Attachment 0036
FMECA Requirements

01 JUN 2014

DRAFT

Distribution Statement A – Approved for Public Release; distribution unlimited

DRAFT

FMECA Requirements for the JLTV Program

April 21

2014

The failure mode, effects, and criticality analysis (FMECA) is an essential function in design from concept through development and outward through sustainment of the weapons platform.

1. Objective

The failure mode, effects, and criticality analysis (FMECA) is an essential function in design from concept through development and outward through sustainment of the weapons platform. To be effective, the FMECA must be iterative to correspond with the nature of the design process itself. The extent of effort and sophistication of approach used in the FMECA will be dependent upon the nature and requirements of the individual acquisition program. This makes it necessary to tailor the requirements for an FMECA to each individual program. Tailoring requires that, regardless of the degree of sophistication, the FMECA must contribute meaningfully to program decision. A properly performed FMECA is invaluable to those who are responsible for making program decisions regarding the feasibility and adequacy of a design approach. The usefulness of the FMECA as a design tool and in the decision making process is dependent upon the effectiveness with which problem information is communicated for early design attention. While the objective of an FMECA is to identify all modes of failure within a system design, its first purpose is the early identification of all catastrophic and critical failure possibilities so they can be eliminated or minimized through design correction at the earliest possible time. Therefore, the FMECA should be initiated as soon as design information is available at the higher system levels and extended to the lower levels as more information becomes available on the items in question. Although the FMECA is an essential reliability task, it also provides vital information for other purposes. The use of the FMECA is called for in maintainability, safety analysis, survivability and vulnerability, logistics support analysis, maintenance plan analysis, and for failure detection and isolation subsystem design. This coincident use must be a consideration in planning the FMECA effort to prevent the proliferation of requirements and the duplication of efforts within the same contractual program.

DRAFT

2. Referenced Documents

- **MIL-HDBK-505**
  Definitions of Item Levels, Item Exchangeability, Models, and Related Terms
- **MIL-HDBK-470**
  Designing and Developing Maintainable Products and Systems
- **MIL-STD-882E**
  System Safety
- **MIL-HDBK-502A**
  Product Support Analysis
- **GEIA-STD-0009**
  Reliability Program Standard for Systems Design, Development, and Manufacturing
- **GEIA-STD-0007**
  Logistics Product Data

3. DEFINITIONS

3.1 Terms. The definitions of terms used herein are in accordance with the definitions in MIL-HDBK-505, MIL-HDBK-470, MIL-STD-882E, MIL-HDBK-502A, GEIA-STD-0009, and GEIA-STD-0007 with the exception and addition of the following:

3.1.1 Contractor. A private sector enterprise engaged to provide services or products within agreed limits specified by a procuring activity. As used in this standard, the term “Contractor” includes certain government operated activities developing or producing military systems and equipment.

3.1.2 Corrective action. A documented design, process, procedure, or materials change implemented and validated to correct the cause of failure or design deficiency.

3.1.3 Compensating provision. Actions that are available or can be taken by an operator to negate or mitigate the effect of a failure on a system.

3.1.4 Criticality. A relative measure of the consequences of a failure mode and its frequency of occurrences.

3.1.5 Criticality analysis (CA). A procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

3.1.6 Severity. The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage, or system damage that could ultimately occur.

3.1.7 Detection mechanism. The means or method by which a failure can be discovered by an operator under normal system operation or can be discovered by the maintenance crew by some diagnostic action.

3.1.8 Environment. The conditions, circumstances, influences, stresses and combinations thereof, surrounding and affecting systems or equipment during storage, handling, transportation, testing, installation, and use in standby status and mission operation.

3.1.9 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 initiate the physical process by which deterioration proceeds to failure.

3.1.10 Failure effect. The consequence(s) a failure mode has on the operation, function, or status of an item. Failure effects are classified as local effect, next higher level, and end effect.

3.1.10.1 Local effect. The consequence(s) a failure mode has on the operation, function, or status of the specific item being analyzed.

3.1.10.2 Next higher level effect. The consequence(s) a failure mode has on the operation, functions, or status of the items in the next higher indenture level above the indenture level under consideration.

3. 1.10.3 End effect. The consequence(s) a failure mode has on the operation, function, or status of the highest indenture level.

3.1.11 Failure mode. The manner by which a failure is observed.
Generally describes the way the failure occurs and its impact on equipment operation.

3.1.12 Failure mode and effects analysis (FMEA). A procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity.

3.1.13 FMECA-Maintainability Information Analysis. A procedure by which each potential failure is analyzed to determined how the failure is detected and the actions to be taken to repair the failure.

3.1.14 Indenture levels. The item levels which identify or describe the relative complexity of assembly or function. The levels progress from the more complex (system) to the simpler (part) divisions.

3.1.14.1 Initial indenture level. The level of the total, overall item which is the subject of the FMECA.

3.1.14.2 Other indenture levels. The succeeding indenture levels (second, third, fourth, etc.) which represent an orderly progression to the simpler division of the item.

3.1.15 Interfaces. The systems, external to the system being analyzed, which provide a common boundary or service and are necessary for the system to perform its mission in an un-degraded mode; for example, systems that supply power, cooling, heating, air services, or input signals.

DRAFT

3.1.16 Logistics Product Data (LPD). The data and results of FMECA or other Logistics Support Analysis (LSA) required for the planning and execution of Integrated Product Support of a system or systems acquired by the US Government.

3.1.17 Single failure point. The failure of an item which would result in failure of the system and is not compensated for by redundancy or alternative operational procedure.

3.1.18 Undetectable (Hidden) failure. A postulated failure mode in the FMEA for which there is no failure detection method by which the operator is made aware of the failure during normal operations.

4. GENERAL REQUIREMENTS

4.1 General. The failure mode, effects, and criticality analysis (FMECA) shall be planned and performed in accordance with the general requirements of this document and the task(s) specified by the Government.

4.2 Implementation. The FMECA is an analysis procedure which documents all probable failures in a system within specified ground rules, determines by failure mode analysis the effect of each failure on system operation, identifies single failure points, and ranks each failure according to a severity classification of failure effect. This procedure is the result of two steps which, when combined, provide the FMECA. These two steps are:

a. Failure mode and effects analysis (FMEA).

b. Criticality analysis (CA).

4.3 FMECA planning. Planning the FMECA work involves the Contractor's procedures for implementing the specified requirements of this document, updating the FMECA to reflect design changes, and the use of the analysis results to provide design guidance. Worksheet formats, ground rules, analysis assumptions, identification of the lowest indenture level of analysis, coding system description, failure definitions, and the method for documenting the FMECA LPD IAW GEIA-STD-0007 and delivering these results per the Government's requirements shall be considered in the FMECA planning.

4.3.1 Ground rules and assumptions. The Contractor shall develop ground rules and analysis assumptions. The ground rules shall identify the FMECA approach (e.g. , hardware, functional or combination), the lowest indenture level to be analyzed, and include general statements of what constitutes a failure of the item in terms of performance criteria and allowable limits. Every effort should be made to identify and record all ground rules and analysis assumptions prior to initiation of the analysis; however, ground rules and analysis assumptions may be added for any item if requirements change.

4.3.2 Indenture level. The indenture level applies to the system hardware or functional level at which failures are postulated. Unless otherwise specified, the Contractor shall establish the lowest indenture level of analysis using the following guidelines:

a. The lowest level required to assure complete inputs for each LSA candidate. At a minimum, all items with a "P" or "X" in the first position of its Source, Maintenance, and Recovery (SMR) code shall be analyzed and documented.

b. The lowest indenture level at which items are assigned a catastrophic (Category I) or critical (Category II) severity classification category (see 4.4.3).

c. The specified or intended maintenance and repair level for items assigned a marginal (Category III) or minor (Category IV) severity classification category (see 4.4.3).

4.3.3 Coding system. For consistent identification of system functions and equipment, and for tracking associated failure modes, the Contractor shall adhere to a coding system based upon the hardware breakdown structure and

DRAFT

LCN coding assigned to each part, sub-system, next-higher assembly, etc. as established within the required LPD information management system.

4.3.4 Failure definition. The Contractor shall develop general statements of what constitute a failure of the item in terms of performance parameters and allowable limits for each specified output. The Contractor's general statements shall not conflict with any failure definitions specified by the procuring activity.

4.3.5 Coordination of effort. Consideration shall be given to the requirements to perform and use the FMECA in support of a reliability program in accordance with IAW GEIA-STD-0009, maintainability program IAW MIL-HDBK-470, safety program IAW MIL-STD-882E, logistics support analysis IAW with MIL-HDBK-502A, Logistics Product Data (LPD) IAW GEIA-STD-0007, and other contractual provisions. The Contractor shall insure that FMECA results will be used by other elements within the acquisition program to preclude duplication of effort.

4.4 General procedures. The FMECA shall be performed in accordance with the requirements specified herein to systematically examine the system to the lowest indenture level specified by the procuring activity. The analysis shall identify potential failure modes. When system definitions and functional descriptions are not available to the specified indenture level, the initial analysis shall be performed to the lowest possible indenture level to provide optimum results. When system definitions and functional definitions are complete, the analysis shall be extended to the specified indenture level.

4.4.1 Contributing information. System definition requires a review of all descriptive information available on the system to be analyzed. The following is representative of the information and data required for system definition and analysis.

4.4.1.1 Technical specifications and development plans. Technical specifications and development plans generally describe what constitutes and contributes to the various types of system failure. These will state the system objectives and specify the design and test requirements for operation, reliability, and maintainability. Detailed information in the plans will provide operational and functional block diagrams showing the gross functions the system must perform for successful operation. Time diagrams and charts used to describe system functional sequence will aid in determining the time-stress as well as feasibility of various means of failure detection and correction in the operating system. Acceptable performance limits under specified operating and environmental conditions will be given for the system and equipment. Information for developing mission and environmental profiles will describe the mission performance requirements in terms of functions describing the tasks to be performed and related to the anticipated environments for each mission phase and operating mode. Function-time relationships from which] the time-stress relationship of the environmental conditions can be developed shall be presented. A definition of the operational and environmental stresses the system is expected to undergo, as well as failure definitions, will either be provided or must be developed.

4.4.1.2 Trade-off study reports. These reports should identify areas of marginal and state-of-the-art design and explain any design compromises and operating restraints agreed upon. This information will aid in determining the possible and most probable failure modes and causes in the system.

4.4.1.3 Design data and drawings. Design data and drawings identify each item and the item configuration that perform each of the system functions. System design data and drawings will usually describe the system's internal and interface functions beginning at system level and progressing to the lowest indenture level of the system. Design data will usually include either functional block diagrams or schematics that will facilitate construction of reliability block diagrams.

4.4.1.4 Reliability data. The determination of the possible and probable failure modes requires an analysis of reliability data on the item selected to perform each of the system internal functions. It is always desirable to use reliability data resulting from reliability tests run on the specific equipment to be used with the tests performed under the identical conditions of use. When such test data are not available, reliability data from OEM projections, reliability modeling from sources such as RAIC 217Plus or other industry standard models, or from operational

DRAFT

experience and tests performed under similar use conditions on items similar to those in the systems should be used.

4.4.2 FMEA process. The FMEA shall be initiated as an integral part of the design/development/testing/production processes of system acquisition and shall be updated to reflect design changes. FMEA analysis shall be a major consideration at each design review from preliminary through the final design. The analysis shall be used to assess high risk items and the activities underway to provide corrective actions. The FMEA shall also be used to define special test considerations, quality inspection points, preventive maintenance actions, operational constraints, useful life, and other pertinent information and activities necessary to minimize failure risk. All recommended actions which result from the FMEA shall be evaluated and formally dispositioned by appropriate implementation or documented rationale for no action. Unless otherwise specified, the following discrete steps shall be used in performing an FMEA:

a. Define the system to be analyzed. Complete system definition includes identification of internal and interface functions, expected performance at all indenture levels, system restraints, and failure definitions. Functional narratives of the system should include descriptions of each mission in terms of functions which identify tasks to be performed for each mission, mission phase, and operational mode. Narratives should describe the environmental profiles, expected mission times and equipment utilization, and the functions and outputs of each item.

b. Construct block diagrams. Functional and reliability block diagrams which illustrate the operation, interrelationships, and interdependencies of functional entities should be obtained or constructed for each item configuration involved in the system's use. All system interfaces shall be indicated.

c. Identify all potential item and interface failure modes and define their effect on the immediate function or item, on the system, and on the mission to be performed.

d. Evaluate each failure mode in terms of the worst potential consequences which may result and assign a severity classification category (see 4.4.3).

e. Identify failure detection methods and compensating provisions for each failure mode.

f. Identify corrective design or other actions required to eliminate failure or control the risk.

g. Identify effects of corrective actions or other system attributes, such as requirements for logistics support.

h. Document the analysis and summarize the problems which could not be corrected by design and identify the special controls which are necessary to reduce failure risk.

4.4.3 Severity classification. Severity classifications are assigned to provide a qualitative measure of the worst potential consequences resulting from design error or item failure. A severity classification shall be assigned to each identified failure mode and each item analyzed in accordance with the loss statements listed below. Where it may not be possible to identify an item of failure mode according to the loss statements in the four categories below, similar loss statements based upon loss of system inputs or outputs shall be developed and included in the FMECA ground rules for subject to Government approval. Severity classification categories which are consistent with MIL-STD-882E severity categories are defined as follows:

Category I - Catastrophic-A failure which may cause death or entire weapon system loss (i.e., aircraft, tank, missile, ship, etc.)

Category II - Critical-A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.

Category III - 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.

DRAFT

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

4.5 FMECA Documentation. The results of the FMEA and CA shall be documented in a format that identifies the level of analysis, summarizes the results, documents the data sources and techniques used in performing the analysis, and includes the system definition narrative, resultant analysis data, and worksheets. Analysis documentation can be collected/stored via computer spreadsheet or database to aid in performing the analyses. Worksheet examples for presenting the analysis findings have been provided. The worksheets shall be organized to first display the highest indenture level of analysis and then proceed down through decreasing indenture levels of the system. The ground rules, analysis assumptions, and block diagrams shall be included, as applicable, for each indenture level analyzed. Interim and final analysis reports shall be available for the Government to review to ensure compliance, and shall be discussed at each design review to provide comparisons of alternative designs and to highlight the Category I and Category II failure modes, the potential single failure points, and the proposed design corrections. The final report shall reflect the final design and provide identification of the Category I and Category II failure modes and the single failure points which could not be eliminated from the design. All LPD resulting from FMECA shall be IAW GEIA-STD-0007 and input, updated as required, and maintained in the Government's LPD information management system for review and use.

TASK 101
FAILURE MODE AND EFFECTS ANALYSIS

1. Purpose. The purpose of the FMEA is to study the results or effects of item failure on system operation and, to classify each potential failure according to its severity. LPD outputs from the Failure Mode and Effects Analysis shall be IAW GEIA-STD-0007 and input, updated as required, and maintained in the Government's LPD information management system for review and use.

2. Analysis approach. Variations in design complexity and available data will generally dictate the analysis approach to be used. There are two primary approaches for accomplishing an FMEA. One is the hardware approach which lists individual hardware items and analyzes their possible failure modes. The other is the functional approach which recognizes that every item is designed to perform a number of functions that can be classified as outputs. The outputs are listed and their failure modes analyzed. For complex systems, a combination of the functional and hardware approaches may be considered. The FMEA may be performed as a hardware analysis, a functional analysis, or a combination analysis and may be initiated at either the highest indenture level and proceed through decreasing indenture levels (top-down approach) or at the part or assembly level and proceed through increasing indenture levels (bottom-up approach) until the FMEA for the system is complete.

2.1 Hardware approach. The hardware approach is normally used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. The hardware is normally utilized in a part level up fashion (bottom-up approach); however, it can be initiated at any level of indenture and progress in either direction. Each identified failure mode shall be assigned a severity classification which will be utilized during design to establish priorities for corrective actions.

2.2 Functional approach. The functional approach is normally used when hardware items cannot be uniquely identified or when system complexity requires analysis from the initial indenture level downward through succeeding indenture levels. The functional approach is normally utilized in an initial indenture level down fashion (top-down approach}; however, it can be initiated at any level of indenture and progress in either direction. Each identified failure mode shall be assigned a severity classification which will be utilized during design to establish priorities for corrective actions.

2.3 Failure mode severity classification. Severity classifications are assigned to each failure mode and each item to provide a basis for establishing corrective action priorities. First priority shall be given to the elimination of the identified Category I (catastrophic) and Category II (critical) (see General Requirements, 4.4.3) failure modes. Where the loss of input or output at a lower indenture level is critical to the operational success of a higher indenture level, action shall be taken to eliminate or control the

DRAFT

identified failure modes. When identified Category I and Category II failure modes cannot be eliminated or controlled to levels acceptable to the Government procuring activity, alternative controls and recommendations shall be presented to the procuring activity.

3. Procedure. Each single item failure, as its effects are analyzed, is to be considered the only failure in the system. Where a single item failure is non-detectable, the analysis shall be extended to determine the effects of a second failure, which in combination with the first undetectable failure, could result in a catastrophic or critical failure condition. Passive and multiple failures which may result in catastrophic or critical conditions shall also be identified. When safety, redundant, or back-up items exist, failure assumptions shall be broadened to include the failure conditions which resulted in the need for the safety, redundant, or back-up item. Design changes or special control measures shall be identified and defined for all catastrophic (Category I) and critical (Category II) failure modes. All single failure points identified during the analyses shall be uniquely identified on the FMEA worksheets to maintain visibility of these failure modes.

3.1 System definition. The first step in performing the FMEA is to define the system to be analyzed. Functional narratives shall be developed for each mission, mission phase, and operational mode and include statements of primary and secondary mission objectives. The narratives shall include system and part descriptions for each mission phase and operational mode, expected mission times and equipment utilization, functions and output of each item, and conditions which constitute system and part failure.

3.1.1 Mission functions and operational modes. The system definition shall include descriptions of each mission in terms of functions which identify the task to be performed and the functional mode of operation for performing the specific function. Mission functions and operational modes shall be identified starting at the highest system level and progressing to the lowest indenture level to be analyzed. When more than one method of performing a particular function is available, the alternative operational modes shall be identified. All multiple functions utilizing different equipment or groups of equipment also shall be identified. The functions and outputs for each indenture level also may be presented in a function-output list or in narrative form.

3.1.2 Environmental profiles. The environmental profiles which present the anticipated environmental conditions for each mission and mission phase shall be defined. When a system will be utilized in more than one environment each different environmental profile shall be described. The intended use, through time, of the system and its equipment shall be developed from the mission time statements for each environmental profile. The use time-environment phasing is used in determining the time stress relationships and the feasibility of failure detection methods and compensating provisions in the operating system.

3.1.3 Mission time. A quantitative statement of system function-time requirements shall be developed and included in the system definition. Function-time requirements shall be developed for items which operate in different operational modes during different mission phases and for items which function only if required.

3.1.4 Block diagrams. Block diagrams which illustrate the operation, interrelationships, and interdependencies of functional entities of a system shall be constructed to provide the ability for tracing failure mode effects through all levels of indenture. Both functional and reliability block diagrams are required to show the functional flow sequence and the series dependence or independence of functions and operations. Block diagrams may be constructed in conjunction with or after defining the system and shall present the system as a breakdown of its major functions. More than one block diagram will usually be required to display alternative modes of operation, depending upon the definition established for the system. All inputs and outputs of the item as a whole shall be shown on the diagram and clearly labeled. Each block shall be designated by a consistent and logical item number that reflects the functional system breakdown order. A uniform identification code IAW General Requirements, 4.3.3, shall be used to provide consistent identification and traceability of system functions and equipment.

DRAFT

3.1.4.1 Functional Block Diagrams. A functional block diagram illustrates the operation and interrelationships between functional entities of a system as defined in engineering data and schematics. A functional block diagram will provide a functional flow sequence for the system and each indenture level of analysis and present hardware indenture and can be used for both hardware and functional method FMEAs.

3.1.4.2 Reliability Block Diagrams. A reliability block diagram defines the series dependence or independence of all functions of a system or functional group for each life-cycle event. The reliability block diagram will provide identification of function interdependencies for the system and can be used for a functional method FMEA.

4. FMEA worksheet. The documentation of the FMEA is the next step and is accomplished by completing the columns of the approved FMEA worksheet. An example of a FMEA worksheet format is shown in Figure 101.

4.1 Identification number. A reference designation identification number is assigned for traceability purposes and entered on the worksheet. A uniform identification code IAW General Requirements, 4.3.3, shall be used to provide consistent identification of system functions and equipment, and provide complete visibility of each failure mode and its relationship to the system function identified in the applicable block diagram.

4.2 Item/Functional Identification. The name or nomenclature of the item or system function being analyzed for failure modes and effects is listed. Schematic diagram symbols or drawing numbers shall be used to properly identify the item or function.

4.3 Function. A concise statement of the function performed by the hardware item shall be listed. This shall include both the inherent function of the part and its relationship to interfacing items.

4.4 Failure modes and causes. All predictable failure modes for each indenture level analyzed shall be identified and described. Potential failure modes shall be determined by examination of item outputs and functional outputs identified in applicable block diagrams and schematics. Failure modes of the individual item function shall be postulated on the basis of the stated requirements in the system definition narrative and the failure definitions included in the ground rules. The most probable causes associated with the postulated failure mode shall be identified and described. Since a failure mode may have more than one cause, all probable independent causes for each failure mode shall be identified and described. The failure causes within the adjacent indenture levels shall be considered. For example, failure causes within the 3rd indenture level shall be considered when conduction a 2nd indenture level analysis. Where functions shown on a block diagram are performed by a replaceable module in the system, a separate FMEA shall be performed on the internal functions of the module, viewing the module as a system. The effects of possible failure modes in the module inputs and outputs describe the failure modes of the module when it is viewed as an item within the system. To assist in assuring that a complete analysis is performed, each failure mode and output function shall, as a minimum, be examined in relation to the following typical failure conditions:

a. Premature operation.

b. Failure to operate at a prescribed time.

c. Intermittent operation.

d. Failure to cease operation at a prescribed time.

e. Loss of output or failure during operation.

f. Degraded output or operational capability.

g. Other unique failure conditions, as applicable, based upon system characteristics and operational requirements or constraints.

DRAFT

4.5 Mission phase/operationa1 mode. A concise statement of the mission phase and operational mode in which the failure occurs. Where subphase, event, or time can be defined from the system definition and mission profiles, the most definitive timing information should also be entered for the assumed time of failure occurrence.

4.6 Failure effect. The consequences of each assumed failure mode on item operation, function, or status shall be identified, evaluated, and recorded. Failure effects shall focus on the specific block diagram element which is affected by the failure under consideration. The failure under consideration may impact several indenture levels in addition to the indenture level under analysis; therefore, “local,” “next higher level,” and end” effects shall be evaluated. Failure effects shall also consider the mission objectives, maintenance requirements and personnel and system safety.

4.6.1 Local effects. Local effects concentrate specifically on the impact an assumed failure mode has on the operation and function of the item in the indenture level under consideration. The consequences of each postulated failure affecting the item shall be described along with any second-order effects which result. The purpose of defining local effects is to provide a basis for evaluating compensating provisions and for recommending corrective actions. It is possible for the "local" effect to be the failure mode itself.

4.6.2 Next higher level. Next higher level effects concentrate on the impact an assumed failure has on the operation and function of the items in the next higher indenture level above the indenture level under consideration. The consequences of each postulated failure affecting the next higher indenture level shall be described.

4.6.3 End effects. End effects evaluate and define the total effect an assumed failure has on the operation, function, or status of the uppermost system. The end effect described may be the result of a double failure. For example, failure of a safety device may result in a catastrophic end effect only in the event that both the prime function goes beyond limit for which the safety device is set and the safety device fails. Those end effects resulting from a double failure shall be indicated on the FMEA worksheets.

4.7 Failure detection method. A description of the methods by which occurrence of the failure mode is detected by the operator shall be recorded. The failure detection means, such as visual or audible warning devices, automatic sensing devices, sensing instrumentation, other unique indications, or none shall be identified.

4.7.1 Other indications. Descriptions of indications which are evident to an operator that a system has malfunctioned or failed, other than the identified warning devices, shall be recorded. Proper correlation of a system malfunction or failure may require identification of normal indications as well as abnormal indications. If no indication exists, identify if the undetected failure will jeopardize the mission objectives or personnel safety. If the undetected failure allows the system to remain in a safe state, a second failure situation should be explored to determine whether or not an indication will be evident to an operator. Indications to the operator should be described as follows:

a. Normal. An indication that is evident to an operator when the system or equipment is operating normally.

b. Abnormal. An indication that is evident to an operator when the system has malfunctioned or failed.

c. Incorrect. An erroneous indication to an operator due to the malfunction or failure of an indicator (i.e., instruments, sensors, devices, visual or audible warning devices, etc.).

4.7.2 Isolation. Describe the most direct procedure that allows an operator to isolate the malfunction or failure. An operator will know only the initial symptoms until further specific action is taken such as performing a more detailed built-in-test (BIT). The failure being considered in the analysis may be of lesser importance or likelihood than another failure that could produce the same symptoms and this must be considered. Fault isolation procedures require a specific action or series of actions by an operator, followed

DRAFT

by a check or cross reference either to instruments, control devices, circuit breakers, or combinations thereof. This procedure is followed until a satisfactory course of action is determined.

4.8 Compensating provisions. The compensating provisions, either design provisions or operator actions, which circumvent or mitigate the effect of the failure shall be identified and evaluated. This step is required to record the true behavior of the item in the presence of an internal malfunction or failure.

4.8.1 Design provisions. Compensating provisions which are features of the design at any indenture level that will nullify the effects of a malfunction or failure, control, or deactivate system items to halt generation or propagation of failure effects, or activate backup or standby items or systems shall be described. Design compensating provisions include:

a. Redundant items that allow continued and safe operation.

b. Safety or relief devices such as monitoring or alarm provisions which permit effective operation or limits damage.

c. Alternative modes of operation such as backup or standby items or systems.

4.8.2 Operator actions. Compensating provisions which require Operator action to circumvent or mitigate the effects of the postulated failure shall be described. The compensating provision that best satisfies the indication(s) observed by an operator when the failure occurs shall be determined. This may require the investigation of an interface system to determine the most correct operator action(s). The consequences of any probable incorrect action(s) by the operator in response to an abnormal indication should be considered and the effects recorded.

4.9 Severity classification. A severity classification category (see General Requirements section 4.4.3) shall be assigned to each failure mode and item according to the failure effect. The effect on the functional condition of the item under analysis caused by the loss or degradation of output shall be identified so the failure mode effects will be properly categorized. For lower levels of indenture where effects on higher indenture levels are unknown, a failure's effect on the indenture level under analysis shall be described by the severity classification categories.

4.10 Remarks. Any pertinent remarks pertaining to and clarifying any other column in the worksheet line shall be noted. Notes regarding recommendations for design improvements shall be recorded and further amplified in the FMECA report, IAW General Requirements, 4.5. This entry also may include a notation of unusual conditions, failure effects of redundant items, recognition of particularly critical design features or any other remarks that amplify the line entry. Since it is improbable that all failure modes in Category I and Category II can be designed out, information shall be provided that other reasonable actions and considerations are or have been accomplished to reduce occurrence of a given failure mode and provide a qualitative basis or rationale for acceptance of the design. The rationale for acceptance of Category I and Category II failure modes shall address the following:

a. Design. Those features of the design that relate to the identified failure mode that minimize the occurrence of the failure mode; i.e. safety factors, parts de-rating criteria, etc.

b. Test. Those tests performed that verify the design features and those tests performed pre-operation or during maintenance that would detect the failure mode occurrence.

c. Inspection. The inspection accomplished to ensure that the hardware is being built to the design requirements and the inspection accomplished during pre-operations or maintenance that would detect the failure mode or evidence of conditions that could cause the failure mode.

d. History. A statement of history relating to this particular design or a similar design.

DRAFT

Figure 101 FMEA Worksheet Format Example

System_____
Indenture_____
Reference Drawing_____
Mission or Phase_____

Date_____
Revision Number_____
Analyst(s)_____

Failure Modes and Effects Analysis

Identification Number	Item/Functional Identification (Nomenclature)	Function	Failure Modes and Causes	Mission Phase / Operational Mode	Failure Effects			Failure Detection Method	Compensating Provisions	Severity Class	Remarks
					Local Effects	Next Higher Level	End Effects				

DRAFT

UNCLASSIFIED

TASK 102

CRITICALITY ANALYSIS

1. Purpose. The purpose of the criticality analysis (CA) is to rank each potential failure mode identified in the FMEA Task 101, according to the combined influence of severity classification and its probability of occurrence based upon the best available data. LPD outputs from the Criticality Analysis shall be IAW GEIA-STD-0007 and input, updated as required, and maintained in the Government's LPD information management system for review and use.

1.1 Application. The CA, Task 102, supplements the FMEA, Task 101, and shall not be performed without first performing Task 101.

2. Analysis approach. One approach from the two specified in 2.1 and 2.2 of Task 102 shall be selected. The availability of specific parts configuration data and failure rate data will determine the analysis approach to be used. The qualitative approach is appropriate when specific failure rate data are not available. The failure probability levels, when used, should be modified as the system is better defined. As parts configuration data and failure race data become available, criticality numbers should be calculated and incorporated in the analysis.

2.1 Qualitative approach. Failure modes identified in the FMEA are assessed in terms of probability of occurrence when specific parts configuration or failure rate data are not available. Individual failure mode probabilities of occurrence should be grouped into distinct, logically defined levels, which establish qualitative failure probability level for entry into the appropriate CA worksheet column. Probability of Occurrence levels are defined as follows:

a. Level A - Frequent. A high probability of occurrence during the item operating time interval. High probability may be defined as a single failure mode probability greater than 0.20 of the overall probability of failure during the item operating time interval.

b. Level B - Reasonably probable. A moderate probability of occurrence during the item operating time interval. Probable may be defined as a single failure mode probability of occurrence which is more than 0.10 but less than 0.20 of the overall probability of failure during the item operating time.

c. Level C - Occasional. An occasional probability of occurrence during item operating time interval. Occasional probability may be defined as a single failure mode probability of occurrence which is more than 0.01 but less than 0.10 of the overall probability of failure during the item operating time.

d. Level D - Remote. An unlikely probability of occurrence during item operating time interval. Remote probability may be defined as a single failure mode probability of occurrence which is more than 0.001 but less than 0.01 of the overall probability of failure during the item operating time.

e. Level E - Extremely Unlikely. A failure whose probability of occurrence is essentially zero during item operating time interval. Extremely unlikely may be defined as a single failure mode probability of occurrence which is less than 0.001 of the overall probability of failure during the item operating time.

2.2 Quantitative approach. The failure rate data source used for the quantitative approach shall be the same as that used for the other reliability and maintainability analyses required by contract. When other analyses are not required by contract or a failure rate data source has not been specified by the procuring activity, failure rates and failure rate adjustment factors (e.g., environmental and quality factors) shall be derived as follows:

DRAFT

a. RAIC 217Plus or another current, industry-standard process or model shall be the primary source of failure rate data for electronic and electro-mechanical parts. Both the base failure rate and all failure rate adjustment factors shall be identified.

b. When parts are similar to those listed in the selected model, base failure rates shall be selected from the model and shall include other adjustment factors such as special quality ^{n}-factors, as may be required to modify the model data for applicability to the particular part.

c. Failure rate data for parts not covered by the selected model shall be selected from appropriate alternative data sources.

2.2.1 CA worksheet. Items in this section and related subsections apply when a quantitative approach has been specified. The calculation of a criticality number or assignment of a probability of occurrence level and its documentation are accomplished by completing the columns of the approved CA worksheet. An example of a CA worksheet format is shown in Figure 102.1. Completed CA worksheets shall be included in the FMECA report, IAW General Requirements, 4.5, following the FMEA worksheet for the same indenture level. The following information is the same as given in the FMEA worksheet and shall be transferred to the CA worksheet:

a. Identification number
b. Item/Functional identification
c. Function
d. Failure modes and causes
e. Mission phase/operational mode
f. Severity classification

2.2.1.1 Failure probability/failure rate data source. When failure modes are assessed in terms of probability of occurrence, the failure probability of occurrence level shall be listed. When failure rate data are to be used in the calculation of criticality numbers, the data source of the failure rates used in each calculation shall be listed. When a failure probability is listed, the remaining columns are not required and the next step will be the construction of a criticality matrix (see Sec. 3 of Task 102).

2.2.1.2 Failure effect probability (β). The β values are the conditional probability that the failure effect will result in the identified criticality classification, given that the failure mode occurs. The β values represent the analyst's judgment as to the conditional probability the loss will occur and should be quantified in general accordance with the following:

Failure Effect	β Value
Actual Loss	**1.0**
Probable Loss	**>0.10 to <1.0**
Possible Loss	**>0 to = 0.10**
No Effect	**0**

2.2.1.3 Failure mode ratio (α). The fraction of the part failure rate (λ_p) related to the particular failure mode under consideration shall be evaluated by the analyst and recorded. The failure mode ratio is **the** probability expressed as a decimal fraction that the part or item will fail in the identified mode. If all potential failure modes of a particular part or item are listed, the sum of the α values for that part or item will equal 1.0 (one). Individual failure mode multipliers may be derived from failure rate source data or from test and operational data. If failure

UNCLASSIFIED

DRAFT

mode data are not available, the $\boldsymbol{\alpha}$ values shall represent the analyst's judgment based upon an analysis of the item's functions.

2.2.1.4 Part failure rate ($\boldsymbol{\lambda_p}$). The part failure rate ($\boldsymbol{\lambda_p}$) from the appropriate reliability prediction or as calculated using the procedure from the selected process or model, shall be listed. Where appropriate, application factors **($\boldsymbol{\pi_A}$),** environmental factors **($\boldsymbol{\pi_E}$),** and other **$\boldsymbol{\pi}$-factors** as may be required shall be applied to the base failure rates ($\boldsymbol{\lambda_p}$) obtained from models, handbooks or other reference material to adjust for differences in operating stresses. Values of **$\boldsymbol{\pi}$-factors** utilized in computing $\boldsymbol{\lambda_p}$ shall be listed.

2.2.1.5 Operating time (t). The operating time in hours or the number of operating cycles of the item per mission shall be derived from the system definition and listed on the worksheet.

2.2.1.6 Failure mode criticality number ($\boldsymbol{C_m}$). The value of the failure mode criticality number ($\boldsymbol{C_m}$) shall be calculated and listed on the worksheet. $\boldsymbol{C_m}$ is the portion of the criticality number for the item due to one of its failure modes under a particular severity classification. For a particular severity classification and operational phase, the $\boldsymbol{C_m}$ for a failure mode may be calculated with the following formula:

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

where:

$\boldsymbol{C_m}$ **=** Criticality number for failure mode**.**

β = Conditional probability of mission loss (2.2.1.2 of Task 102).

α = Failure mode ratio {2.2.1.3 of Task 102).

$\boldsymbol{\lambda_p}$ = Part failure rate (2.2.1.4 of Task 102).

t = Duration of applicable mission phase usually expressed in hours or number of operating cycles (2.2.1.5 of Task 102).

2.2.1.7 Item criticality numbers ($\boldsymbol{C_r}$). The second criticality number calculation is for the item under analysis. Criticality numbers **($\boldsymbol{C_r}$)** for the items of the system shall be calculated and listed on the worksheet. A criticality number for an item is the number of system failures of a specific type expected due to the item's failure modes. The specific type of system failure is expressed by the severity classification for the item's failure modes. For a particular severity classification and mission phase, the $\boldsymbol{C_r}$ for an item is the sum of the failure mode criticality numbers, $\boldsymbol{C_m}$**,** under the severity classification and may also be calculated using the following formula:

DRAFT

$$C_r \sum_{n-1}^{j} \left(\beta \alpha \lambda_p t\right)_n$$

and

$$n = 1,2,3, \ldots j$$

where:

$\boldsymbol{C_r}$= Criticality number for the item.

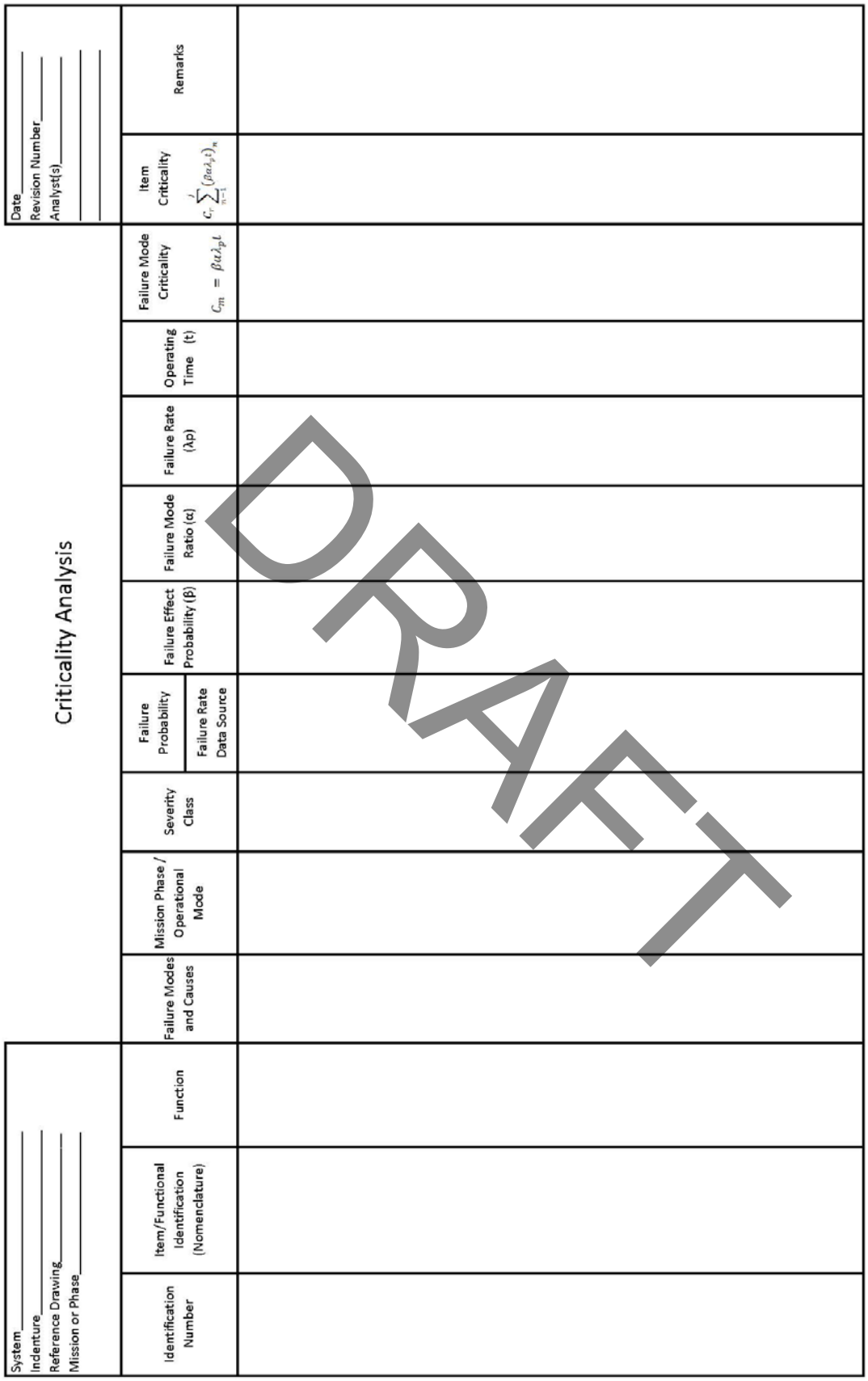
$\boldsymbol{n}$ = The failure modes in the items that fall under a particular criticality classification.

$\boldsymbol{j}$ = Last failure mode in the item under the criticality classification.

3. Criticality matrix. The criticality matrix provides a means of identifying and comparing each failure mode to all other failure modes with respect to severity. The matrix is constructed by inserting item or failure mode identification numbers in matrix locations representing the severity classification category and either the probability of occurrence level or the criticality number $\boldsymbol{(C_r)}$ for the item's failure modes. The resulting matrix display shows the distribution of criticality of item failure modes and provides a tool for assigning corrective action priorities. As shown in Figure 102.2, the further along the diagonal line from the origin the failure mode is recorded, the greater the criticality and the more urgent the need for implementing corrective action. The example criticality matrix in Figure 102.2 was constructed to show how either the criticality number $\boldsymbol{(C_r)}$ or probability of occurrence level can be used for the horizontal axis. The completed criticality matrix shall be included in the FMECA report, IAW General Requirements, 4.5.

DRAFT

Figure 102.1 Criticality Analysis Worksheet Example



System_____
Indenture_____
Reference Drawing_____
Mission or Phase_____

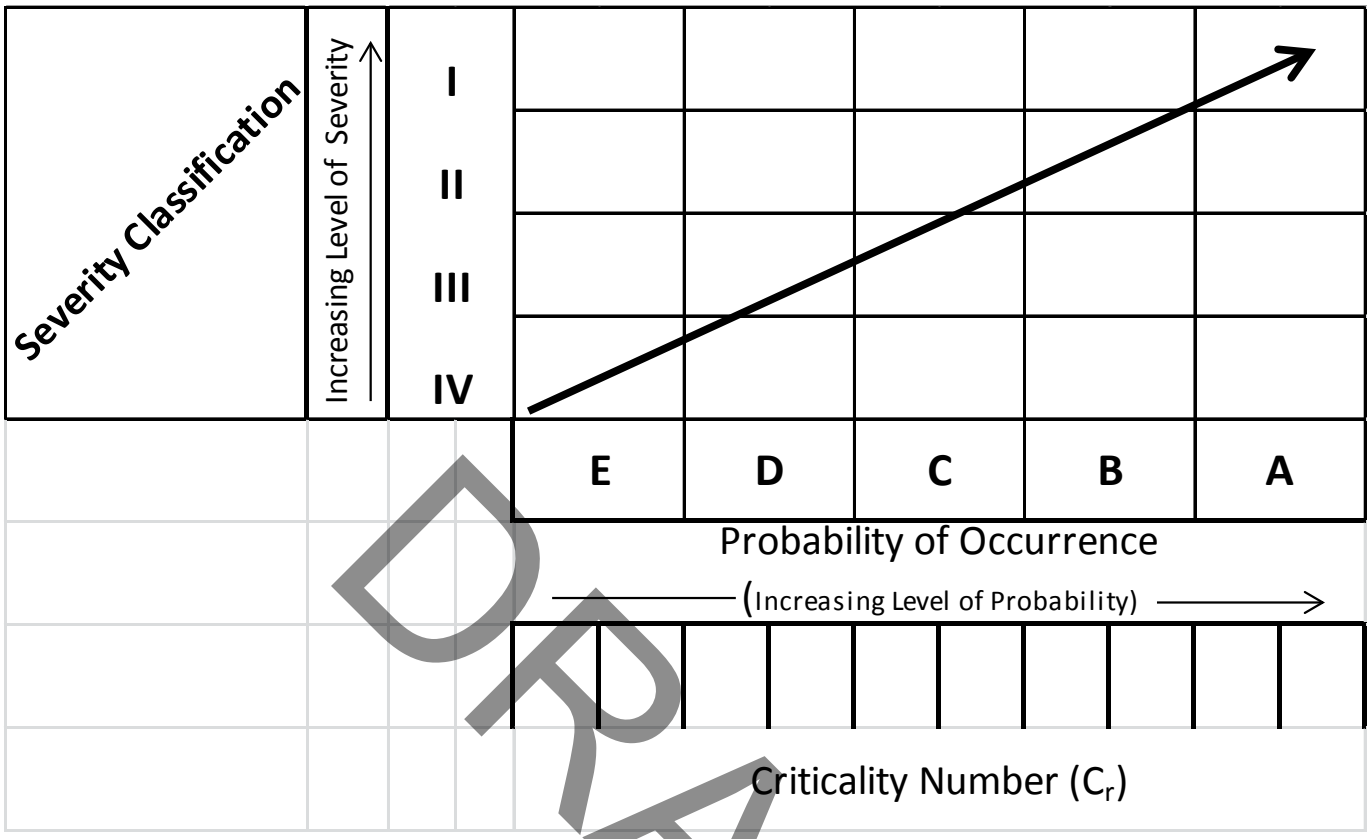
Criticality Analysis

Date_____
Revision Number_____
Analyst(s)_____

Identification Number	Item/Functional Identification (Nomenclature)	Function	Failure Modes and Causes	Mission Phase / Operational Mode	Severity Class	Failure Probability	Failure Rate Data Source	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λp)	Operating Time (t)	Failure Mode Criticality $C_m = \beta\alpha\lambda_p t$	Item Criticality $C_r \sum_{n=1}^{j} (\beta\alpha\lambda_p t)_n$	Remarks

DRAFT

Figure 102.2 Criticality Matrix Example



DRAFT

TASK 103

FMECA-MAINTAINABILITY INFORMATION

1. Purpose. The purpose of the FMECA-maintainability information analysis is to provide early criteria for maintenance planning analysis (MPA), logistics support analysis (LSA), test planning, inspection and checkout requirements, and to identify maintainability design features requiring corrective action. LPD outputs from the FMECA-Maintainability Information Analysis will be IAW GEIA-STD-0007 and input, updated when required, and maintained in the Government's LPD information management system for review and use.

1.1 Application. The FMECA-maintainability information analysis, Task 103, supplements the FMEA, Task 101, and shall not be performed without first performing Task 101.

1.2 Planning. Planning for the FMECA-maintainability information analysis includes considering the requirements to perform and use the FMECA in support of a reliability program in accordance with IAW GEIA-STD-0009, maintainability program IAW MIL-HDBK-470, safety program IAW MIL-STD-882E, logistics support analysis IAW with MIL-HDBK-502A, Logistics Product Data (LPD) IAW GEIA-STD-0007, and other contractual

provisions. The Contractor shall insure that FMECA results will be used by other elements within the acquisition program to preclude duplication of effort**.**

2. FMECA-Maintainability Information worksheet. Documentation of the maintainability information is accomplished by completing the approved FMECA-maintainability information worksheet. An example of an FMECA-maintainability worksheet format is shown in Figure 103. Completed worksheets shall be included in the FMECA report, IAW General Requirements, 4.5, following the FMEA worksheet for the same indenture level. The following information is the same as that given in the FMEA worksheet and shall be transferred to the FMECA-maintainability information worksheet:

a. Identification number

b. Item/functional identification

c. Function

d. Failure modes and causes

c. Failure effects (Local, next higher level, end)

f. Severity classification

2.1 Failure predictability. Enter information on known incipient failure indicators (e.g., operational performance variations) which are peculiar to the item failure trends and permit predicting failures in advance. When a failure is predictable in advance, describe the data that must be collected, how it will be used to predict failure, and identify any tests or inspections that may be accomplished to detect evidence of conditions which could cause the failure mode.

2.2 Failure detection means. Identify how each failure mode will be detected by the Field-Level maintenance technician and to what indenture level they will be localized. Describe the method by which ambiguities are resolved when more than one failure mode causes the same failure indication. Describe any monitoring or warning device that will provide an indication of impending failure and any planned tests or inspections which could detect occurrence of the failure mode. Identify to what indenture level failures can be isolated by the use of built-in-test features and indicate when ancillary test equipment will be required for fault isolation**.**

2.3 Basic maintenance actions. Describe the basic actions which, in the analyst's judgment, must be taken by the maintenance technician to correct the failure. Identify the special design provisions for modular replacement and the probable adjustments and calibration requirements following repair.

2.4 Remarks. Any pertinent remarks pertaining to and clarifying any other columns shall be noted. Notes regarding recommendations for design improvement shall be recorded and further amplified in the FMECA report, IAW General Requirements, 4.5.

DRAFT

Figure 103 FMECA-Maintainability Information Worksheet Example

System_____
Indenture_____
Reference Drawing_____
Mission or Phase_____

Failure Modes Effects and Criticality Analysis
Maintainability Information

Date_____
Revision Number_____
Analyst(s)_____

Identification Number	Item/Functional Identification (Nomenclature)	Function	Failure Modes and Causes	Failure Effects			Severity Class	Failure Predictability	Failure Detection Means	Basic Maintenance Actions	Remarks
				Local Effects	Next Higher Level	End Effects					

DRAFT