.054 441 911	160 905	7.34	1.77	6.37
		E29-420	Motor, electric, synchronous, > 600 V	241.0	2	0.008 298 661	1 055 592	36.00	3.00	4.65
Motor generator set	3 phase			509.9	23	0.045 104 339	194 216	6.71	0.84	0.84
		E27-120	Motor generator set, 3 phase, 400 Hz	202.6	1	0.004 937 036	1 774 344	8.00	2.87	2.89

		E27-110	Motor generator set, 3 phase, 60 Hz	307.4	22	0.071 573 093	122 392	6.62	0.82	0.83
Motor starter				4056.8	33	0.008 134 545	1 076 889	4.33	0.62	1.34
	≤ 600 V	E28-100	Motor starter, ≤ 600 V	3505.6	28	0.007 987 258	1 096 747	3.37	0.72	1.66
	> 600 V	E28-200	Motor starter, > 600 V	551.2	5	0.009 071 298	965 683	9.15	0.48	0.87
Network hub				234.0	2	0.008 545 408	1 025 112	2.75		2.75
	Ethernet	C07-100	Network hub, Ethernet	229.0	2	0.008 732 057	1 003 200	2.75		2.75
	Fiber-optic	C07-200 ^a	Network hub, fiber-optic	5.0	0	0.138 553 516	85 929			
Network printer				13 311.4	4682	0.351 727 580	24 906	1.69	1.55	3.29
	Inkjet	NWP-100	Network printer, inkjet	1260.0	670	0.531 744 876	16 474	1.74	1.78	5.57
	Laser	NWP-200	Network printer, laser	12 051.4	4012	0.332 906 396	26 314	1.68	1.50	2.87
Oil cooler	All types	E30-000	Oil cooler	92.9	3	0.032 302 791	271 184	13.25	0.50	2.20
Pipe				14 886.9	22	0.001 477 814	5 927 674	8.38	7.72	7.72
	Flex			1818.8	10	0.005 498 167	1 593 258	3.38	4.00	3.50
		H25-112	Pipe, flex, non-reinforced, > 100 mm (4 in)	206.3	3	0.014 544 485	602 290	3.33	4.00	3.60
		H25-111	Pipe, flex, reinforced, < 100 mm (4 in)	273.8	3	0.010 957 670	799 440	8.00		8.00
		H25-122	Pipe, flex, reinforced, > 100 mm (4 in)	1338.7	4	0.002 987 876	2 931 848	2.25		2.25
	Refrigerant			11 221.0	6	0.000 534 713	16 382 612	9.33	3.06	3.20
		H25-310	Pipe, refrigerant, < 25 mm per 30.5 m (1 in per 100 ft)	7913.6	3	0.000 379 094	23 107 704	10.67	2.00	2.11
		H25-320	Pipe, refrigerant, 25 mm to 80 mm per 30.5 m (1 in to 3 in per 100 ft)	3307.4	3	0.000 907 065	9 657 520	8.00	8.78	8.73
	Water			1847.1	6	0.003 248 338	2 696 764	14.08	8.00	8.01
		H25-410 ^a	Pipe, water, ≤ 50 mm per 30.5 m (2 in per 100 ft)	462.5	0	0.001 498 852	7 943 294			
		H25-450 ^a	Pipe, water, > 300 mm per 30.5 m (12 in per 100 ft)	8.2	0	0.084 984 454	140 094			
		H25-420	Pipe, water, 50 mm to 100 mm per 30.5 m (2 in to ≤ 4 in per 100 ft)	292.3	6	0.020 530 031	426 692	14.08		14.08
		H25-430 ^a	Pipe, water, 100 mm to 200 mm per 30.5 m (4 in to 8 in per 100 ft)	268.7	0	0.002 579 961	4 614 729			

		H25-440 ^a	Pipe, water, 200 mm to 300 mm per 30.5 m (8 in to 12 in per 100 ft)	815.6	0	0.000 849 893	14 008 612		8.00	8.00
Pressure control assembly	All types	C08-000	Pressure control assembly	896.3	82	0.091 485 687	95 753	8.10	3.53	4.08
Pressure regulator	Hot gas	C09-100	Pressure regulator, hot gas	2711.4	29	0.010695434	819 041	2.94	1.68	19.52
Programmable logic controller	All types	C10-000	Programmable logic controller (PLC)	203.9	6	0.029 422 829	297 728	23.50	2.00	73.27
Pump				25 386.6	3097	0.121 993 479	71 807	11.83	1.75	6.24
	Centrifugal			23 888.4	2917	0.122 109 700	71 739	11.91	1.92	6.47
		H26-110	Pump, centrifugal, with drive	21 835.4	2655	0.121 591 798	72 045	11.95	2.21	7.95
		H26-120	Pump, centrifugal, w/o drive	2052.9	262	0.127 621 356	68 641	11.28	1.04	1.52
	Positive displacement	H26-200	Pump, positive displacement	1498.2	180	0.120 140 438	72 915	7.91	0.70	4.74
Recloser (interrupter)				8368.5	85	0.010 157 168	862 445	5.00	6.02	5.97
	Electronic	E31-100	Recloser (interrupter), electronic	1949.4	13	0.006 668 840	1 313 572			
	Hydraulic	E31-200	Recloser (interrupter), hydraulic	2939.1	58	0.019 734 144	443 901		8.00	8.00
	Undefined type	E31-099 ^a	Recloser (interrupter), undefined type	3480.0	14	0.004 022 941	2 177 511	5.00	5.00	5.00
Rectifiers	All types	E32-000	Rectifiers, all types	563.4	2	0.003 549 686	2 467 824	16.00	3.45	3.47
Relay	Electromechanical			5307.4	5	0.000 942 089	9 298 488	26.33	3.63	3.70
		E33-110	Relay, electromechanical, differential, differential voltage	828.1	2	0.002 415 059	3 627 240	35.50	4.28	4.51
		E33-120 ^a	Relay, electromechanical, drawout	790.4	0	0.000 876 976	13 576 000			
		E33-130	Relay, electromechanical, overcurrent	3688.8	3	0.000 813 265	10 771 400	8.00	3.35	3.36
Router	Wired	RTR-100	Router, wired	2763.5	262	0.094 806 605	92 399	2.14	1.13	3.37
Sending unit				43 914.1	171	0.003 893 968	2 249 633	6.39	0.07	1.56
	Air velocity	C13-100	Sending unit, air velocity	7492.2	47	0.006 273 186	1 396 420	6.96	0.04	1.30
	Pressure	C13-200	Sending unit, pressure	7565.9	95	0.012 556 363	697 654	5.82	0.10	2.22
	Temperature	C13-300	Sending unit, temperature	28 856.0	29	0.001 004 991	8 716 496		0.25	0.39
Server				8145.9	540	0.066 290 672	132 145	3.02	1.00	2.41

	Blade	SVR-100	Server, blade	526.0	25	0.047 528 517	18 310	2.68	0.70	2.29
	Rack mount	SVR-200	Server, rack mount	6323.2	387	0.061 203 480	143 129	3.02	0.98	2.38
	Tower case	SVR-300	Server, tower case	1296.8	128	0.0987 065 589	88 748	3.08	1.09	2.49
Strainer				9788.4	88	0.008 990 193	974 395	16.96	0.35	0.62
	Air or gaseous	H27-110	Strainer, air or gaseous, air systems	304.2	1	0.003 287 222	266 4864			
	Liquid			9484.2	87	0.009 173 117	954 964	16.96	0.35	0.62
		H27-210 ^a	Strainer, liquid, coolant	488.2	0	0.001 419 921	8 384 847		1.62	1.62
		H27-220 ^a	Strainer, duplex fuel/lube oil	280.2	0	0.002 473 565	4 813 224		0.86	0.86
		H27-230 ^a	Strainer, liquid, fuel oil	460.4	0	0.001 505 416	7 908 659		1.67	1.67
		H27-240	Strainer, liquid, lube oil	1161.2	25	0.021 528 741	406 898	14.29	1.85	4.12
		H27-251	Strainer, water, ≤ 100 mm (4 in)	6466.1	25	0.003 866 327	2 265 716	2.25	0.00	0.00
		H27-252	Strainer, water, > 100 mm (4 in)	628.1	37	0.058 908 203	148 706	25.58	4.03	8.99
Switch				36 667.8	385	0.010 499 665	834 312	8.63	2.01	7.08
	Automatic transfer			2883.7	101	0.035 024 398	250 111	7.89	2.40	2.96
		E34-110	Switch, automatic transfer, ≤ 600 V, > 600 A	1030.8	27	0.026 193 875	334 429	2.66	8.98	8.32
		E34-120	Switch, automatic transfer, ≤ 600 V, 0 A to 600 A	1852.9	74	0.039 936 775	219 347	9.90	1.82	2.42
	Disconnect			19 349.5	23	0.001 188 660	7 369 646	17.83	1.75	1.90
		E34-211	Switch, disconnect, enclosed, ≤ 600 V	8372.7	6	0.000 716 616	12 224 124		2.09	2.09
		E34-212	Switch, disconnect, enclosed, > 600 V to ≤ 5 kV	2238.8	2	0.000 893 351	9 805 776	46.00	3.03	3.38
		E34-213	Switch, disconnect, enclosed, > 5 kV	2091.2	15	0.007 172 820	1 221 277	15.82	2.08	2.86
		E34-222 ^a	Switch, disconnect, fused, dc, > 600 A; ≤ 600 V	861.5	0	0.000 804 591	14 797 365			
		E34-221 ^a	Switch, disconnect, fused, dc, ≤ 600 A; ≤ 600 V	5785.4	0	0.000 119 811	99 372 047		0.54	0.54
	Electric	E34-310	Switch, electric, on/off breaker type, non-knife, ≤ 600 V	3115.2	2	0.000 642 008	13 644 684	1.00	0.01	0.01
	Float	E34-400	Switch, float, electric	2513.6	87	0.034 611 071	253 098	9.84	0.91	22.86
	Manual transfer			640.4	0	0.001 082 408	10 999 388			

		E34-510 ^a	Switch, manual transfer, ≤ 600 V, ≤ 600 A	266.6	0	0.002 599 818	4 579 482			
		E34-520 ^a	Switch, manual transfer, ≤ 600 V, > 600 A	373.8	0	0.001 854 517	6 419 906			
	Oil filled	E34-610 ^a	Switch, oil filled, ≥ 5 kV	300.2	0	0.002 308 614	5 157 129		1.38	1.38
	Pressure	E34-700	Switch, pressure	6661.0	169	0.025 371 639	345 267	7.04	3.08	16.89
	Static			921.5	2	0.002 170 468	4 035 996	13.00	2.04	2.11
		E34-810 ^a	Switch, static, ≤ 600 V, 0 A to 600 A	498.4	0	0.001 390 875	8 559 953		0.03	0.03
		E34-820	Switch, static, ≤ 600 V, > 600 A ≤ 1000 A	130.0	1	0.007 692 794	1 138 728	2.00	0.05	0.08
		E34-830	Switch, static, ≤ 600 V, > 1000 A	271.7	1	0.003 680 066	2 380 392	24.00	3.47	3.58
		E34-850 ^a	Switch, static, with insulated-gate bipolar transistor (IGBT) technology	15.3	0	0.045 210 636	26 3341			
		E34-860 ^a	Switch, static, w/o IGBT technology	6.0	0	0.114 582 754	103 906			
	Vibration	E34-900	Switch, vibration	282.7	1	0.003 537 644	2 476 224		0.50	0.50
Switchgear				6747.6	47	0.006 965 393	1 257 646	24.32	3.35	3.56
	Bare bus			4229.7	42	0.009 929 718	882 200	24.31	3.64	3.94
		E36-110	Switchgear, bare bus, ≤ 600 V (circuit breaker not included)	2493.6	23	0.009 223 683	949 729	7.91	4.28	4.35
		E36-130	Switchgear, bare bus, > 5 kV (circuit breaker not included)	895.7	15	0.016 746 168	523 105	2.27	1.28	1.30
		E36-120	Switchgear, bare bus, > 600 V to ≤ 5 kV (circuit breaker not included)	840.4	4	0.004 759 530	1 840 518	195.75	6.59	9.67
	Insulated bus			1713.6	5	0.002 917 820	3 002 242	24.40	2.90	2.97
		E36-210 ^a	Switchgear, insulated bus, ≤ 600 V (circuit breaker not included)	505.2	0	0.001 372 077	8 677 224		3.18	3.18
		E36-220	Switchgear, insulated bus, > 600 V to ≤ 5 kV (circuit breaker not included)	405.8	2	0.004 928 902	1 777 272	5.00	0.77	0.78
		E36-230	Switchgear, insulated bus, > 5 kV (circuit breaker not included)	802.7	3	0.003 737 584	2 343 760	37.33	14.01	14.43

	Load center (free standing unit)	E36-300 ^a	Switchgear, load center (free standing unit)	804.3	0	0.000 861 792	13 815 200		0.59	0.59
Tank				4876.1	137	0.028 096 327	311 785	18.02	1.11	3.10
	Air	E37-110	Tank, air, receiver	1519.1	22	0.014 482 011	604 888	11.53	1.25	1.63
	Liquid			3357.0	115	0.034 257 224	255 712	18.99	0.88	5.31
		E37-210	Tank, liquid, day, fuel	484.8	2	0.004 125 040	2 123 616	5.00	0.31	0.35
		E37-220	Tank, liquid, fuel	614.7	21	0.034 162 930	256 418	13.80	1.28	2.52
		E37-230	Tank, liquid, water	2257.4	92	0.040 754 653	214 945	20.57	0.91	7.23
Thermocouple	All types	C14-000	Thermocouple	5761.5	101	0.017 530 270	499 707	13.48	14.00	479.86
Thermostat	Radiator	C15-100	Thermostat, radiator	8735.0	153	0.017 515 835	500 119	3.16	1.13	2.00
Transducer				26 305.4	81	0.003 079 211	2 844 885	3.74	0.06	0.09
	Flow	C16-100	Transducer, flow	1188.0	5	0.004 208 706	2 081 400	2.00	1.17	1.18
	Pressure	C16-200	Transducer, pressure	2139.0	28	0.013 090 212	669 202	7.50	2.28	3.07
	Temperature	C16-300	Transducer, temperature	22 978.4	48	0.002 088 916	4 193 563	1.89	0.02	0.03
Transformer				164 239.4	456	0.002 776 435	3 155 125	14.92	10.83	11.43
	Dry			96 735.4	248	0.002 563 695	3 416 944	3.63	2.77	3.40
		E38-111	Transformer, dry, air cooled, ≤ 500 kVA	86095.4	226	0.002 624 996	3 337 148	2.13	2.36	2.33
		E38-112	Transformer, dry, air cooled, > 500 kVA ≤ 1500 kVA	1700.3	3	0.001 764 436	4 964 760	2.00	5.41	36.50
		E38-113 ^a	Transformer, dry, air cooled, > 1500 kVA ≤ 3000 kVA	999.7	0	0.000 693 337	17 171 772		4.39	4.39
		E38-114 ^a	Transformer, dry, air cooled, > 3000 kVA ≤ 5000 kVA	1142.2	0	0.000 606 854	19 618 918		5.50	5.50
		E38-121	Transformer, dry, isolation, delta wye, < 600 V	6797.8	19	0.002 795 011	3 134 156	21.26	0.93	2.52
	Liquid			67 504.0	208	0.00 3081 299	2 842 957	36.89	13.29	14.16
		E38-211	Transformer, liquid, forced air, ≤ 5000 kVA	5849.5	52	0.008 889 630	985 418	8.69	0.98	2.08
		E38-212	Transformer, liquid, forced air, > 5000 kVA ≤ 10 000	600.6	23	0.038 292 418	228 766	251.00	22.96	23.60
		E38-213	Transformer, liquid, forced air, > 10 000 kVA ≤ 50 000 kVA	482.1	34	0.070 518 976	124 222	965.33	21.69	24.34
		E38-214	Transformer, liquid, forced air, > 50 000	18.6	24	1.289 752 650	6792	11.95	2.43	5.30
		E38-221	Transformer, liquid, non-forced air, ≤ 3000 kVA	59 708.0	63	0.001 055 134	8 302 262	2.33	2.00	2.02

		E38-222	Transformer, liquid, non-forced air, > 3000 kVA ≤ 10 000 kVA	190.7	1	0.005 242 671	1 670 904	1.00	2.67	2.50
		E38-223	Transformer, liquid, non-forced air, > 10 000 kVA ≤ 50 000 kVA	654.3	11	0.016 811 614	521 068	6.09	0.58	0.65
UPS				1232.8	65	0.052 726 440	166 141	5.24	2.08	6.48
	Rotary	E39-100	Uninterruptible power supply (UPS), rotary	134.7	2	0.014 848 263	589 968	8.75	6.11	7.81
	Small computer room floor	E39-200	Uninterruptible power supply (UPS), small computer room floor	724.7	41	0.056 575 669	154 837	6.25	2.12	3.74
	Solid state			373.4	22	0.058 919 780	148 677	2.93	1.14	11.44
		E39-310	Uninterruptible power supply (UPS), solid state, 60 Hz/module	357.3	22	0.061 578 810	142 257	2.93	1.09	13.83
		E39-320 ^a	Uninterruptible power supply (UPS), solid state, with IGBT technology	16.1	0	0.042 990 437	276 941		1.30	1.30
Valve				157 135.7	1345	0.008 559 481	1 023 427	11.94	2.62	8.08
	3-way			16 490.6	7	0.000 424 484	20 636 822	5.86	0.52	0.81
		H28-110	Valve, 3-way, diverting/sequencing	736.9	4	0.005 428 034	1 613 844	9.13	0.02	0.59
		H28-120	Valve, 3-way, mixing control	15 753.7	3	0.000 190 432	46 000 792	1.50	1.02	1.03
	Backflow preventer	H28-200	Valve, backflow preventer	742.6	30	0.040 401 283	216 825	13.27	1.11	15.63
	Ball			2703.6	5	0.001 849 362	4 736 770	1.20	0.19	0.24
		H28-310 ^a	Valve, ball, normally closed (NC)	1092.7	0	0.000 634 368	18 768 000		0.19	0.19
		H28-320	Valve, ball, normally open (NO)	1611.0	5	0.003 103 705	2 822 434	1.20		1.20
	Butterfly			18 225.8	26	0.001 426 553	6 140 677	3.88	0.55	0.67
		H28-410	Valve, butterfly, normally closed (NC)	2809.7	26	0.009 253 770	946 641	3.88	1.01	1.67
		H28-420 ^a	Valve, butterfly, normally open (NO)	15 416.1	0	0.000 044 963	64 793 976		0.48	0.48
	Check	H28-500	Valve, check	4699.2	44	0.009 363 323	935 565	26.69	1.11	8.60
	Control			22 796.4	647	0.028 381 678	308 650	17.32	0.50	15.34
		H28-610	Valve, control, normally closed (NC)	17 563.1	388	0.022 091 808	396 527	17.76	0.23	8.54

		H28-620	Valve, control, normally open (NO)	5233.3	259	0.049 490 515	177 004	16.93	1.56	38.85
	Expansion	H28-700 ^a	Valve, expansion	1984.1	0	0.000 349 348	34 080 094			
	Gate			19 302.5	97	0.005 025 268	1 743 191	10.45	0.81	33.26
		H28-830	Valve, gate, double flap	173.2	76	0.438 785 195	19 964	10.67		10.67
		H28-810	Valve, gate, normally closed (NC)	1830.5	8	0.004 370 485	2 004 354	7.50	0.59	0.99
		H28-820	Valve, gate, normally open (NO)	17 298.8	13	0.000 751 498	11 656 721	9.31	1.30	150.13
	Globe			41 402.3	66	0.001 594 112	5 495 221	16.65	1.00	1.74
		H28-910 ^a	Valve, globe, normally closed (NC)	22 125.4	0	0.000 031 328	80 035 718		1.00	1.00
		H28-920	Valve, globe, normally open (NO)	19 277.0	66	0.003 423 773	2 558 581	16.65	0.40	129.72
	Plug			15 233.3	148	0.009 715 539	901 648	1.81	0.05	1.59
		H28-A10	Valve, plug, normally closed (NC)	8845.9	123	0.013 904 727	630 002	1.37	0.05	1.17
		H28-A20	Valve, plug, normally open (NO)	6387.4	25	0.003 913 946	2 238 151	4.00		4.00
	Reducing	H28-B10	Valve, reducing, makeup water	701.9	100	0.142 473 496	61 485	5.56	0.59	17.99
	Relief	H28-C00	Valve, relief	10 598.4	165	0.015 568 452	562 676	7.55	102.91	137.61
	Suction	H28-D00	Valve, suction	2255.1	10	0.004 434 439	1 975 447	7.25	0.61	0.77
Valve operator				10 025.1	80	0.007 980 004	1 097 744	10.02	1.06	1.47
	Electric	C17-100	Valve operator, electric	3684.0	43	0.011 672 052	750 511	16.42	0.98	1.40
	Hydraulic	C17-200	Valve operator, hydraulic	68.2	6	0.087 937 681	99 616	3.00	2.16	2.20
	Pneumatic	C17-300	Valve operator, pneumatic	6272.8	31	0.004 941 961	1 772 576	2.92	0.98	1.76
Voltage regulator	Static	E40-100	Voltage regulator, static	3381.5	77	0.022 771 080	384 698	15.73	0.53	2.23
Water cooling coil	Fan coil unit	H29-100	Water cooling coil, fan coil unit	16 076.0	96	0.005 971 646	1 466 932	3.72	2.04	2.09
Water heater	Domestic hot water			1399.8	44	0.031 431 955	278 697	6.37	1.28	12.85
		H30-110	Water heater, domestic hot water, electric	957.5	19	0.019 843 370	441 457	9.64	0.82	29.64
		H30-130	Water heater, domestic hot water, gas	442.4	25	0.056 516 246	155 000	3.53	1.35	9.11
Workstation	All types	WST-000	Workstation	169 635.1	7948	0.046 853 516	186 966	0.73	0.62	1.11

^a Failure rate calculated using 50% single-sided confidence interval. Part 2: Equipment reliability surveys conducted between 1976 and 1994.

APPENDIX E GLOSSARY

E-1 ACRONYMS.

AC	Alternating Current
AIAG	Automotive Industry Action Group
BIT	Build-in-Test
C5ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance
CA	Criticality Analysis
CAIP	Critical Asset Identification Process
CBA	Cost-Benefit Analysis
CND	Cannot Duplicate
CM	Corrective Maintenance
DOD	Department of Defense
DOE	Design of Experiments
EMSG	European Maintenance System Guide
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
FEA	Finite Element Analysis
FIT	Framework for Integrated Test
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FRACAS	Failure Reporting Analysis and Corrective Actions
FTA	Fault Tree Analysis
HFE	Human Factors Engineering
HVAC	Heating, Ventilating and Air Conditioning
IEEE	Institute of Electrical and Electronic Engineers

LRU	Line Replaceable Unit
MDT	Mean Downtime
MSG	Maintenance Steering Group
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
NASA	National Aeronautics and Space Administration
NEC	National Electrical Code
NERC	North American Electric Reliability Corporation
NDI	Nondestructive Inspection
NPRD	Nonelectronic Parts Reliability Data
O&M	Operations and Maintenance
O&S	Operating & Support
OEM	Original Equipment Manufacturer
OH	Operating Hours
OSHA	Occupational Safety and Health Administration
PC	Personal Computer
PDF	Probability Density Function
PLC	Programmable Logic Controller
PM	Preventative Maintenance
PREP	Power Reliability Enhancement Program
PREPIS	Power Reliability Enhancement Program Information System
QFD	Quality Function Deployment
R/A	Reliability/Availability
R&M	Reliability and Maintainability
R&R	Remove and Replace

RAM	Reliability, availability, and maintainability
RBD	Reliability Block Diagram
RCM	Reliability-Centered Maintenance
RGT	Reliability Growth Test
RPN	Risk Priority Number
RTOK	Retest OK
SCA	Sneak Circuit Analysis
SCADA	Supervisory Control and Data Acquisition
SE	Systems Engineering
TA	Thermal Analysis
TAAF	Test Analyze and Fix
TM	Technical Manual
UFC	Unified Facilities Criteria
UPS	Uninterruptable Power Supply
US	United States
USACE	United States Army Corps of Engineers
WCCA	Worst Case Circuit Analysis
WRA	Weapon Replaceable Assembly

E-2 DEFINITION OF TERMS.

Active Redundancy: Two or more components in a parallel combination where all are powered and active simultaneously. Not all components are required to function for the system (or next higher assembly) to function.

Active Time: That time during which an item is in an operational inventory.

Affordability: Affordability is a measure of how well customers can afford to purchase, operate, and maintain a product over its planned service life. Affordability is a function of product value and product costs. It is the result of a balanced design in which long-term support costs are considered equally with near-term development and manufacturing costs.

Alignment: Performing the adjustments that are necessary to return an item to specified operation.

Alpha (α): The probability, expressed as a decimal that a given part will fail in the identified mode. The sum of all alphas for a component will equal one (1).

Assessment: Current evaluation of a component's or system's reliability. A prediction.

Availability: The instantaneous probability that a component will be up.

Availability, Inherent (A_i): The instantaneous probability that a component will be up. A_i considers only downtime for repair due to failures. No logistics delay time, preventative maintenance, etc. is included.

Availability, Operational (A_o): A_o is the instantaneous probability that a component will be up but differs from inherent availability in that it includes ALL downtime. Included is downtime for both corrective maintenance and preventative maintenance, including any logistics delay time.

Beta (β): The conditional probability that the effect of a failure mode will occur, expressed as a decimal. If a failure is to occur, what is the probability that the outcome will occur.

Block Diagrams: Availability block diagrams and reliability block diagrams are visual representations of the interactions between contributors to reliability, availability, and maintainability. Each block tends to represent a physical component in the system and its associated reliability/availability.

Boolean Algebra: Boolean algebra is a method of calculating system availability based on logical interactions between components. AND and OR operators define mathematical operations.

Brownout: Occurs during a power failure when some power supply is retained, but the voltage level is below the minimum level specified for the system. A very dim household light is a symptom of a brownout.

Calibration: A comparison of a measuring device with a known standard and a subsequent adjustment to eliminate any differences. Not to be confused with alignment.

Cannot Duplicate (CND): A situation when a failure has been noted by the operator but cannot be duplicated by maintenance personnel attempting to correct the problem. Also see Retest OK.

Checkout: Tests or observations of an item to determine its condition or status.

Compensating Provision: Actions available or that can be taken to negate or reduce the effect of a failure on a system.

Component: A piece of electrical or mechanical equipment viewed as an entity for the purpose of reliability evaluation.

Condition-Based PM: Maintenance performed to assess an item's condition and performed as a result of that assessment. Some texts use terms such as predictive maintenance and on-condition. The definition of condition-based PM used herein includes these concepts. In summary, the objectives of condition-based PM are to first evaluate the condition of an item, then, based on the condition, either determine if a hidden failure has occurred or determine if a failure is imminent, and then take appropriate action. Maintenance that is required to correct a hidden failure is, of course, corrective maintenance.

Confidence Level/Interval: A statistical measure of the uncertainty associated with an estimate. For example, an estimate of MTBF is 103 hours. Using statistical techniques (such as the chi-square method) a 95% confidence interval of 100.1 to 105.9 is obtained. That is, 95% of the time, the actual MTBF will be between 100.1 and 105.9 hours. The confidence interval depends on sample size and variance.

Corrective Action: A documented design, process, procedure, or materials change implemented and validated to correct the cause of failure or design deficiency.

Corrective Maintenance (CM): All actions performed as a result of failure, to restore an item to a specified condition. Corrective maintenance can include any or all the following steps: Localization, Isolation, Disassembly, Interchange, Reassembly, Alignment and Checkout.

Cost: The expenditure of resources (usually expressed in monetary units) necessary to develop, acquire, or use a product over some defined period of time.

Critical Equipment/Systems: Critical equipment/systems include those items of equipment or systems that directly supply power to equipment and systems used to perform the primary mission(s) of the C5ISR site.

Criticality: A relative measure of the consequences of a failure mode and the frequency of its occurrence.

Criticality Analysis (CA): A procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

Critical Load: That portion of the technical load used to successfully accomplish the site missions and having a requirement for 100 percent continuity in power service, such as from the Uninterruptible Power Supply (UPS) system. These loads also include any equipment which, upon loss of power, will create an unacceptable impact on the mission or mission equipment.

Dependability: A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission. (Item state during a mission includes the combined effects of the mission-related system R&M parameters but excludes non-mission time; see availability).

Design Agency: The agency responsible for the overall design of the facility.

Detection Method: The method by which a failure can be discovered by the system operator under normal system operation or by a maintenance crew carrying out a specific diagnostic action.

Diagnostics: The hardware, software, or other documented means used to determine that a malfunction has occurred and to isolate the cause of the malfunction. Also refers to "the action of detecting and isolating failures or faults."

Downtime: That element of time during which an item is in an operational inventory but is not in condition to perform its required function.

Effectiveness: The degree to which PM can provide a quantitative indication of an impending functional failure, reduce the frequency with which a functional failure occurs, or prevent a functional failure.

End Effect: The consequence a failure mode has upon the operation, function, or status at the highest indenture level.

Equipment: A general term designating an item or group of items capable of performing a complete function.

Failure (f): The termination of the ability of a component or system to perform a required function.

Failure, Catastrophic: A failure that causes loss of the item, human life, or serious collateral damage to property.

Failure, Hidden: A failure that is not evident to the operator; that is, it is not a functional failure. A hidden failure may occur in two different ways. In the first, the item that has failed is one of two or more redundant items performing a given function. The loss of one or more of these items does not result in a loss of the function. The second way in which a hidden failure can occur is when the function performed by the item is

normally inactive. Only when the function is eventually required will the failure become evident to the operator. Hidden failures must be detected by maintenance personnel.

Failure, Intermittent: Failure for a limited period of time, followed by the item's recovery of its ability to perform within specified limits without any remedial action.

Failure, Random: A failure, the occurrence of which cannot be predicted except in a probabilistic or statistical sense.

Failure Analysis: Subsequent to a failure, the logical systematic examination of an item, its construction, application, and documentation to identify the failure mode and determine the failure mechanism and its basic course.

Failure Cause: The physical or chemical processes, design defects, quality defects, part misapplication or other processes which are the basic reason for failure, or which can initiate the physical process by which deterioration proceeds to failure.

Failure Effect: The consequence(s) a failure mode has on the operation, function, or status of an item. Failure effects are typically classified as local, next higher level, and end.

Failure Mechanism: The physical, chemical, electrical, thermal, or other process which results in failure.

Failure Mode: The way in which a failure is observed, describes the way the failure occurs, such as, short, open, fracture and excessive wear.

Failure Mode and Effects Analysis (FMEA): A procedure by which each potential failure mode in a product (system) is analyzed to determine the results or effects thereof on the product and to classify each potential failure mode according to its severity or risk probability number.

Failure Modes, Effects, and Criticality Analysis (FMECA): The term is used to emphasize the classifying of failure modes as to their severity (criticality).

Failure Rate (λ): The mean (arithmetic average, also known as the forced outage rate) number of failures of a component and/or system per unit exposure time. The most common unit in reliability analyses is hours (h). However, some industries use failures per year (f/y) which is denoted by the symbol (λ_y).

Failure Reporting and Corrective Action System (FRACAS): A closed-loop system for collecting, analyzing, and documenting failures and recording any corrective action taken to eliminate or reduce the probability of future such failures.

False Alarm: A fault indicated by BIT or other monitoring circuitry where no fault can be found or confirmed.

Fault: Immediate cause of failure (for example, maladjustment, misalignment, defect, etc.).

Fault Detection (FD): A process that discovers the existence of faults.

Fault Isolation (FI): The process of determining the location of a fault to the indenture level necessary to affect repair.

Fault Tree Analysis: An analysis approach in which each potential system failure is traced back to all faults that could cause the failure. It is a top-down approach, whereas the FMEA is a bottom-up approach.

Hidden Failure: See Failure, Hidden.

Hours Downtime Per Year (Hrdt/Year): Average hours the item is expected to be not functional in a one-year period, caused by both preventative maintenance and failures. This includes any logistics delay time.

Indenture Levels: The levels which identify or describe the relative complexity of an assembly or function.

Isolation: Determining the location of a failure to the extent possible, using accessory equipment.

Item: Used interchangeably in this document with product or equipment. Usually refers to the individual article rather than the inclusive class or kind of product.

Item Criticality Number (C_r): A relative measure of consequence of an item failure and its frequency of occurrence. This factor is not applicable to a qualitative analysis.

Laplace Statistic: A statistic used to determine if a data set indicates a positive or negative trend, at a given level of confidence.

Levels of Maintenance: The division of maintenance, based on different and requisite technical skill, which jobs are allocated to organizations in accordance with the availability of personnel, tools, supplies, and the time within the organization. Typical maintenance levels are organizational, intermediate, and depot.

Life Cycle Cost (LCC): The sum of acquisition, logistics support, operating, and retirement and phase-out expenses.

Line Replaceable Unit (LRU): A unit designed to be removed upon failure from a larger entity (product or item) in the operational environment, normally at the organizational level.

Local Effect: The consequence a failure mode has on the operation, function or status of the specific item being analyzed.

Localization: Determining the location of a failure to the extent possible, without using accessory test equipment.

Logistic Delay Time: That element of downtime during which no maintenance is being accomplished on the item because of either supply or administrative delay.

Logistics Support: The materials and services required to enable the operating forces to operate, maintain, and repair the end item within the maintenance concept defined for that end item.

Maintainability: The relative ease and economy of time and resources with which an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. Also, the probability that an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

Maintenance: All actions necessary for retaining an item in or restoring it to a specified condition.

Maintenance Action: An element of a maintenance event. One or more tasks (such as, fault localization, fault isolation, servicing, and inspection) necessary to retain an item's condition or restore it to a specified condition.

Maintenance Concept: A description of the planned general scheme for maintenance and support of an item in the operational environment. It provides a practical basis for design, layout, and packaging of the system and its test equipment. It establishes the scope of maintenance responsibility for each level of maintenance and the personnel resources required to maintain the system.

Maintenance Event: One or more maintenance actions required to effect corrective and preventive maintenance due to any type of failure or malfunction, false alarm, or scheduled maintenance plan.

Maintenance Task: The maintenance effort necessary for retaining an item in or changing/restoring it to a specified condition.

Maintenance Time: An element of downtime that excludes modification and delay time.

Mean: Also called the expected value of a random variable, the mean is defined as follows: Let X be a continuous random variable with a probability density function = f . The expected value of X is:

$$E(X) = \int_x xf(x)dx$$

The mean, or expected value, is analogous to the concept of center of mass in mechanics.

Mean Downtime (MDT): The average downtime caused by preventative and corrective maintenance, including any logistics delay time. This is synonymous with mean time to restore system (MTTRS) as found in some publications.

Mean Time Between Failures (MTBF): The mean exposure time between consecutive failures of a component. MTBF is a required measurement used for calculating inherent availability. It can be estimated by dividing the exposure time by the number of failures in that period.

Mean Time Between Maintenance (MTBM): The average time between all maintenance events that cause downtime, both preventative and corrective maintenance, and includes any associated logistics delay time.

Mean Time To Failure (MTTF): The mean exposure time between consecutive repairs (or installations) of a component and the next failure of that component. MTTF is commonly found for nonrepairable items such as fuses or bulbs, etc.

Mean Time To Maintain (MTTM): The average downtime for preventative maintenance. This includes any logistics delay time.

Mean Time To Repair (MTTR): The mean time to replace or repair a failed component. Logistics delay time associated with the repair, such as parts acquisitions, crew mobilization, are not included. It can be estimated by dividing the summation of repair times by the number of repairs and, therefore, is practically the average repair time. The most common unit in reliability analyses is hours (h/f).

Mission Phase Operational Mode: The statement of the mission phase and mode of operation of the system or equipment in which the failure occurs.

Mission Reliability: The probability that a system will complete its intended mission. Hardware failures that do not hinder the success of the mission (for example, due to redundancy) are not counted against mission reliability.

Next Higher Level Effect: The consequence a failure mode has on the operation, functions, or status of the items in the next higher indenture level above the specific item being analyzed.

Non-Destructive Inspection (NDI): Any method used for inspecting an item without physically, chemically, or otherwise destroying or changing the design characteristics of the item. However, it may be necessary to remove paint or other external coatings to use the NDI method. A wide range of technology and methods are usually described as nondestructive inspection, evaluation, or testing (collectively referred to as non-destructive evaluation or NDE). The core of NDE is commonly thought to contain ultrasonic, visual, radiographic, eddy current, liquid penetrant, and magnetic particle inspection methods. Other methodologies include acoustic emission, use of laser interference, microwaves, NMR and MRI, thermal imaging, and so forth.

On-Condition Maintenance: See Condition-based PM.

One-Line Diagram: A one-line diagram is a drawing of an electrical or mechanical system that shows how the parts interact. It shows paths of electrical flow, water flow, gas flow, etc. It will also list system component and component sizes.

Operating and Support (O&S) Costs: Those costs associated with operating and supporting (such as, using) a product after it is purchased or fielded.

Operational Readiness: The ability of a military unit to respond to its operation plan(s) upon receipt of an operations order. (A function of assigned strength, item availability, status, or supply, training, etc.).

Operational Reliability: The reliability of a system or equipment after it is put in operation.

Parallel Combination: The combining of two or more items in such a way that not all components are required for operation – thus, the parallel combination is characterized by alternate paths of operation.

Predicted: That which is expected at some future time, postulated on analysis of past experience and tests.

Predictive Maintenance: See Condition-based PM.

Preventative Maintenance (PM): All actions performed in an attempt to retain an item in a specified condition. These actions may or may not result in downtime for the component and may or may not be performed on a fixed interval.

Probability Distribution: A formula that describes the probabilities associated with the values of a discrete random variable.

Product: An equipment, item, or hardware contracted for by a customer. Usually used to describe the inclusive class or kind of item, equipment, etc., rather than each individual entity.

Qualitative Analysis: A means of conducting an analysis without data. Team member subjectively rank probabilities of occurrence, typically 1-10, in place of failure rates.

Quantitative Analysis: An analysis that is supported with data. Data is available for assigning failure rates and failure mode probabilities.

Reassembly: Assembling the items that were removed during disassembly and closing the reassembled items.

Redundancy: The existence of more than one means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical.

Reliability (R(t)): The probability that a component can perform its intended function for a specified time interval (t) under stated conditions. This calculation is based on the exponential distribution.

Reliability-Centered Maintenance (RCM): A disciplined logic or methodology used to identify preventive and corrective maintenance tasks to realize the inherent reliability of equipment at a minimum expenditure of resources, while ensuring safe operation and use.

Reliability Prediction: An estimate of reliability based on information that includes historical data, piece parts count, complexity, and piece part failure rates.

Retest Ok (RTOK): A situation where a failure was detected on the system, either through inspection or testing, but no fault can be found in the item that was eventually removed for repair at a field or depot location. Also see Cannot Duplicate.

Risk Priority Number (RPN): The Risk Priority Number (RPN) is the product of the Severity (1-10) and the Occurrence (1-10) ranking. The Risk Priority Number is used to rank and identify the concerns or risks associated with the operation due to the design. $RPN = (S) \times (O)$.

Severity: Considers the worst possible consequence of a failure classified by the degree of injury, property damage, system damage and mission loss that could occur.

Scheduled Maintenance: Periodic prescribed inspection and/or servicing of products or items accomplished on a calendar, mileage, or hours of operation basis. Included in Preventive Maintenance.

Servicing: The performance of any act needed to keep an item in operating condition, (such as lubricating, fueling, oiling, cleaning, etc.), but not including preventive maintenance of parts or corrective maintenance tasks.

Single-Point Failure: A failure of an item that causes the system to fail and for which no redundancy or alternative operational procedure exists.

Standby Redundancy: Two or more components in a parallel combination where not all components are required at any time. The other components are disconnected, and power is applied prior to or simultaneously with switching.

Subsystem: A combination of sets, groups, etc. that performs an operational function within a product (system) and is a major subdivision of the product. (Example: Data processing subsystem, guidance subsystem).

Success: Achievement of an objective or completion of a function or set of functions.

Switch: A device that selects one component in a parallel or redundant configuration as the functioning component. Used for standby redundancy. Incorporates such provisions as logic circuits and fault detection.

System: A group of components connected or associated in a fixed configuration to perform a specified function.

System Downtime: The time interval between the commencement of work on a system (product) malfunction and the time when the system has been repaired and/or checked by the maintenance person, and no further maintenance activity is executed.

Technical Load: That portion of the operational which consists of general lighting and heating, ventilating, and air conditioning (HVAC) systems necessary to maintain normal operations and loads directly associated with the C5ISR missions at the site.

Testability: A design characteristic that allows status (operable, inoperable, or degraded) of an item to be determined and the isolation of faults within the item to be performed in a timely manner.

Total Downtime Events (Tde): The total number of downtime events (including scheduled maintenance and failures) during the Tp.

Total Failures (Tf): The total number of failures during the Tp.

Total Maintenance Actions (Tma): The total number of preventative maintenance actions which take the component down during the Tp.

Total Period (Tp): The calendar time over which data for the item was collected.

Total System Downtime: The time interval between the reporting of a system (product) malfunction and the time when the system has been repaired and/or checked by the maintenance person, and no further maintenance activity is executed.

Unscheduled Maintenance: Corrective maintenance performed in response to a suspected failure.

Uptime: That element of ACTIVE TIME during which an item is in condition to perform its required functions. (Increases availability and dependability).

Useful Life: The number of life units from manufacture to when the item has an unreparable failure or unacceptable failure rate. Also, the period of time before the failure rate increases due to wearout.

User: The using Government Agency.

Using Government Agency: The Government Agency that will be responsible for completing the site missions and will have operational authority for the facility.

Wearout: The process that results in an increase of the failure rate or probability of failure as the number of life units increases.

Year (y): The unit of time measurement approximately equal to 8765.81277 hours (h). Any rounding of this value will have adverse effects on analyses depending on the magnitude of that rounding. 8766 is used commonly as it is the result of rounding to 365.25×24 (which accounts for a leap year every 4th year). 8760, which is 365×24 , is the most commonly used value in the power reliability field. By convention, 8760 will be used throughout this document.

CANCELLED

This Page Intentionally Left Blank

APPENDIX F REFERENCES

DEPARTMENT OF DEFENSE

DOD Instruction 3020.45, *Defense Critical Infrastructure Program (DCIP) Implementation*

MIL-M-24100, *Functionally Oriented Maintenance Manuals (FOMM) for Electronic, Electromechanical, and Ordnance Equipment, Systems, and Platforms*

MIL-STD-756, *Reliability Modeling and Prediction*

MIL-STD-785B, *Reliability Program for Systems and Equipment Development and Production*

MIL-STD-882, *Department of Defense Standard Practice: System Safety*

MIL-STD-1472, *Department of Defense Design Criteria Standard: Human Engineering*

MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*

GOVERNMENT

NASA, *Reliability Centered Maintenance Guide for Facilities and Collateral Equipment*

TM 5-691, *Utility Systems Design Requirements for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*

TM 5-698-1, *Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Facilities*

TM 5-698-2, *Reliability-Centered Maintenance (RCM) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*

TM 5-698-3, *Reliability Primer for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*

TM 5-698-4, *Failure Modes, Effects and Criticality Analysis (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*

TM 5-698-5, *Survey of Reliability and Availability Information for Power Distribution, Power Generation, and Heating, Ventilating and Air Conditioning (HVAC) Components for Commercial, Industrial, and Utility Installations*

TM 5-698-6, *Reliability Data Collection Manual for Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Facilities*

NON-GOVERNMENT

AIAG, *Potential Failure Mode and Effects Analysis – FMEA*

FMD-97, *Failure Mode/Mechanism Distribution-97*

IEEE 446 (3005), *Recommended Practice for Improving the Reliability of Emergency and Standby Power Systems*

IEEE 493-2007, *Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*

John Wiley and Sons, Inc., *Methods for Statistical Analysis of Reliability and Life Test Data*

North American Electric Reliability Corporation, *“Reliability Issues Steering Committee Report on Resilience,” November 8, 2018.*

[https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20Resilience%20Report Approved RISC Committee November 8 2018 Board Accepted.pdf](https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20Resilience%20Report%20Approved%20RISC%20Committee%20November%208%202018%20Board%20Accepted.pdf)

NPRD-95, *Non-electric Parts Reliability Data-95*

Reliability Analysis Center, *Fault Tree Analysis Application Guide, Report No. FTA, Reliability Analysis Center’*

Reliability Analysis Center, *Practical Application of Reliability Centered Maintenance Report No. RCM*

Reliability Analysis Center, *Practical Statistical Analysis for the Reliability Engineer (SOAR-2)*

Reliability Analysis Center, *Reliability Toolkit: Commercial Practices Edition*

Rome Air Development Center, *RADC-TR-77-287, A Redundancy Notebook, Rome Laboratory*

UNIFIED FACILITIES CRITERIA

<https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc>

UFC 1-200-01, *DoD Building Code*

UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*

UFC 3-540-01, *Engine-Driven Generator Systems for Prime and Standby Power Application*