TM 5-698-4

TECHNICAL MANUAL

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA) FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

HEADQUARTERS, DEPARTMENT OF THE ARMY
29 SEPTEMBER 2006

REPRODUCTION AUTHORIZATION/RESTRICTIONS

Technical Manual
No. 5-698-4

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, *29 September 2006*

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSES (FMECA) FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

CONTENTS

CONTENTS

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION TO FMECA

1-1. Purpose

The purpose of this manual is to guide facility managers through the Failure Mode, Effects and Criticality Analysis (FMECA) process, directing them how to apply this type of analysis to a command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facility. These facilities incorporate several redundant systems used to achieve extremely high availability that require specialized tools, which are described in this manual, to conduct an accurate analysis.

1-2. Scope

The information in this manual will provide the facility manager the necessary tools needed to conduct a realistic approach to establish a relative ranking of equipments' effects on the overall system. The methods used in this manual have been developed using existing concepts from various areas. These methods include an easy to use evaluation method to address redundancy's affect on failure rates and probability of occurrence. Because a C4ISR facility utilizes numerous redundant systems this method is very useful for conducting a FMECA of a C4ISR facility. Examples will be provided to illustrate how this can be accomplished by quantitative (with data) or qualitative means (without data). Although heating, ventilation and air conditioning (HVAC) systems are used as examples, the FMECA process can be applied to any electrical or mechanical system.

1-3. References

Appendix A contains a list of references used in this manual. Prescribed forms are also listed in appendix A. These five forms may be found on the Army Printing Directorate (APD) website http://www.apd.army.mil/.

1-4. 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 C4ISR facility

a. 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 in order 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

1-5. History

The FMECA was originally developed by the National Aeronautics and Space Administration (NASA) to improve and verify the reliability of space program hardware. The cancelled MIL-STD-785B, entitled *Reliability Program for System and Equipment Development and Production*, Task 204, *Failure Mode, Effects and Criticality Analysis* calls out the procedures for performing a FMECA on equipment or systems. The cancelled MIL-STD-1629A is the military standard that establishes requirements and procedures for performing a FMECA, to evaluate and document, by failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, maintainability and system performance. Each potential failure is ranked by the severity of its effect so that corrective actions may be taken to eliminate or control design risk. High risk items are those items whose failure would jeopardize the mission or endanger personnel. The techniques presented in this standard may be applied to any electrical or mechanical equipment or system. Although MIL-STD-1629A has been cancelled, its concepts should be applied during the development phases of all critical systems and equipment whether it is military, commercial or industrial systems/products.

1-6. 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.

a. Therefore, by 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 various other analyses such as a Fault Tree Analysis or a Reliability-Centered Maintenance (RCM) analysis.

b. The Fault Tree Analysis is a tool used for identifying multiple point failures; more than one condition to take place in order 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.

c. 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.

d. 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.

1-7. 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.

1-8. FMECA characteristics

The FMECA should be scheduled and completed concurrently as an integral part of the design process. Ideally this analysis should begin early in the conceptual phase of a design, when the design criteria, mission requirements and performance parameters are being developed. To be effective, the final design should reflect and incorporate the analysis results and recommendations. However, it is not uncommon to initiate a FMECA after the system is built in order to assess existing risks using this systematic approach. Figure 1-1 depicts how the FMECA process should coincide with a facility development process.

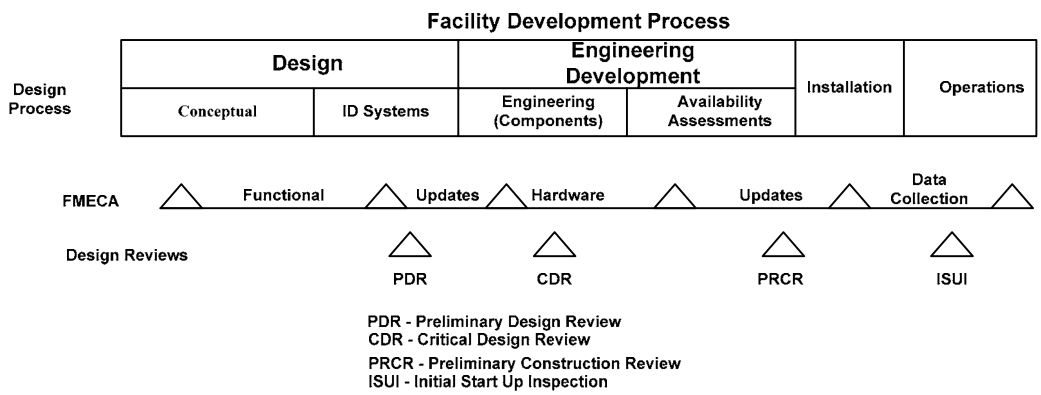


Figure 1-1. Facility development process

Since the FMECA is used to support maintainability, safety and logistics analyses, it is important to coordinate the analysis to prevent duplication of effort within the same program. The FMECA is an iterative process. As the design becomes mature, the FMECA must reflect the additional detail. When changes are made to the design, the FMECA must be performed on the redesigned sections. This ensures that the potential failure modes of the revised components will be addressed. The FMECA then becomes an important continuous improvement tool for making program decisions regarding trade-offs affecting design integrity.

CHAPTER 2
PRELIMINARY ITEMS REQUIRED

2-1. Requirements

In order to perform an accurate FMECA, the team must have some basic resources to get started.

a. These basic resources are:

(1) Schematics or drawings of the system.

(2) Bill of materials list (for hardware only)

(3) Block diagram which graphically shows the operation and interrelationships between components of the system defined in the schematics. (See figures 3-4 & 3-5)

(4) Knowledge of mission requirements

(5) An understanding of component, subsystem, & systems operations

b. Once the team has all of these resources 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.

2-2. 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.

CHAPTER 3
FMEA METHODOLOGY STEPS

3-1. Methodology - foundation

In order 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 Criticality Analysis. This section will discuss the process flow of a FMEA, see figure 3-1, 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.

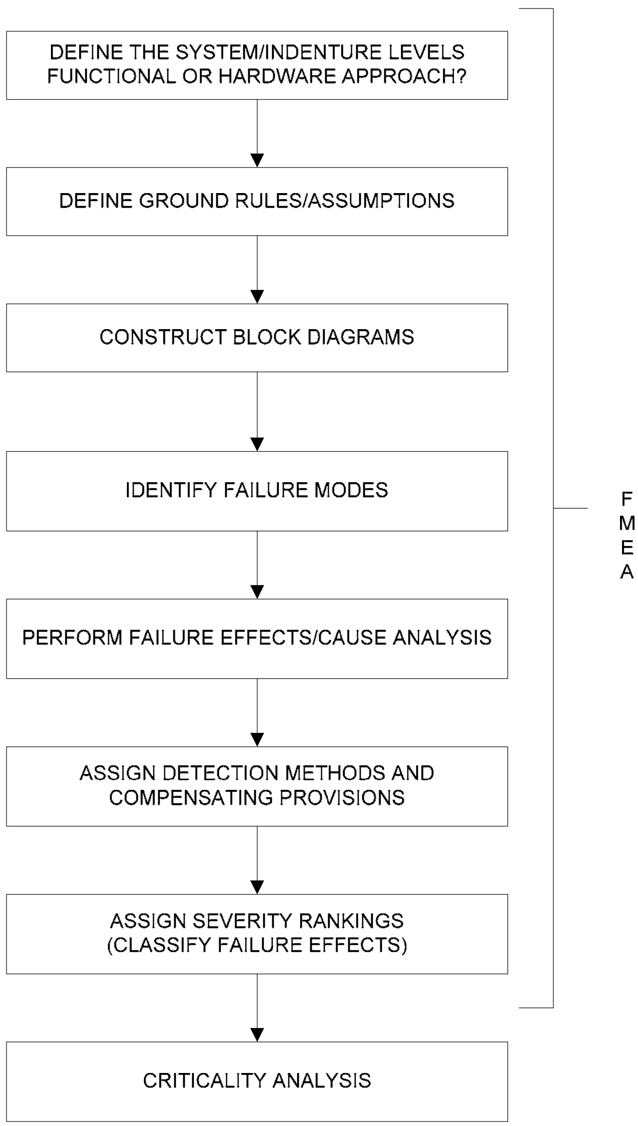


Figure 3-1. Typical FMECA flow

3-2. 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 ultimate 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.

a.. The system indenture levels must be identified. Figure 3-2 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 3-3.

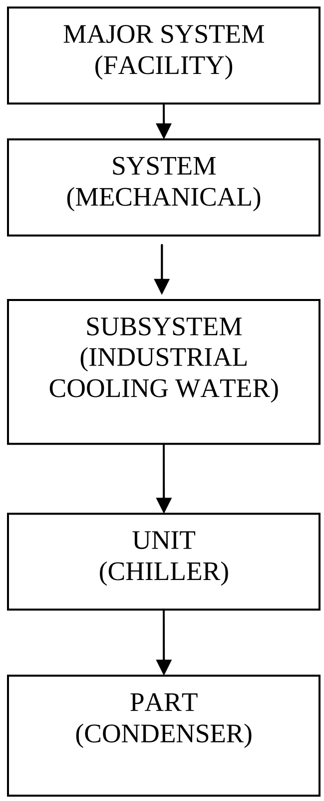


Figure 3-2. Functional method

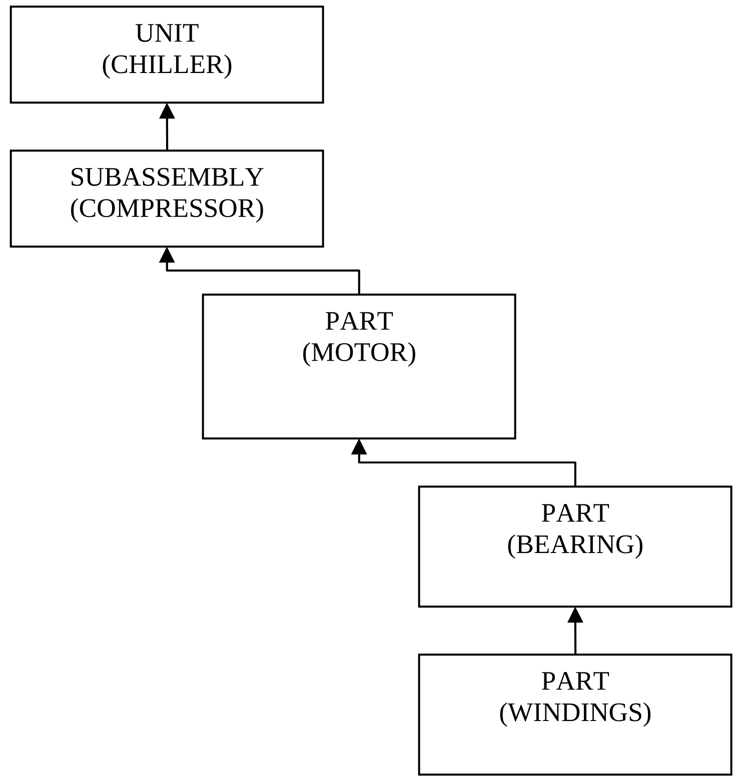


Figure 3-3. Hardware method

b. 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 in order 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 3-3. To perform a functional FMEA the analyst will need:

(1) System definition and functional breakdown

(2) Block diagrams of the system

(3) Theory of operation

(4) Ground rules and assumptions including mission requirements

(5) Software specifications

c. 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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.

i. 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:

(1) Complete theory or knowledge of the system

(2) Reliability block diagrams/functional block diagrams

(3) Schematics

(4) Bill of materials/parts list

(5) Definitions for indenture levels

(6) Ground rules and assumptions including mission requirements

j. 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 where as the hardware approach may identify a particular part that failed.

3-3. Ground rules and assumptions

To help the reader understand the FME(C)A 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 (see table 3-1 on page 3-15)

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. (supervisory control and data acquisition (SCADA), alarms, warnings)

3-4. Block diagrams

A functional and reliability block diagram 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.

a. 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.

b. 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 FMEA's.

c. The functional block diagram in figure 3-4 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.

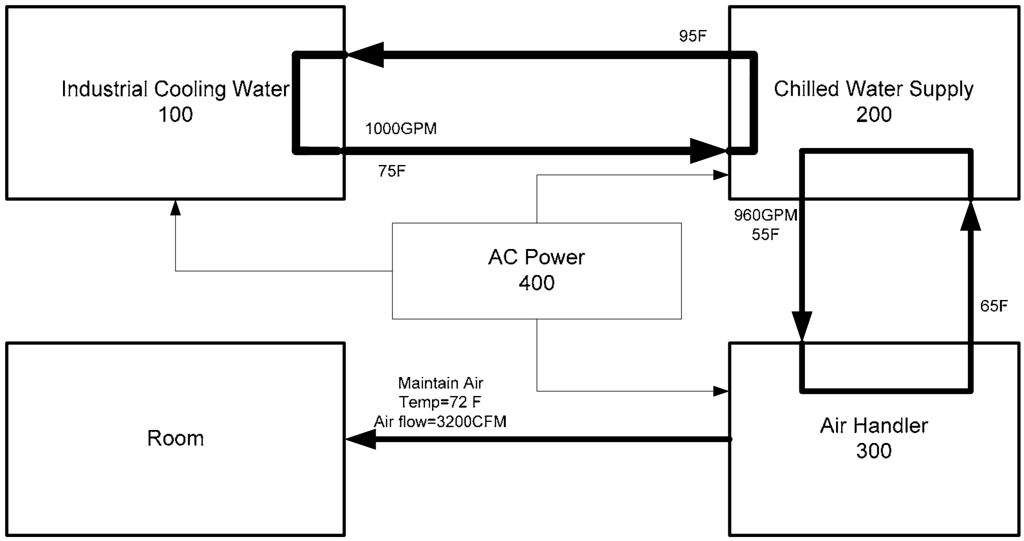


Figure 3-4. Functional block diagram of system

d. The next step is to provide a functional diagram within each sub-system indicating what types of components are required and their outputs. Figure 3-5 is an example of the same system but provides the basic components and their relationship within their system and other systems.

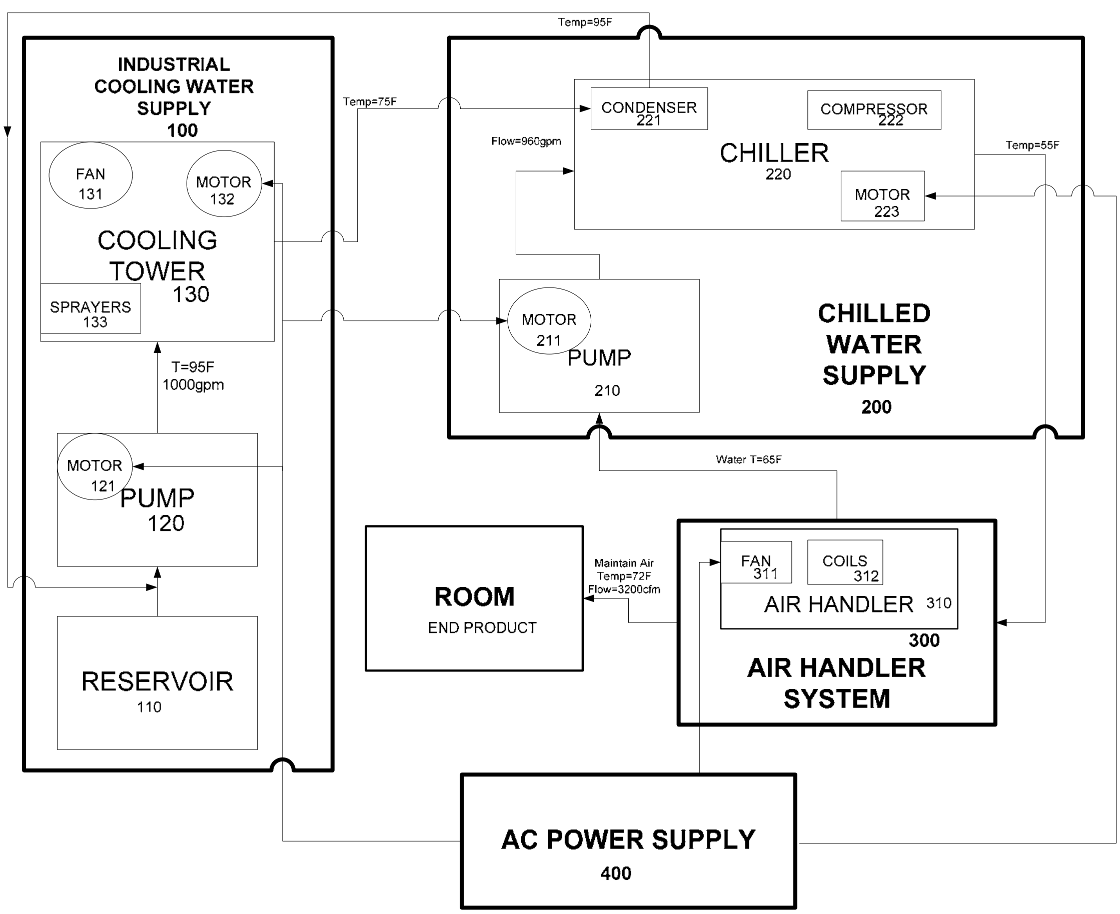


Figure 3-5. Functional block diagram of the sub-systems

e. 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. Additional information on the construction of functional block diagrams can be found in currently cancelled MIL-M-24100 entitled *Manual, Technical; Functionally Oriented Maintenance Manuals for Systems and Equipment*.

f. The reliability block diagram of the same system is shown in figure 3-6. It is used to illustrate the relationship of all the functions of a system or functional group. All of the redundant components should be shown. This diagram should also indicate how many of the redundant components are actually 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.

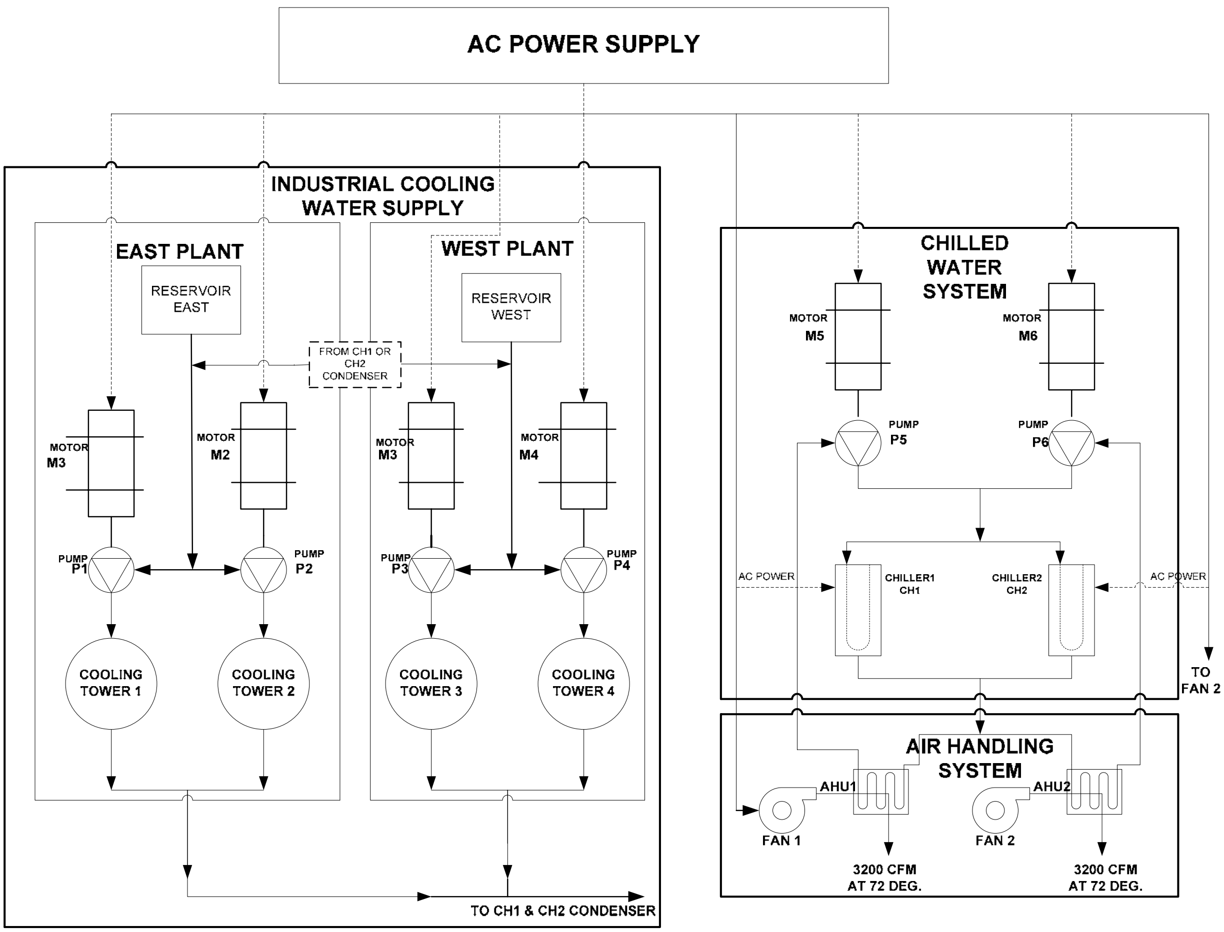


Figure 3-6. Reliability block diagram

g. 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.

h. 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.

i. 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.

j. The example shown provides symbols for components, but “blocks” clearly labeled are all that is necessary to be effective. Information on the construction of reliability block diagrams may be found in the currently cancelled MIL-STD-756 entitled *Reliability Prediction*. There are also numerous software programs available to aid in the construction of these diagrams. A simple search on the internet for “reliability block diagram” will provide some sources.

k. 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 (figure 3-7, DA Form 7610) . *Important:* The FMEA should be filled out in a column by column manner. *Never go across the sheet.* If you go across the sheet you will get confused. Start by filling in *all* of the item #'s 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.

l. The only exception to this rule is when it comes time to assign item #s 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 figure 3-8.

m. 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.

n. A sample FMEA worksheet for just the industrial cooling water is presented in figure 3-7 to indicate the flow of the process using DA Form 7610, Failure Mode and Effects Analysis..

3-5. 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 past history of failures in similar systems. All probable independent failure modes for each item should be identified.

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

(1) Failure to operate at the proper time
(2) Intermittent operation
(3) Failure to stop operating at the proper time
(4) Loss of output
(5) Degraded output or reduced operational capability

b. The example used in figure 3-10 is a functional approach of analyzing the upper system levels 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 figure 3-11.

c. 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? – Seal was not replaced during last pm.

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

d. As you can see, the root cause should be the "seal was cracked". By analyzing further you chase the cause "out of bounds". The analysts must use their judgments to decide how far to investigate root causes.

3-6. Failure effects analysis

A failure effects analysis is performed on each item of the reliability block diagram. 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.

a. Example failure effect levels are shown in Figure 3-9 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.

b. Example end or system level effects of item failures are also shown in Figure 3-9 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.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

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

SYSTEM: Mechanical System

PART NAME: Industrial Water Supply

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 1 of: 1

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNC-TIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPEN-SATING 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 APD V1.00

Figure 3-7. Example of DA Form 7610, FMEA worksheet flow (one column at a time)

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)
For use of this form, see TM 5-698-4; the proponent agency is USACE.

SYSTEM: Mechanical System
PART NAME: Industrial Water Supply
REFERENCE DRAWING:
MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819
SHEET: 1 of: 1
COMPILED BY: AAA
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 APD V1.00

Figure 3-8. Example of DA Form 7610, Functional FMEA system level

c. 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 on in the analysis.

d. Failures at the system level are those failures which hinder the performance or actual completion of the specified mission. Failures at each indenture level are 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 a maximum allowed operating temperature 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.

e. Figure 3-9 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.

3-7. 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 (supervisory control and data acquisition) 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 or not an indication will be evident to the operator or maintenance technician.

a. 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 a*bnormal* indication is an indication to the operator that the system has malfunctioned or failed. (alarm-chiller overheated)

(3) An i*ncorrect* indication is an erroneous indication to the operator that a malfunction has occurred when actually there is no fault. Conversely, an indication that the system is operating normally when, in fact, there is a failure.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

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

SYSTEM: Mechanical System

PART NAME: Industrial Water Supply

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 1 of: 1

COMPILED BY: AAA

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 sig-nificant				
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 system	Condenser in chiller will not function. Chiller will overheat	Air temp will rise above maximum allowed. Mission				

DA FORM 7610, AUG 2006 APD V1.00

Figure 3-9. Example of DA Form 7610, FMEA progression

b. 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 in order 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.

c. 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 over-heating, 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.

3-8. 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.

a. 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.

b. 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.

c. 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 in order to bring in the backup pump. If by chance the operator/technician inadvertently actuates the wrong valve there may be undesirable consequences as a result of their actions. This is a basic example but should be considered in the analysis on all failure modes.

3-9. Severity Ranking

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 criticality analysis to establish relative "severity" rankings of all potential failure modes.

a. 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.

b. A severity classification is assigned to each identified failure mode and each item analyzed in accordance with the categories in table 3-1.

Table 3-1. 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	Hazard	Potential Safety, Health or Environmental issue. Failure will occur **without** warning

c. 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* criticality analysis. These categories are used to "flag" the analysts to items with high severity.

d. Do *not* use this method to categorize severity in a qualitative analysis. The qualitative analysis requires an equal scale (i.e. 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 criticality analysis.

(1) Category I - Minor: A failure not serious enough to cause injury, property damage or system damage, but which will result in unscheduled maintenance or repair.

(2) Category 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.

(3) Category 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.

(4) Category IV - Catastrophic**:** A failure which may cause death or lack of ability to carry out mission without warning (power failure, over-heating).

e. A FMEA at the component level will have high severity rankings due to the fact that there is no redundancy at that level. At the system level, however, the severity may decrease due to the fact that 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.

f. 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.

g. An example of a completed functional FMEA of only the Industrial Cooling Water Supply is provided in figure 3-10. Hardware FMEA's on all of the systems are shown in figure 3-11. Notice that the functional FMEA did not include any redundancy as a consideration when assigning the effects.

3-10. Results of the 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 Criticality Analysis.

a. Once all of the information has been entered into the FMEA, the foundation for the Criticality Analysis has been established. The FMEA sheet will be referenced while creating the Criticality Analysis. Due to the amount of information on the FMEA, it is not feasible to include all of it on the CA. Consequently, a different sheet, which includes some of the information from the FMEA, will be used for the FMECA.

b. In this particular 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.

c. Once they are completed the steps discussed in the next section for the criticality analysis should be applied in order to complete the FMECA process.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

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

SYSTEM: Mechanical System

PART NAME: Industrial Water Supply

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE (YYYYMMDD): 20050819

SHEET: 1 of: 1

COMPILED BY: AAA

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 $$	Air temp may rise but not significant	temp sensor/water analysis	SCADA indicator	6	If drain pipe breaks the secondary containment will be filled
100.1		Provide water less than 75°F	Fan will not turn off	Too much cooling will take place	Chiller will be less efficient and use more energy	No effect to Air temp	Alarm temp sensor	SCADA indicator	2	
100.2		Provide water less than 1000GPM	Degraded Pump	pump will not be able to provide enough flow or pressure	Condenser not efficient, Chiller will use more energy $$	Air temp may rise but not sig-nificant	flow/pressure sensor	SCADA indicator	4	
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	10	Safety hazard, when pipe ruptures injury could occur.
100.4			blockage in pipe or pump failure	no water will be provided through 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 APD V1.00

Figure 3-10. Example of DA Form 7610, Completed FMEA (functional) for industrial water supply

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

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

SYSTEM: Mechanical System
PART NAME: HVAC System
REFERENCE DRAWING: C-20005-B
MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819
SHEET: 1 of: 3
COMPILED BY: AAA
APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS			DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
				LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				
110.0	Reservoir/contain 6000 gallons of water	Leak,	Crack in wall, Drain pipe 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 1000 gpm	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	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	Inspec-tion/water analysis	Redundant system	6	
130.1		Clogged sprayers	Untreated/ unfil-tered water	Water will not be cooled	Condenser will not be efficient	Room tempera-ture will rise slightly	Inspec-tion/water analysis	Redundant system	5	

DA FORM 7610, AUG 2006 APD V1.00

Figure 3-11. Example of DA Form 7610, Completed FMEA (hardware) for HVAC system

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

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

SYSTEM: Mechanical System — DATE *(YYYYMMDD)*: 20050819

PART NAME: HVAC System — SHEET: 2 of: 3

REFERENCE DRAWING: C-20005-B — COMPILED BY: AAA

MISSION: Provide Temperature Control to Room — APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS: LOCAL EFFECTS	FAILURE EFFECTS: NEXT HIGHER LEVEL	FAILURE EFFECTS: END EFFECTS	DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
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 chilled water supply at 960GPM	Degraded operation-produce water at a rate less than 960gpm	Impeller degraded, gasket leak, motor degraded	Pump cannot 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	refigerent 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	
220.1		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 — APD V1.00

Figure 3-11. Example of DA Form 7610, Completed FMEA (hardware) for HVAC system (cont'd)

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

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

SYSTEM: Mechanical System

PART NAME: HVAC System

REFERENCE DRAWING: C-20005-B

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 3 of: 3

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM	FAILURE EFFECTS: LOCAL EFFECTS	FAILURE EFFECTS: NEXT HIGHER LEVEL	FAILURE EFFECTS: END EFFECTS	DETECTION METHOD	COMPENSATING PROVISION	SEVERITY CLASS	REMARKS
310.0	Air Handler/ Maintain room temp of 72°F, 3200cfm	Maintain air temp higher than 72°F	Dirty coil	Air handler will run continuous.	Chiller will be required to drop water temp further	Minimal change in temperature	Temp sensor	Redundant air handler	4	
310.1		Provide airflow at a rate less than 3200cfm	reduced motor output, belt slippage, dirty intake filter	Airflow is decreased. Heat transfer will be decreased	Chiller will be required to drop water temp further	Temperature variations in room dependant on location.	Temp/flow sensor	Redundant air handler	3	
310.2		Produce no air flow	broken belt, motor failure, bearing seizure in fan, No AC power	Fan will not work. Air flow ceases	Room air will not be cooled	Temperature will rise above maximum allowed.	Temp/flow sensor	Redundant air handler	7	

DA FORM 7610, AUG 2006 APD V1.00

Figure 3-11.Example of DA Form 7610, Completed FMEA (hardware) for HVAC system (cont'd)

CHAPTER 4
FMECA METHODOLOGY

4-1. Methodology – moving into Criticality Analysis

The FMECA is composed of two separate analyses, the FMEA and the Criticality Analysis (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 Criticality Analysis 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 sections. Figure 4-1 shows the process for conducting a FMECA using quantitative and qualitative means.

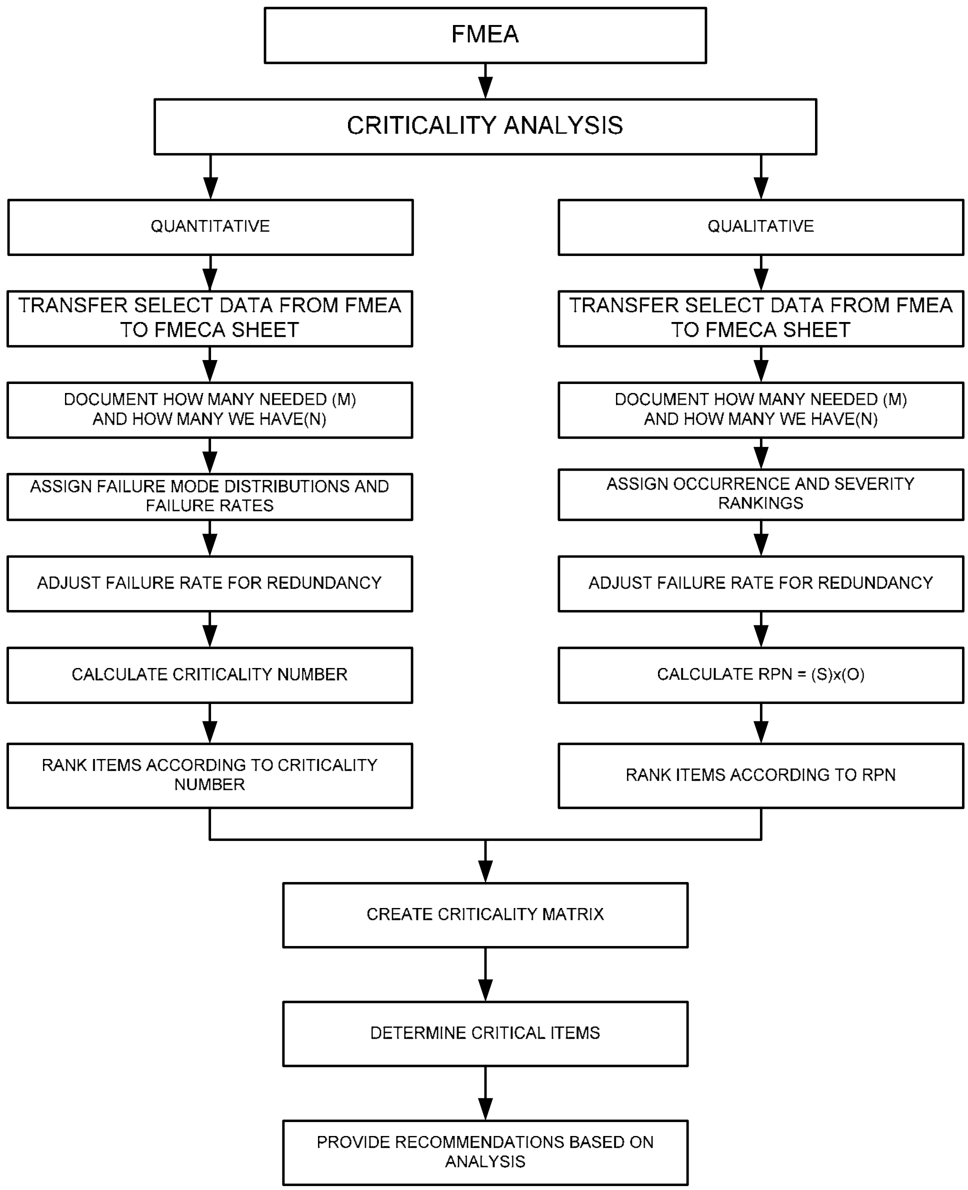


Figure 4-1. FMECA flow

4-2. Criticality Analysis

The Criticality Analysis (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.

a. The CA can be performed using either a quantitative or a qualitative approach. Figures 4-2 and 4-3 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 figure 4-2 when actual component data is available and use figure 4-3 when no actual component data or only generic component data is available.

b. Figure 4-4 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.

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

PART NAME: Industrial Water Supply

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE (YYYYMMDD): 20050819

SHEET: 1 of: 2

COMPILED BY: AAA

APPROVED BY: BBB

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

DA FORM 7611, AUG 2006 APD V1.00

Figure 4-2. Example of DA Form 7611, FMECA worksheet – quantitative

QUALTITATIVE 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

PART NAME: Industrial Water Supply

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 1 of: 1

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNC-TIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM					REMARKS AND/OR RECOMMENDED ACTIONS
					OCCUR	SEVER-ITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR	SEVER-ITY	RPN (O')X(S)	

DA FORM 7612, AUG 2006 APD V1.00

Figure 4-3. Example of DA Form 7612, FMECA worksheet – qualitative

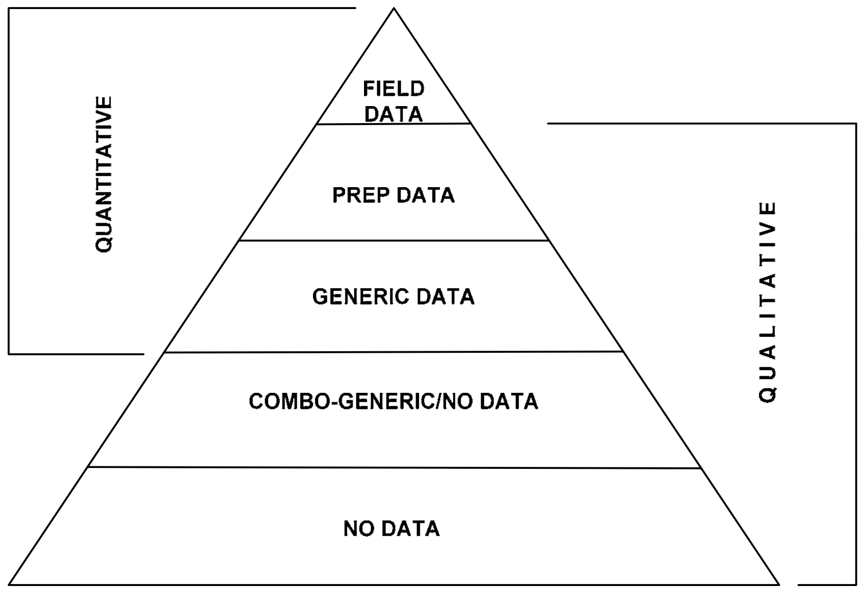


Figure 4-4. Data triangle

(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 fault tree analysis and a reliability centered maintenance (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.

4-3. Transfer select data from FMEA sheet

The information from the FMEA sheet that will be used in the FMECA worksheet will aid in developing the criticality analyses. Given the fact that not all of 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.

a. The major contributing factors for not including all of the information are space and clarity. All of the information on the FMEA can sometimes be difficult to read by its own not to mention if it is combined with both analyses on one document. 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 manual is just a guide and is meant to be flexible in order to achieve the objective of the analysis.

b. 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 figures 4-2 and 4-3.

c. The following categories will be transferred from the FMEA sheet:

(1) Item Number

(2) Item/Functional ID

(3) Failure Modes

(4) Failure Mechanisms

(5) Failure Effects (qualitative only due to space limitations)

(6) Severity Classification/Ranking

d. All other categories from the FMEA will be referenced during the criticality analysis.

4-4. 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 figure 4-2 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 C4ISR facility. The required amount 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 4-5. A description of each category and variable used in the CA is listed below.

a. 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 1. An example would be if the generator engine shuts down (failure mode), we can confidently state 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).

b. Alpha (α) is the probability, expressed as a decimal fraction, that the given part or item will fail in the identified mode. If all of 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 statistically derived and 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 4-1.

Table 4-1. Failure mode ratio (α)

Part Failure Modes	Failure Mode Ratio (α)
Blows too little air	0.55 or 55%
Blows too much air	0.05 or 5%
Blows no air	0.40 or 40%
The sum of the 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 in order to only consider the worst possible end effect as a result of a failure mode.

c. 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. These sources are mentioned in appendix B.

(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 4-5. When entering in the failure rate on the FMECA sheet, in parentheses you should identify that the failure rate is the single item component failure rate or the failure rate of the redundant system. The example at the end of this section 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.

d. 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:

$$\lambda_m = \alpha \lambda_p \qquad \text{(Equation 4-1)}$$

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

e. 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 in order to rank importance based on its failure rate. The equation used to calculate this number is as follows:

$$C_m = (\beta \alpha \lambda_p t) \qquad \text{(Equation 4-2)}$$

where:

C_m = Failure mode criticality number
β = Conditional probability of the current failure mode's failure effect
α = Failure mode ratio
λp = 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 4-4d. 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 (λp): 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 (No output) = (1 x .29 x 12.058 x 1)

C_m (No output) = 3.5 x 10^{-6}

C_m (Degraded) = (1 x .71 x 12.058 x 1)

C_m (Degraded) = 8.56 x 10^{-6}

f. 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 of 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:

$$C_r = \sum (C_m) \qquad \text{(Equation 4-3)}$$

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 (λp): 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 (Cr):

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

$$C_r = (1 \text{ x } .29 \text{ x } 12.058 \text{ x } 1) + (1 \text{ x } .71 \text{ x } 12.058 \text{ x } 1)$$

$$C_r = 12.058$$

4-5. 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 is 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).

a. 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.

$$\lambda_{(n-q)/n} = \frac{n!(\lambda)^{q+1}}{(n-q-1)!(\mu)^q}\text{, with repair} \qquad \text{(Equation 4-4)}$$

where:

n	=	number of active on line 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 (μ=1/MTTR; where MTTR is the mean time to repair (hour).

b. Therefore, if a system has five active units, each with a failure rate of 220 f/10^6 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?

c. Substituting the following values into the equation:

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

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

$$\lambda_{3/5} = \frac{5!(220x10^{-6})^3}{(5-2-1)!(1/3)^2} = 5.75x10^{-9} \text{ failures/hour}$$

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

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

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

$$\lambda_{(n-q)/n} = \frac{\lambda}{\sum_{i=n-q}^{n} \frac{1}{i}}, \text{ without repair} \qquad \text{(Equation 4-5)}$$

f. Using the same problem from above and substituting into this formula

$$\lambda_{3/5} = \frac{220x10^{-6}}{\left(\frac{1}{3}\right)+\left(\frac{1}{4}\right)+\left(\frac{1}{5}\right)} = \frac{220x10^{-6}}{\frac{47}{60}}$$

$$\lambda_{3/5} \approx 280x10^{-6} \text{ failures/hour}$$

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

g. A noticeable increase in failure rate due to the fact that the components are not repaired!

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

i. 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.

$$\lambda_{n/n+1} = \frac{n[n\lambda + (1-P)\mu]\lambda}{\mu + n(P+1)\lambda}, \text{ with repair} \qquad \text{(Equation 4-6)}$$

$$\lambda_{n/n+1} = \frac{n\lambda}{P+1}, \text{ without repair} \qquad \text{(Equation 4-7)}$$

where:

n	=	number of active on line 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 (μ=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)

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

$$\lambda_{1/2} = \frac{\lambda_A \lambda_B \left[(\mu_A + \mu_B) + (\lambda_A + \lambda_B)\right]}{(\mu_A)(\mu_B) + (\mu_A + \mu_B)(\lambda_A + \lambda_B)}, \text{ with repair} \qquad \text{(Equation 4-8)}$$

$$\lambda_{1/2} = \frac{\lambda_A{}^2 \lambda_B + \lambda_A \lambda_B{}^2}{\lambda_A{}^2 + \lambda_B{}^2 + \lambda_A \lambda_B}, \text{ without repair} \qquad \text{(Equation 4-9)}$$

k. These new failure rates (λ) should then be placed back in the equation, $Crc = \sum_{n=1}^{j} (\beta\alpha\lambda pt)n$, to calculate the new Criticality Number which accounts for redundancy.

l. If your particular situation is not addressed in the preceding formulas, 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.

m. 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.

4-6. 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 of 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 in order to decrease the negative impact on the mission.

a. Once it is determined that a qualitative approach will be used the Criticality worksheet that looks like figure 4-3 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 4-6g. Adjustments to occurrence rankings to compensate for redundant components within a typical C4ISR facility must be addressed as well and will be discussed in paragraph 4-7.

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. Figure 4-5 is an example of the quantitative FMECA worksheet 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
PART NAME: Industrial Water Supply
REFERENCE DRAWING:
MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819
SHEET: 1 of: 3
COMPILED BY: AAA
APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNC-TIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVER-ITY	REDUNDANCY		FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBAB-ILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	FAILURE MODE CRITICALITY NUMBER (C_M)	ITEM CRITICALITY NUMBER (ΣC_M)	REMARKS
					HAVE (N)	NEED (M)							
110.0	Reservoir/contain 6000 gallons of water	Leak	Crack in wall, Ruptured drain pipe	4	2	1	1.500x10-6 (single) NPRD-95 .0104x10-6 (redundant)	1	1	61,320	6.38 x10-4	6.38 x10-4	
120.0	Pump #1/ Transport industrial water at 1000GPM	Transport water at a rate below 1000GPM	impeller degraded, gasket leak, motor degraded	3	4	1	12.058x10-6 (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 APD V1.00

Figure 4-5. 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 NAME: Industrial Water Supply

SHEET: 2 of: 3

REFERENCE DRAWING:

COMPILED BY: AAA

MISSION: Provide Temperature Control to Room

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL 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_M)*	ITEM CRITICALITY NUMBER (ΣC_M)	REMARKS
					HAVE (N)	NEED (M)							
130.2		Fan failure	Motor winding open, No voltage to motor	3				1	.2	61,320	1.54x10-12	1.54x10-12	
210.0	Pump #5/ Transport chilled-water supply 960GPM	Degraded operation-produce water at less than 960GPM	impeller degraded, gasket leak, motor degraded	3	2	1	12.058x10-6 (single) NPRD-95 8.72x10-10 (redundant)	1	.35	61,320	3.00x10-13	8.58x10-13	
210.1		produce no water flow	broken coupling, suction line leak, motor inoperable	3				1	.65	61,320	5.58x10-13		
220.0	Chiller/ Remove heat(10°F) from chilled water	Degraded operation-remove less than 10°F	refrig. leak, degraded comp., tube leak, dirty coil	3	2	1	9.2791x10-6 (single) NPRD-95 1.72x10-10 (redundant)	1	.92	61,320	9.70 x10-6	9.70 x10-6	
220.1		remove no heat	compressor seizure, motor failure	4				1	.08	61,320	8.45 x10-6	8.45 x10-6	Expensive and time consuming to repair

DA FORM 7611, AUG 2006 APD V1.00

Figure 4-5. 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

PART NAME: Industrial Water Supply

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 3 of: 3

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	SEVERITY	REDUNDANCY HAVE (N)	REDUNDANCY NEED (M)	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	OPERATING TIME (t)	FAILURE MODE CRITICALITY NUMBER (C_M)	ITEM CRITICALITY NUMBER (ΣC_M)	REMARKS
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	1.34 x10-7	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	1.53 x10-7		
310.2		Provide no air flow	broken belt, motorfailure, fan bearing seizure, No AC power	3				1	.25	61,320	9.56 x10-8		

DA FORM 7611, AUG 2006 APD V1.00

Figure 4-5. Example of DA Form 7611, Quantitative FMECA with redundant components (cont'd)

b. 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. Adjust the failure rates for your particular application. Rates can be hours, days, cycles …etc.

c. Possible qualitative occurrence rankings (O) are shown in Table 4-2.

Table 4-2. 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 given volume/loads
4	1/1,000	Occasional failure rate. Similar to past design that has had 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

d. The severity ranking, as mentioned in paragraph 3-9, 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

e. The severity rankings (S) from table 3-1 are again shown here in table 4-3.

Table 4-3. 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 t facility function. Repair to failure can be accomplished during trouble call.
3	Low	Minor disruption t 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	Hazard	Potential Safety, Health or Environmental issue. Failure will occur **without** warning

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

$$RPN = (S) \times (O) \qquad \text{(Equation 4-10)}$$

g. 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 in order 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.*

h. 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.

$$RPN = (S) \times (O) \times (D) \qquad \text{(Equation 4-11)}$$

i. Where *detection* is ranked (1-10), shown in table 4-4, in a similar fashion as *severity* and *occurrence*;

Table 4-4. 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

j. This variable 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.

k. 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.

l. In addition, a C4ISR facility has a different "product" than the auto industry. The auto industry is producing parts and the C4ISR facility is 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 C4ISR facility. The system's goal in a C4ISR facility is to be available. Just because you have detected a failure does not necessarily mean that the end level effect is prevented. However, it may minimize the downtime, thus increasing availability. This would be taken into consideration when you assign severity. For that reason, even though detection is considered in classifying severity, it does not hold the same relative importance.

4-7. 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 we deal with criticality rankings for like components within a single redundant system.

a. For example, consider an occurrence ranking of 9 for a chilled water supply pump (see figure 4-6). 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 can we subjectively, but meaningfully, rank like redundant components with the same system function?"

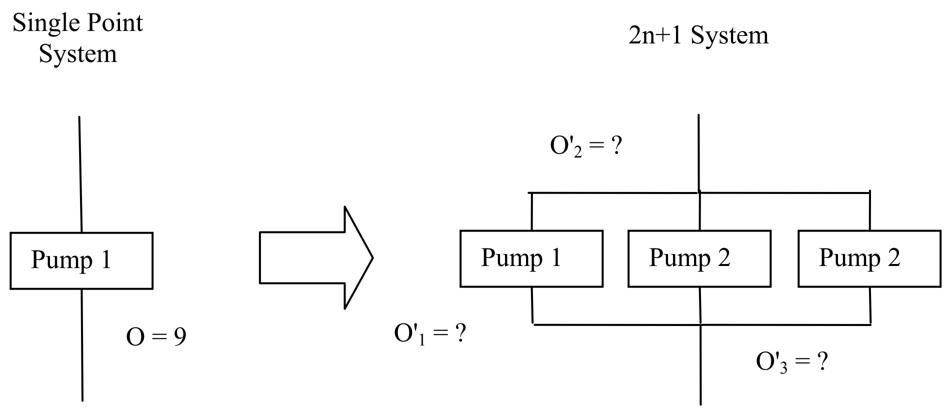


Figure 4-6. Single point system vs. redundant system

b. 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.

c. 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 paragraph (4-5a equation 4-4).

d. 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.

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

$$O' = O \times \frac{M}{N-1} \qquad \text{(Equation 4-12)}$$

where:

O = Occurrence level for loss of subsystem / system function
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

f. Note that using this formula with only 1 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:

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

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

g. Likewise, if only 2 items are needed and 4 are available and the occurrence is 9:

$$M=2$$
$$N=4$$
$$O' = O \times \frac{2}{4-1}$$
$$O' = 9 \times \frac{2}{3}$$
$$O' = 6$$

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

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

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

i. When sufficient failure rate data is available it is always recommended that quantitative criticality analysis 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 4-12 can be incorporated to quickly emulate the redundancy/occurrence relationship as part of a qualitative analysis.

j. This "combined" method allows for an analysis to be conducted using the qualitative (subjective) approach and also 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.

k. 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:

$$\text{RPN} = (O') \times (S)$$

l. This adjusted RPN will then be used in the final ranking process. Figure 4-7 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.*

QUALTITATIVE 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

PART NAME: HVAC System

REFERENCE DRAWING:

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 1 of: 3

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNC-TIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM					REMARKS AND/OR RECOMMENDED ACTIONS
					OCCUR	SEVER-ITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR	SEVER-ITY	RPN (O')X(S)	
110.0	Reservoir/contain 6000 gallons of water	leak	Crack in wall, Drain pipe breaks	No immediate effect. The surrounding area will be saturated.	2	6	12	2	1	2	4	8	If drain pipe breaks, secondary contain-ment will be filled
120.0	Pump #1/ Transport Industrial water supply at 1000gpm	Transport water at a rate below 1000 gpm	Impeller degradation, 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 APD V1.00

Figure 4-7. Example of DA Form 7612, FMECA worksheet using qualitative rankings

QUALTITATIVE 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 NAME: HVAC System
SHEET: 2 of: 3

REFERENCE DRAWING:
COMPILED BY: AAA

MISSION: Provide Temperature Control to Room
APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM					REMARKS AND/OR RECOMMENDED ACTIONS
					OCCUR	SEVER-ITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR	SEVER-ITY	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 chilled water supply at 960gpm	Degraded operation-pro duce water at a 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-Missi on 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 APD V1.00

Figure 4-7. Example of DA Form 7612, FMECA worksheet using qualitative rankings (cont'd)

QUALTITATIVE 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
PART NAME: HVAC System
REFERENCE DRAWING:
MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819
SHEET: 3 of: 3
COMPILED BY: AAA
APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNC-TIONAL ID	POTENTIONAL FAILURE MODES	FAILURE MECHANISM (CAUSE)	FAILURE EFFECTS	SINGLE COMPONENT			REDUNDANT SYSTEM					REMARKS AND/OR RECOMMENDED ACTIONS
					OCCUR	SEVER-ITY	RPN (O)X(S)	HAVE (N)	NEED (M)	OCCUR	SEVER-ITY	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 dependant 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 APD V1.00

Figure 4-7. Example of DA Form 7612, FMECA worksheet using qualitative rankings (cont'd)

CHAPTER 5
CRITICALITY RANKING – QUANTITATIVE AND QUALITATIVE

5-1. Criticality ranking

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.

a. 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 figure 5-1 for an example *failure mode criticality ranking* using DA Form 7613. Figure 5-2 using DA Form 7614 is another type of ranking that only ranks the *item criticality number* (equation 4-3) that was discussed in paragraph 4-4f. This is called an i*tem 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.

b. The *failure mode criticality ranking*, i*tem 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. This is why it is highly suggested that this ranking should be complimented by developing a *criticality matrix*. The matrix is explained in the next section.

c. 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 of 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 fault tree analysis, thereby enabling improvements in the design.

5-2. 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 in order to prioritize components.

a. 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.

b. The matrix is constructed by inserting the assigned Item #, 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 5-3 is representative of the HVAC system FMECA example in figure 4-5. If there is not sufficient space available in the matrix to paste the Item # 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.

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 NAME: HVAC System | SHEET: 1 of: 3

REFERENCE DRAWING: C-20005-B | COMPILED BY: AAA

MISSION: Provide Temperature Control to Room | APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL 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_m)*
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 APD V1.00

Figure 5-1. Example of DA Form 7613, Failure mode criticality ranking

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 NAME: HVAC System | SHEET: 2 of: 3
REFERENCE DRAWING: C-20005-B | COMPILED BY: AAA
MISSION: Provide Temperature Control to Room | APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL 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_m)*
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 at a rate below 1000 gpm	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.	Scaling (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 APD V1.00

Figure 5-1. Example of DA Form 7613, Failure mode criticality ranking (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 NAME: HVAC System | SHEET: 3 of: 3

REFERENCE DRAWING: C-20005-B | COMPILED BY: AAA

MISSION: Provide Temperature Control to Room | APPROVED BY: BBB

ITEM NUMBER	ITEM/FUNCTIONAL ID	POTENTIONAL 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_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 (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.	Scaling (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 APD V1.00

Figure 5-1. Example of DA Form 7613, Failure mode criticality ranking (cont'd)

ITEM CRITICALITY RANKING (QUANTITATIVE)

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

SYSTEM: Mechanical System

PART NAME: HVAC System

REFERENCE DRAWING: C-20005-B

MISSION: Provide Temperature Control to Room

DATE (YYYYMMDD): 20050819

SHEET: 1 of: 2

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM / FUNCTION	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	OPERATING TIME (t)	ITEM CRITICALITY NUMBER (ΣC_m)
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	6.38 x10-4

DA FORM 7614, AUG 2006 APD V1.00

Figure 5-2. Example of DA Form 7614, Item criticality ranking

ITEM CRITICALITY RANKING (QUANTITATIVE)

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

SYSTEM: Mechanical System

PART NAME: HVAC System

REFERENCE DRAWING: C-20005-B

MISSION: Provide Temperature Control to Room

DATE *(YYYYMMDD)*: 20050819

SHEET: 2 of: 2

COMPILED BY: AAA

APPROVED BY: BBB

ITEM NUMBER	ITEM / FUNCTION	SEVERITY	FAILURE RATE λ_p (SOURCE)	FAILURE EFFECT PROBABILITY (β)	OPERATING TIME (t)	ITEM CRITICALITY NUMBER (ΣC_M)
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

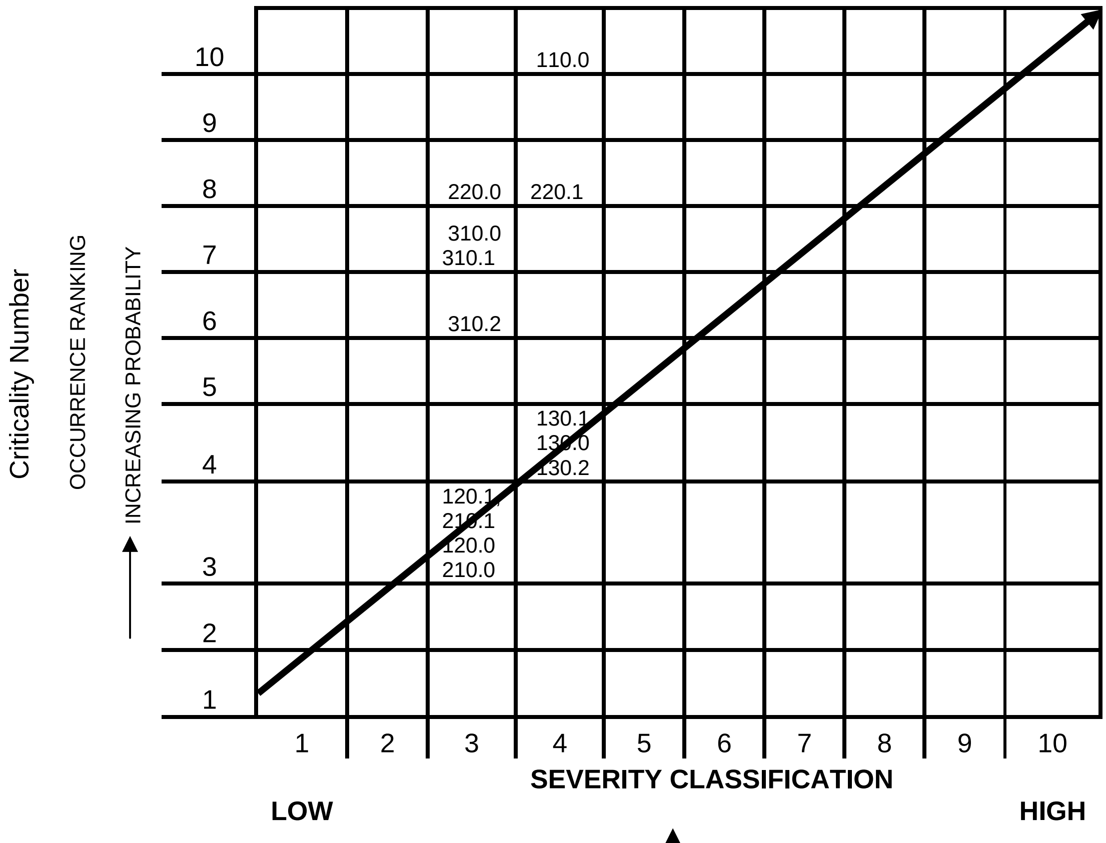
DA FORM 7614, AUG 2006

APD V1.00

Figure 5-2. Example of DA Form 7614, Item criticality ranking (cont'd)

c. Item #'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 (i.e., design in redundancy) is an alternative approach. As you move 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.

d. 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 in order to minimize the downtime of the system



Item #	Failure Mode	Modal Criticality Number
110.0	leak	$6.38x10^{-4}$
120.0	Transport water at a rate below 1000 gpm	$3.00x10^{-13}$
120.1	produce no water flow	$5.58x10^{-13}$
130.0	Scaling(deposits) on media	$2.87x10^{-12}$
130.1	Clogged sprayers	$3.51x10^{-12}$
130.2	Fan failure	$1.54x10^{-12}$
210.0	Degraded operation-produce water at a rate less than 960gpm	$3.00x10^{-13}$
210.1	produce no water flow	$5.58x10^{-13}$
220.0	Degraded operation-remove less than 10°F	$9.70x10^{-6}$
220.1	remove no heat	$8.45x10^{-6}$
310.0	Maintain air at a temp higher than 72°F	$1.34x10^{-7}$
310.1	Provide airflow at a rate less than 3200cfm	$1.53x10^{-7}$
310.2	Provide no air flow	$9.56x10^{-8}$

Figure 5-3. Criticality matrix

CHAPTER 6
RESULTS OF FMECA

6-1. 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 Criticality Analysis.

a. 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.

b. Recommendations cited must be fed back into the design process as early as possible in order 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.

6-2. 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 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.

a. Item #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.

b. Item #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.

c. Item numbers 310.0, 310.1, & 310.2 are all associated with the air handler system. #310.0 and #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 semi-annually.

d. 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 chemical treatment should eliminate or lower the possibilities of these failures occurring. Filtering the water 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 in order to quickly respond to a spontaneous failure in these locations.

e. 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 due to the fact that 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 semi-annual 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.

CHAPTER 7
CONCLUSIONS

7-1. 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.

a. 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.

b. 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.

7-2. Results

a. 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 Fault Tree Analysis (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.

b. In conclusion 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.

c. 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 C4ISR facility.

APPENDIX A

REFERENCES

Required Publications

Government Publications

Department of Defense

MIL-M-24100 (inactive), *Manual, Technical; Functionally Oriented Maintenance Manuals for Systems and Equipment*. (Cited in paragraph 3-4e)

MIL-STD-756 (cancelled), *Reliability Prediction* (Cited in paragraph 3-4j)

MIL-STD-785B (cancelled), *Reliability Program for System and Equipment Development and Production*, 15 September 1980. (Cited in paragraph 1-5)

MIL-STD-1629A (cancelled), *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* 24 November 1980. (Cited in paragraph 1-5)

National Aeronautical Space Agency

NASA's Reliability Centered Maintenance Guide for Facilities and Collateral Equipment, February 2000. (Cited in paragraph 1-6d(3))

Non-Government Publications

Automotive Industry Action Group (AIAG), *Potential Failure Mode and Effects Analysis – FMEA*, second edition, February 1995. (Cited in paragraph 4-6h)

Failure Mode/Mechanism Distributions-97, FMD-97, Reliability Analysis Center & Rome Laboratory, Rome, NY, 13440. (Cited in paragraph 4-4e(2)

Ned H. Criscimagna, *Practical Application of Reliability Centered Maintenance*, Report No. RCM, Reliability Analysis Center, 201 Mill Street, Rome, NY, 2001. (Cited in paragraph 1-6d(1))

Non-electric Parts Reliability Data-95, NPRD-95, Reliability Analysis Center, 201 Mill Street, Rome, NY, 2001. (Cited in paragraph 4-4e(2))

David Mahar, James W. Wilbur, *Fault Tree Analysis Application Guide,* Report No. FTA, Reliability Analysis Center, 201 Mill St., Rome, NY: 1990. (Cited in paragraph 1-6d(2))

Reliability Toolkit: Commercial Practices Edition, Reliability Analysis Center & Rome Laboratory, Rome, NY, 13440, pg 161. (Cited in paragraph 4-5)

Rome Air Development Center, RADC-TR-77-287, *A Redundancy Notebook*, Rome Laboratory, 1977. (Cited in paragraph 4-5l)

Related Publications

Government Publications

Department of Defense

MIL-STD-2070, *Procedures for Performing a Failure Mode, Effects & Criticality Analysis for Aeronautical Equipment*, 12 June 1977

Non-Government Publications

Borgovini, Robert; Pemberton, Stephen; Rossi, Michael, *Failure Mode, Effects and Criticality Analysis (FMECA)*, Report No. CRTA-FMECA, Reliability Analysis Center, 201 Mill Street, Rome, NY: April 1993.

Chopra, P.S., Wolosewicz, R. M., *Application of Reliability, Maintainability, and Availability Engineering to Solar Heating and Cooling Systems*, Proceedings of the Annual Reliability and Maintainability Symposium, 22-24 January 1980, pp. 248-253.

Collett, R.E., P.W. Bachant., *Integration of BIT Effectiveness with FMECA*, Proceedings of the Annual Reliability and Maintainability Symposium, 1984, pp. 300-305.

Himanen, R., *Failure Mode and Effect Analysis by Matrix Method in the Availability Analysis*, Proceedings of the 10th Annual Engineering Conference on Reliability, Availability, and Maintainability for the Electric Power Industry, 1983, pp. 189-194.

IEEE Std 352-1975/ANSI N411.4 1976, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems.*

Reliability, Maintainability, Supportability (RMS) Committee, *Failure Modes Effects and Criticality Analysis (FMECA), Reliability, Maintainability and Supportability Guidebook*, SAE G-11, Published by the Society of Automotive Engineers (SAE), Inc., 400 Commonwealth Drive, Warrendale, Pennsylvania: 1990. pp. 139-147.

Prescribed Forms

The following forms are printed in the back of this manual and are also available on the Army Electronic Library (AEL) CD-ROM and the USAPA Web site (www.usapa.army.mil)

DA Form 7610
Failure Modes and Effects Analysis (FMEA)
(Cited in paragraph 3-4n)

DA Form 7611
Quantitative Failure Modes Effects and Criticality Analysis (FMECA)
(Cited in paragraph 4-2a)

DA Form 7612
Qualitative Failure Modes Effects and Criticality Analysis (FMECA)
(Cited in paragraph 4-2a)

DA Form 7613
Failure Mode Criticality Ranking (Quantitative)
(Cited in paragraph 5-1a)

DA Form 7614
Item Criticality Ranking (Quantitative)
(Cited in paragraph 5-1a)

APPENDIX B

FAILURE MODE DISTRIBUTION SOURCES

Component failure mode distribution information is available from a variety of sources. Many FMECA's are accomplished with failure mode distributions based on a compilation of in-house failure analysis from actual field failure returns. This type of information is typically a better indicator of field performance than the generic data found in published sources. Most often, data specific to an exact part type or exact part number item can not be obtained. In these cases, published literature should be used as sources for generic failure mode distribution data. Some are listed here:

William Crowell, William Denson, Paul Jaworski and David Mahar. Failure Mode/Mechanism Distributions 1997, Report No. FMD-97.

Reliability Analysis Center, 201 Mill St., Rome, NY: 1997.

Gubbins, L.J. Study of Part Failure Modes, Report No. RADC-TR-64-377, Rome Air Development Center, Griffiss AFB, NY 13441: 1964.

William Denson, Greg Chandler, William Crowell, Amy Clark and Paul Jaworski. Nonelectronic Parts Reliability Data 1995, Report No. NPRD-95, Reliability Analysis Center, 201 Mill St., Rome, NY: 1995.

PREP (Power Reliability Enhancement Program) Data., Alion Science and Technology, WSTIAC (Weapons System Technology Information Analysis Center), 201 Mill St., Rome, NY: 2005.

GLOSSARY

-A-

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).

-B-

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.

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.

-C-

COMPENSATING PROVISION: Actions available or that can be taken to negate or reduce the effect of a failure on a system.

CORRECTIVE ACTION: A documented design, process or procedure change used to eliminate the cause of a failure or design deficiency.

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.

-D-

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.

-E-

END EFFECT: The consequence a failure mode has upon the operation, function or status at the highest indenture level.

-F-

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 a failure mode has upon the operation, function or status of a system or equipment.

FAILURE MODE: The way in which a failure is observed, describes the way the failure occurs, and its impact on equipment operation.

FAILURE RATE: The mean (arithmetic average, also known as the forced outage rate) is the number of failures of a component and/or system per unit exposure time. The most common unit in reliability analyses is hours (h) or years (y). Therefore, the failure rate is expressed in failures per hour (f/h) or failures per year (f/y)

FAULT ISOLATION: The process of determining the location of a fault to the indenture level necessary to affect repair.

-I-

INDENTURE LEVELS: The levels which identify or describe the relative complexity of an assembly or function.

ITEM CRITICALITY NUMBER (Cr): A relative measure of consequence of an item failure and its frequency of occurrence. This factor is not applicable to a qualitative analysis.

-L-

LOCAL EFFECT: The consequence a failure mode has on the operation, function or status of the specific item being analyzed.

-M-

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.

-N-

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.

-Q-

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.

-R-

REDUNDANCY: The existence of more than one means for accomplishing a given function.

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) x (O).

-S-

SECONDARY EFFECTS: The results or consequences indirectly caused by the interaction of a damage mode with a system, subsystem or component of the system.

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.

SINGLE POINT FAILURE: The failure of an item which can result in the failure of the system and is not compensated for by redundancy or alternative operational procedure.

The proponent agency of this publication is the Chief of Engineers, United States Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQUSACE, (ATTN: CEMP-OS-P), Washington, DC 20314-1000.

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

Distribution:

To be distributed in accordance with Initial Distribution Number (IDN) 344816, requirements for non-equipment TM 5-698-4.

PIN: 083559-000