



AEROSPACE RECOMMENDED PRACTICE

ARP5580™

Issued 2001-07
Reaffirmed 2020-08

Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications

RATIONALE

ARP5580 has been reaffirmed to comply with the SAE five-year review policy.

FOREWORD

Engineers have always had to consider the effects of component failures on the systems and structures that they design. However, formal methodologies for these types of analyses were not developed until the early 1960s when the obvious safety and reliability requirements of the aerospace industry began to demand them (Reference 2.3.1). In the late 1960s several professional societies began to publish procedures for performing a Failure Modes and Effects Analysis (FMEA). One of the earliest of these was the Society of Automotive Engineers' Aerospace Recommended Practice, ARP926, "Fault/Failure Analysis Procedure" (Reference 2.1.1), published in 1967. In 1974 MIL-STD-1629 (ships), "Procedures for Performing a Failure Mode, Effects and Criticality Analysis" (Reference 2.2.2) was published and, through several revisions, established the basic approach for analyzing a system. By the 1980s FMEA had become a standard part of the design process – at least in the aerospace industry. In 1988 Ford Motor Company published "Potential Failure Mode and Effects Analysis In Design (Design FMEA) and For Manufacturing and Assembly Processes (Process FMEA) Instruction Manual" (Reference 2.3.7) which applied the methodology to manufacturing processes as well as to the design of a product. This procedure focused on the particular needs of the automobile industry and, with input from the major American automobile manufacturing companies and their suppliers, evolved into SAE Surface Vehicle Recommended Practice, J1739 (Reference 2.1.4), issued by the SAE in 1994.

In June of 1994, then Secretary of Defense William Perry issued a memorandum titled "Specifications and Standards – A New Way of Doing Business", which directed the Department of Defense to increase their reliance on commercial products and practices. As a result of "the Perry Memo", many US military standardization documents, including MIL-STD-1629, were cited for cancellation. Around the same time the Defense Standards Improvement Council (DSIC) was chartered to oversee the standardization reform process. DSIC coordinated its position on MIL-STD-1629 with the Society of Automotive Engineers, which through its G-11, Reliability, Maintainability, Supportability and Logistics (RMSL) Division had already chartered a subcommittee to create a new FMEA procedure updating MIL-STD-1629. The subcommittee was comprised of representatives from industry, government and academia. In response to that charter, this recommended best practice has been developed.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2020 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER:
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS:

Full document details: [SAE ARP5580](#)

For more information on this standard, visit
<https://www.sae.org/standards/content/ARP5580>

Documents
Document Sharing Hub

TABLE OF CONTENTS

1. SCOPE	4
1.1 Purpose	4
2. REFERENCES	4
2.1 SAE Publications	4
2.2 U.S. Government Publications	5
2.3 Applicable References	5
2.4 Definitions	6
3. INTRODUCTION	13
3.1 Overview of the Process	14
3.1.1 Functional FMEA	16
3.1.2 Interface FMEA	17
3.1.3 Detailed FMEA	18
3.1.4 FMEA Verification	19
3.1.5 Documentation	19
3.2 FMEA Applications	19
3.2.1 Product Design Hardware FMEA	20
3.2.2 Product Design Software FMEA	21
3.2.3 Process Design FMEA	24
3.3 Cautions	24
4. FMEA PLANNING	25
4.1 FMEA Ground Rules and Assumptions	26
4.2 Analysis Tailoring	27
4.2.1 Depth of Analysis	28
4.3 Supplier/Subcontractor Integration	28
4.4 Analysis Maintenance	30
4.4.1 FMEA Repeatability	30
4.4.2 FMEA Traceability	30
4.4.3 FMEA Coding	31
4.5 Analysis Libraries	31
5. FUNCTIONAL REQUIREMENTS ANALYSIS	32
5.1 Requirements Analysis	33
5.2 Requirements Allocation	34

TABLE OF CONTENTS (Continued)

6. FMEA TASKS	34
6.1 Postulate Failure Modes	35
6.1.1 Failure Mode Modeling.....	36
6.1.2 Failure Mode Ratios	39
6.2 Identify Failure Consequences.....	40
6.2.1 Identify Failure Effects	41
6.2.2 Identify Severity	42
6.2.3 Detecting Monitors	42
6.2.4 Corrective Action Recommendations	45
6.2.5 Identify Compensating Provisions.....	46
6.3 Identify Failure Mode Equivalence	46
6.4 Assess Failure Frequency of Occurrence	48
6.4.1 Constant Failure Rate	49
6.4.2 Process Variation	50
6.4.3 Qualitative Assessment.....	52
6.5 Failure Latency Analysis	52
7. FMEA DOCUMENTATION AND REPORTING	53
7.1 System or End-Item Description	53
7.2 Block Diagrams	53
7.3 FMEA Ground Rules and Assumptions	54
7.4 Analysis Worksheets.....	54
7.4.1 Version/Date	54
7.4.2 Analyst	54
7.4.3 End-item/Process Identifier.....	54
7.4.4 Subsystem/Subprocessor Identifier	54
7.4.5 Item/Function/Action Name.....	54
7.4.6 Item/Function/Action Identifier.....	55
7.4.7 Failure Mode	55
7.4.8 Failure Mode Identifier	55
7.4.9 Failure Mode Probability	56
7.4.10 Fault Equivalence Identifier.....	56
7.4.11 Operating Mode(s)	56
7.4.12 Operating Mode identifier	56
7.4.13 Remarks	57
7.5 Summarize Analysis Results.....	57

1. SCOPE:

Recommended Failure Modes and Effects Analysis (FMEA) Practices For Non-Automobile Applications describes the basic procedures for performing a Failure Modes and Effects Analysis (FMEA). It encompasses functional, interface, and detailed FMEA, as well as certain pre-analysis activities (FMEA planning and functional requirements analysis), post-analysis activities (failure latency analysis, FMEA verification, and documentation), and applications to hardware, software, and process design. It is intended for use by organizations whose product development processes use FMEA as a tool for assessing the safety and reliability of system elements, or as part of their product improvement processes. A separate, Surface Vehicle Recommended Practice, J1739, is intended for use in automobile applications.

1.1 Purpose:

In developing this procedure the subcommittee has endeavored to develop a procedure that reflects the best current commercial practices. This procedure was developed in recognition of today's intense and competitive market demands for high reliability, affordability, and speed to market. The subcommittee had several objectives in defining the FMEA process:

1. Define a basic methodology to include functional, interface, and detailed FMEA. This will facilitate performing the analysis throughout the design process, from early in the conceptual stage to implementation and production.
2. Extend the methodology to include both product and process FMEAs. The methodology can be applied to the many technologies (e.g., mechanical, electrical, software, etc.) used in the development of a product. This helps to facilitate communications between all the parties involved in the development of a system and is useful in a concurrent engineering environment.
3. Provide simple techniques for ranking failure modes for corrective actions and for identifying fault equivalencies.
4. Define the types of information needed for the FMEA in electronic databases, thus facilitating semi-automation of the analysis.
5. Provide procedures for managing the FMEA and for getting the most benefit from the analysis.

2. REFERENCES:

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

2.1 SAE Publications:

Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

- 2.1.1 "Fault/Failure Analysis Procedure", Society of Automotive Engineers, Aerospace Recommended Practice, ARP926, Sept. 15, 1967, ARP926A, Nov. 15, 1979.

- 2.1.2 "Fault/Failure Analysis For Digital Systems and Equipment", Society of Automotive Engineers, Aerospace Recommended Practice, ARP1834, Aug. 1986.
- 2.1.3 Reliability, Maintainability, and Supportability Guidebook, SAE International RMS Committee (G-11), 2nd Ed. Society of Automotive Engineers, 1992.
- 2.1.4 "Potential Failure Mode and Effects Analysis In Design (Design FMEA) and Potential Failure Mode and Effects Analysis In Manufacturing and Assembly Processes (Process FMEA) Reference Manual", Society of Automotive Engineers, Surface Vehicle Recommended Practice, J1739, July 1994.
- 2.1.5 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", Society of Automotive Engineers, Aerospace Recommended Practice, ARP4761, December 1996.

2.2 U.S. Government Publications:

Available from DODSSP, Subscription Services Desk, Building 4D, 700 robbins Avenue, Philadelphia, PA 19111-5094.

- 2.2.1 "Electronic Reliability Design Handbook", MIL-HDBK-338-1, Volume I, Oct. 12, 1988.
- 2.2.2 "Procedures For Performing A Failure Mode Effects and Criticality Analysis", US MIL-STD-1629 (ships) Nov. 1, 1974; US MIL-STD-1629A, Nov. 24, 1980; US MIL-STD-1629A/Notice 2, Nov. 28, 1984.
- 2.2.3 "Reliability Prediction of Electronic Equipment", MIL-HDBK-217F, Dec. 10, 1993.
- 2.2.4 "System Design and Analysis", Advisory Circular 25.1309-1A, Federal Aviation Administration (FAA), June 1988.
- 2.2.5 "Fault Tree Handbook", NUREG-0492, U.S. Nuclear Regulatory Commission, Jan. 1981.

2.3 Applicable References:

- 2.3.1 J. S. Coutinho, "Failure-Effect Analysis", Trans. New York Academy of Sciences, 1964, pp. 564-584.
- 2.3.2 "Failure Mode, Effects, and Criticality Analysis (FMECA)", CRTA-FMECA, Reliability Analysis Center, Rome, NY, 1993.
- 2.3.3 "Nonelectronic Parts Reliability Data -1995", NPRD-95, Reliability Analysis Center, Rome NY, 1995.
- 2.3.4 "Failure Mode/Mechanism Distributions 1997", FMD-97, 1997, Reliability Analysis Center.

- 2.3.5 "Analysis Techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)", International Electrotechnical Commission, IEC Standard Pub. 812, 1985.
- 2.3.6 "Failure Mode and Effect Analyses", Electronic Industries Association G-41 Committee on Reliability, Reliability Bulletin No. 9, November 1971.
- 2.3.7 "Potential Failure Mode and Effects Analysis In Design (Design FMEA) and For Manufacturing and Assembly Processes (Process FMEA) Instruction Manual", Ford Motor Company, Sept 1988.
- 2.3.8 "Reliability Prediction Procedure for Electronic Equipment", Bellcore, TR-TSY-332, Issue 5, December 1995.
- 2.3.9 "Software Considerations in Airborne Systems and Equipment Certification", Radio Technical Commission for Aeronautics, RTCA/DO-178B, Dec. 1992.
- 2.3.10 C. S. Spangler, "Systems Engineering – The Fault Analysis Process For Commercial Avionics Application," Proceedings of the Third Annual International Symposium of the National Council on Systems Engineering, 1993.
- 2.3.11 C. S. Spangler, "Equivalence Relations within the Failure Mode and Effects Analysis". Proc. Ann. Reliability and Maintainability Symp. (Washington, DC), 1999, pp. 352-357.
- 2.3.12 P. L. Goddard, "Validating The Safety Of Embedded Real-Time Control Systems Using FMEA", Proc. Ann. Reliability and Maintainability Symposium, January 1993, pp. 227-230.
- 2.3.13 M. A. Friedman, P. Y. Tran, and P. L. Goddard, Reliability of Software Intensive Systems, Noyes Data Corporation, ISBN: 0-8155-1361-5, 1995.
- 2.3.14 M. A. Friedman, J. Voas, Software Assessment: Reliability, Safety, Testability, John Wiley, ISBN: 0-4710-1009-X, 1995.
- 2.3.15 R. S. Carson, "A Set Theory Model for Anomaly Handling in System Requirements Analysis", Proceedings of the Fifth Annual International Symposium of the National Council on Systems Engineering, 1995.
- 2.3.16 P. D. T. O'Connor, Practical Reliability Engineering, 3rd revised Ed., John Wiley, 1995.

2.4 Definitions:

ALLOCATION: The results of the process of assigning an identified portion of a functional requirement to a specific item of hardware or software, a facility, or to personnel.

BUILT-IN-TEST (BIT): Diagnostic tests included as part of the system design.

BOTTOM-UP ANALYSIS: Analysis of a component, part or subsystem which starts with the failure modes of the lowest indenture level items of the system and successively iterates through the next higher levels ending at the system level.

2.4 (Continued):

CIRCUIT: A description of the task, action, or operation performed by a group of parts at the lowest indenture level.

COMPENSATING PROVISIONS: Design provisions, or operator actions, which circumvent or mitigate the effects of a failure. Compensating design provisions are features at any indenture level that will nullify the effects of a malfunction or failure but do not prevent its occurrence.

COMPONENT TYPE: Classification of a piece-part based on its characteristics and the ways in which it typically fails. Examples: digital integrated circuits; resistors; capacitors; transformers; valves; actuators; air conditioners; batteries; condensers; compressors; filters; fans; fuses; hoses; springs; regulators; relays; seals; pumps; switches; transistors; etc. Piece-part failure modes are postulated based on the "Component Type".

COMPUTER SOFTWARE CONFIGURATION ITEM (CSCI): An aggregation of software that satisfies an end-use function and is intended for separate configuration management by the acquirer. CSCIs are selected based on tradeoffs among software function, size, host, or target computers, developer, support concept, plans for reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors.

COMPUTER SOFTWARE COMPONENT (CSC): An aggregation of software which is part of a CSCI that satisfies one or more end-use functions. A CSC is generally composed of more than one software unit. CSCs are selected based on tradeoffs among software function, size, host, or target computers, developer, plans for reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors.

CORRECTIVE ACTION: A documented design, process, procedure or materials change implemented and validated to eliminate design deficiencies or mitigate failure consequences.

CRITICALITY: A relative measure of the impact of a failure mode on the mission objective. Criticality combines the frequency of occurrence and the level of severity of a failure mode.

CRITICALITY ANALYSIS: A procedure by which each potential failure mode is ranked according to the combined influence of its severity and probability of occurrence.

DETAILED FAILURE MODE & EFFECTS ANALYSIS (DETAILED FMEA): An analysis that assesses the failure causes and effects of failure modes on the individual items (piece-parts, software routines, or process steps) that comprise the system being analyzed.

DETAILED FAILURE MODES, EFFECTS & CRITICALITY ANALYSIS (DETAILED FMECA): An extension of the Detailed FMEA to include an assessment of failure mode severity and probability of occurrence.

DETECTED FAILURE: A postulated failure mode whose presence can be discovered. See Detection Mechanism.

2.4 (Continued):

DETECTION MECHANISM: The means or methods by which a failure can be discovered. Some common detection mechanisms are: (1) an operator under normal system operation; and (2) a maintenance crew by some diagnostic action.

END EFFECT: See End Level Effect.

END-ITEM: The highest level item in a hierarchical analysis of a system. See Item.

END LEVEL EFFECT: The impact or consequence of a failure mode on the operation, function, or status of the end-item. This is derived from analyzing the effects of a failure mode on the major subsystems that make up the complete system. See Mission Impact.

EXPOSURE TIME: The period (in clock time or cycles) during which an item is exposed to a failure. The period is measured from when the function was verified to be functioning to when it is verified again.

FAILURE: The inability of an item to perform its required function within previously specified limits.

FAILURE ANALYSIS: The logical, systematic examination of an item or its diagrams to identify and analyze the probability, causes, and consequences of potential and real failures.

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 process which leads to failure. Failure cause answers the question "Why does the part fail?"

FAILURE EFFECT: The consequences of a failure mode on the operation, function, or status of an item. Failure effects are classified as local effect, next higher level effect, and end effect.

FAILURE MECHANISM: The process involved in the cause of failure. Failure Mechanism answers the question "What is the failure process?"

FAILURE MODE: The manner in which an item fails. Failure Mode answers the question "How does the part fail?"

FAILURE MODE RATIO: The fraction of item failures apportioned to the failure mode under consideration.

FAILURE MODE AND EFFECTS ANALYSIS (FMEA): A procedure by which each potential failure mode or fault of a system is analyzed to determine the consequences or effects thereof on the system, to classify each potential failure mode according to its severity, and to recommend actions to eliminate, or compensate for, unacceptable effects.

FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS (FMECA): An extension of the FMEA procedure to include assessment of the failure mode severity and probability of occurrence.

2.4 (Continued):

FAILURE-REPORTING-AND-CORRECTIVE-ACTION-SYSTEM (FRACAS): A system for reporting failures and tracking them to ensure that corrective actions are taken to correct the problem.

FAN-IN: The specified number of standard load sources that drive an input without impairing normal operations.

FAN-OUT: The specified number of standard loads that an output can drive without impairing normal operations.

FAULT: An anomaly in the functional operation of an equipment or system.

FAULT DETECTION: The process of discovering that a failure has occurred.

FAULT EQUIVALENT FAILURE MODES: A set of failure modes whose consequences are identical.

FAULT INDICATION: The means by which a failure is detected: visual, audible, odorous, console display, printout, etc.

FAULT ISOLATION: The process of determining the location of a fault to effect repair.

FAULT SIGNATURE: Indicators by which a specific system fault can be recognized. It has two parts: (1) the test conditions, consisting of the operator or test stimulus; and (2) the primary output response consisting of measurable parameter changes or monitor indications by which the specific system fault can be recognized.

FAULT TREE: A pictorial representation of the combinations of subsystem and component failures which can result in a specific, often hazardous, system event. The fault tree, when annotated with failure probabilities, can be evaluated to establish the probability of the ultimate undesirable end-level event occurring as a function of the probabilities of the identifiable contributory events.

FD/FI: See Fault Detection, Fault Isolation.

FMEA: See Failure Mode and Effects Analysis.

FMECA: See Failure Mode, Effects and Criticality Analysis.

FUNCTION: Actions which must be performed by an element or elements of the system in order for the system to accomplish its intended purpose.

Within the context of Functional Analysis a function is a description of the task, duty, action, or operation performed by a group of elements at the functional building block level. See Functional Block Diagram.

2.4 (Continued):

FUNCTION TYPE: A classification of a functional block (or function) based on the single task, duty, action, or operation it performs. The classification is done irrespective of the physical implementation of the item. Examples: amplifier, filter, mixer, etc. Functional failure modes are postulated on a per "Function Type" basis. See Function, Functional Block Diagram.

FUNCTIONAL ANALYSIS: The process of examining the characteristics of a defined function to identify all necessary sub-functions. The sub-functions are then arranged to show their relationships.

FUNCTIONAL BLOCK DIAGRAM: A diagram which illustrates the operation, interrelationships, and interdependencies of the functions (shown as functional blocks) of a system/subsystem. See Function, Function Type.

FUNCTIONAL FAILURE MODE AND EFFECTS ANALYSIS (FUNCTIONAL FMEA): A top-level analysis of the failure effects of a system (or subsystem) based upon a failure mode occurring within functional partitions of the system (or subsystem).

FUNCTIONAL FAILURE MODE, EFFECTS & CRITICALITY ANALYSIS (FUNCTIONAL FMECA): An extension of the Functional FMEA to include an assessment of the failure mode severity and probability of occurrence.

HARDWARE: A composite, at any level of complexity, of equipment which is designated to perform a specific function or mission.

HIERARCHY: A partitioning scheme that establishes an ordered relationship between the items in a system. A parent/child or "contained in" ordering is most often used to establish a hierarchical system ordering.

HIGHEST LEVEL INDENTURE: The most complex division of the specific item being analyzed. See Indenture Level.

INDENTURE LEVEL: The item levels which identify or describe the relative complexity of an assembly or function. The levels progress from the more complex to the simpler divisions.

INDUCTIVE ANALYSIS: An analytical approach involving the evaluation of the parts of a system to determine characteristics of the whole system.

INTERFACE: The means by which equipment is interconnected.

INTERFACE FAILURE MODE AND EFFECTS ANALYSIS (INTERFACE FMEA): An analysis which determines the failure effects of failure modes within the interconnections between interfacing hardware or software elements in a system or subsystem. The interconnections may be signals, cables, wires, fiber optics, hydraulic lines, etc.

2.4 (Continued):

INTERFACE FAILURE MODE, EFFECTS & CRITICALITY ANALYSIS (INTERFACE FMECA): An extension of the Interface FMEA to include an assessment of the failure mode severity and probability of occurrence.

ITEM: A non-specific term used to denote any product, including systems, subsystems, parts, components, subassemblies, sets, accessories, software, etc.

LATENT FAILURE: A failure for which the annunciation to the operator is delayed beyond some acceptable threshold such that its occurrence can not be circumvented or corrected.

LINE REPLACEABLE UNIT (LRU): A piece of equipment that is removed and replaced in the field to get the system up and running again. Actual repair may take place elsewhere.

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

LOWEST LEVEL INDENTURE: The simplest division of the specific item being analyzed, usually a piece-part. See Indenture Level and piece-parts.

LRU: See Line Replaceable Unit.

MAINTENANCE LEVELS: The levels within a hierarchically organized maintenance organization at which different repair operations are performed. Typically, Line Level Maintenance refers to line maintenance operations such as the Removal and Replacement (R&R) of an LRU; Shop Level Maintenance refers to repair center (or depot) operations such as R&R of SRUs from an LRU; R&R of piece-parts from an SRU; or checkout of a refurbished SRU.

MISSION: The objective or task, together with the purpose, which clearly indicates the action to be taken.

MISSION IMPACT: The "Go/No Go" failure assessment concerning the ability of the system to operate or complete its mission. This is derived from the end-level effects the failure has on those major subsystems required by the system to operate or complete its mission. See End Level Effect, Failure Effect.

MODULE: A self-contained unit or subsystem that performs a specific task or class of tasks in support of the major function of the system.

NEXT HIGHER LEVEL EFFECT: The consequence a failure has on the operation, functions, or status of the items in the next higher indenture level above the indenture level under consideration. See Failure Effect.

OPERATING MODE: A state or phase of operation in which a system or subsystem can exist. The types of modes examined during the analyses can include normal operating modes, test modes, and transitions between modes, as defined in the applicable system requirements documents.

2.4 (Continued):

PART FAILURE NUMBER: A unique identifier for an individual failure mode.

PIECE-PART: The lowest indenture level hardware item at which a FMEA is usually performed.

PIECE-PART FAILURE MODE & EFFECTS ANALYSIS (PIECE-PART FMEA): An analysis that assesses the failure causes and effects of failure modes on the physical piece-parts which comprise the SRUs and LRUs of a system or subsystem.

PIECE-PART FAILURE MODE, EFFECTS & CRITICALITY ANALYSIS (PIECE-PART FMECA): An extension of the piece-part FMEA to include an assessment of the failure mode severity and its probability of occurrence.

RELIABILITY: The probability that an item will perform its intended function for a specified interval under stated operational and environmental conditions.

SCHEMATIC BLOCK DIAGRAM: A diagram showing the interrelationships of components or piece-parts of a system, subsystem, or function.

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

SEVERITY CLASSIFICATIONS: Severity classifications are assigned to provide a qualitative measure of the worst potential consequences resulting from design error or item failure.

SHOP REPLACEABLE UNIT: A shop level maintenance item located within an LRU.

SINGLE POINT FAILURE: A failure of an item which is not compensated for by redundancy or alternative operational procedures that results in adverse end level effects.

SRU: See Shop Replaceable Unit.

SUBSYSTEM: A combination of components which perform an operational function within a system. Any indenture level or logical (by function) partitioning of the system being analyzed. A subsystem may be implemented physically as one LRU, or it may contain many LRUs.

SUPPLIED REQUIREMENT: A requirement placed on the end-item system by the procuring activity and supplied to the contractor in the product specification or statement of work.

SYSTEM: A composite of equipment, skills, and techniques capable of performing or supporting an operational role. The term system is commonly used to refer to the highest level of requirements and resource grouping applicable to the particular analysis being performed. The actual analysis for some programs could be at the system segment level (e.g., engine system).

2.4 (Continued):

SYSTEM INDICATIONS: The response of the system monitoring provisions that provide the operator with information about the system state, including performance, operational, and failure conditions.

UNDETECTED FAILURE: A postulated failure mode for which there is no system indication.

VALIDATION: The process of confirming on an authoritative basis to accepted engineering principles.

VERIFICATION: (a) The process of proving that a product complies with its formally established requirements. (b) The process of proving by special engineering inspections, analyses, demonstrations, or tests that a system, segment, or configuration item satisfies the requirements of the pertinent development specification.

3. INTRODUCTION:

Failure Modes and Effects Analysis (FMEA) is a formal and systematic approach to identifying potential system failure modes, their causes, and the effects of the failure mode occurrence on the system operation. FMEA provides a basis for identifying potential system failures and unacceptable failure effects that prevent achieving design requirements from postulated failure modes. A FMEA is used in many system design analyses including assessing system safety, planning system maintenance activities, defining provisions for fault recovery, fault tolerance, and failure detection and isolation, and identifying design modifications and corrective actions needed to mitigate the effects of a failure on the system. When the analysis is extended to compare failure modes according to the combined influence of the severity of their effects and the probability of occurrence of the effect, it is called a Failure Mode, Effects, and Criticality Analysis (FMECA).¹

Early identification of design deficiencies minimizes the potential cost of necessary design changes. The objectives and uses of a FMEA include:

1. enhancing system safety by uncovering failure modes that result in hazardous conditions;
2. assessing the mission related effects of critical and/or undetectable failures;
3. influencing the design to mitigate the impact of failures on the final product;
4. supporting verification processes;
5. assuring that the Fault Detection/Fault Isolation (FD/FI) capability designed into the system will meet the FD/FI requirements imposed by the end-item specifications;
6. assisting the design engineer to select a design with a high probability of operational success; and
7. providing data for development of effective maintenance support.

1. Throughout this document the term FMEA is used in a generic sense to include both the failure modes and effects analysis and the prioritization if that is done.

3. (Continued):

FMEA efforts and the design disciplines must work together to correct design deficiencies and mitigate the consequences of failures. When failures are found that present unacceptable consequences, the design is modified to comply with requirements, or derived requirements are fed back into the design to fix or improve it. By focusing attention on the weaknesses of a design and on what can go wrong in building and supporting a product, the FMEA plays a central role in improving the product design.

3.1 Overview of the Process:

FMEA is an inductive analysis that determines how every possible item failure mode affects the system operation. Failure modes are postulated for each item and the effects are traced through the system to determine the resulting system operation. The FMEA interfaces with the System Design, Detailed Design, and Reliability Prediction tasks. Each of these tasks provides inputs to the FMEA. The System Design task provides the requirements baseline and end-item architecture. The Detailed Design task implements the baseline requirements. The Reliability Prediction task provides an assessment of the failure frequency of occurrence that the design is expected to experience in the field due to the given failure mode.

As shown in Figure 1, the FMEA process is initiated during the program Conceptual Design phase and continues through the Preliminary Design phase to verify the adequacy of requirements. During the product's early development there is a great deal of uncertainty: customer needs are not fully understood, and requirements and specifications are usually incomplete. This inherent uncertainty is gradually resolved as the design develops from conception to completion. Refinements to the FMEA track the design as it matures. In the Preliminary Design phase Functional Analysis of the end-item facilitates the reduction of the design uncertainty by assessing how the item functions, both fault-free and with failures. In the Detailed Design phase the analysis is used to verify design compliance with requirements. Testing during the Verification and Validation phase provides a measure of the accuracy of the analysis and helps to maintain the integrity of design changes. Field data for assessing the accuracy of the analysis and maintenance troubleshooting procedures is collected during the Product Use and Support phase.

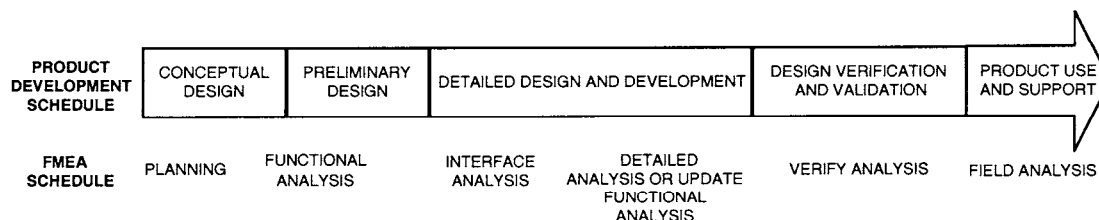


FIGURE 1 - Typical Product Development Cycle Versus FMEA Schedule

3.1 (Continued):

To achieve the objectives of the FMEA process, several analysis tasks are performed. These include:

1. Analysis Planning, initiated during the conceptual design phase;
2. Functional Requirements Analysis, initiated during the conceptual design phase;
3. Failure Mode and Effects Analysis which consists of:
 - a. Functional Analysis, initiated during the conceptual or preliminary design phase;
 - b. Interface Analysis, initiated during the preliminary or detailed design phase; and
 - c. Detailed Analysis, typically initiated during the detailed design phase. In some cases the Functional Analysis may be updated during the detailed design phase rather than do a Detailed Analysis.
4. FMEA verification, initiated during the design verification and validation phase.

Figure 2 shows the general flow of the FMEA process. (The numbers in the boxes indicate the sections in which the indicated tasks are discussed.)

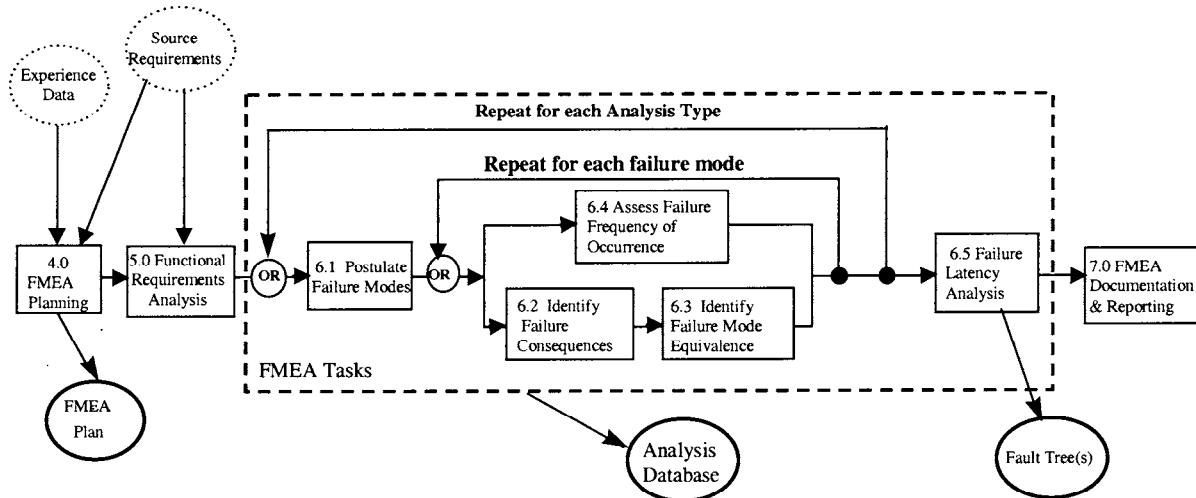


FIGURE 2 - Diagram of the FMEA Process

3.1 (Continued):

Before beginning the analysis the system requirements and operating concept must be specified to the degree that they are known. These include the system operating modes and functions, required performance levels, environmental considerations, and safety or regulatory requirements. Data such as field reports, design rules, checklists, and other guidelines based on lessons learned, technology advances, and the history or analyses of similar systems are collected and studied.

Analysis planning is performed to identify the use of the analysis results to provide design guidance, the procedures for verifying specified requirements and design compliance to requirements. The analysis process is identified to establish how the process and methodology complies with internal guidelines and specified standards, requirements and objectives. (See Section 4.)

Models (often in the form of block diagrams) are developed to illustrate the physical and functional relationships between items and interfaces within the system. From these models, come postulated failure modes to be analyzed for their effects on the system. Potential design weaknesses are identified by assessing the consequences of each failure, and the failure's effect on the system safety, readiness, mission success, demand for maintenance, or logistic support. Ways of detecting the failures and any compensating provisions or design changes needed to mitigate their effects are identified and prioritized based on each failure's severity and probability of occurrence.

A FMEA is classified as either functional, interface, or detailed² according to the way in which the failure modes are postulated. Each type represents a refinement of the system model. As the design details become available the analysis iterates and the system models are expanded and refined until the system has been completely defined, analyzed and documented. The functional, interface, and detailed analyses, combined with the FMEA planning and Functional Requirements Analysis form the basis for the FMEA process outlined previously. These different analysis types are performed during the various phases of the product development cycle. Conducting the analysis in this iterative manner at increasing levels of detail enforces a disciplined review of the baseline design and allows timely feedback to the design process.

- 3.1.1 Functional FMEA: A Functional FMEA is performed on the conceptual design to support the architectural definition and verify necessary design compensation and failure recovery requirements derived by the Functional Requirements Analysis. A Functional FMEA is "black box" in the sense that the functions an item performs are analyzed rather than the characteristics of the specific components used in its implementation. Functional FMEAs may be performed on control systems, processes, software, and complex devices, whose functionality are more readily understood than the details of their operation. A Functional FMEA benefits the design by influencing the definition of the design prior to constructing hardware, coding software, or implementing a process.

2. When applied to hardware, the "detailed" FMEA has historically been called a "piece-part" FMEA. The new terminology recognizes that the FMEA can be applied to a broader range of applications.

3.1.1 (Continued):

A Functional FMEA is performed following guidelines developed in the analysis ground rules. A functional analysis focuses on the functions that an item, group of items, or process performs rather than the characteristics of the specific implementation. The analysis begins with a functional block diagram or equivalent system representation.

The functional block diagrams of the system elements are examined to identify specific types of functions. Each function type identifies a set of previously postulated functional failure modes. Each function is analytically failed, one at a time, in its respective failure modes. The fault characteristics (effects and fault signatures) of each failure mode on the subsystem(s) are determined for each applicable operating mode. As more design details become available, the functional block diagrams and analyses are refined. The analysis iterates in this manner until all the system elements are completely defined and documented. Any single-point failures or undetected failures that cause undesirable end-effects such as loss of end-item functions are reviewed with the respective design discipline. Deficiencies are corrected by making design modifications to the conceptual design or the baseline requirements. The Functional FMEA is then revised to reflect the modifications.

The Functional FMEA is documented through a collection of analysis worksheets. Characteristics of the postulated failure modes are captured on worksheets, usually on a subsystem basis. The worksheets organize all failure modes that exhibit identical consequences into fault equivalence groups.

- 3.1.2 Interface FMEA: An Interface FMEA is performed in the same manner as the Functional FMEA to verify compliance to requirements. Interconnections between subsystems, particularly those designed by separate design groups provide the basis for the postulated failure modes. The advantage of a separate Interface FMEA is that it can be performed before the detailed design of the interconnected subsystems is available. It is begun as soon as the system interconnections are defined to assure that the proper interface protocols are designed. Typical outputs of this analysis are interface failure modes that need to be eliminated or mitigated by interface design changes.

The Interface FMEA is the process of determining and recording characteristics of failures in the interconnections between interfacing system elements. The Interface FMEA begins with the gathering of information on the interfaces of system elements. As shown in Figure 3 interconnections between interfacing hardware elements may be cables, wires, fiber optic lines, hydraulic lines, pneumatic lines, etc. Additionally, information on the software interfaces between system elements should be identified. Previously obtained or generated unit interface diagrams, interface requirements specifications, and interface control documents are examined to identify specific types of interfaces. Failure modes specific to the interfaces are defined and their characteristics (effects and fault signatures) are determined.

Each type of interconnect has its appropriate corresponding failure modes. For example, if the interface is an electrical power system cable, the effect of the "open" failure mode is considered for each wire composing the cable.

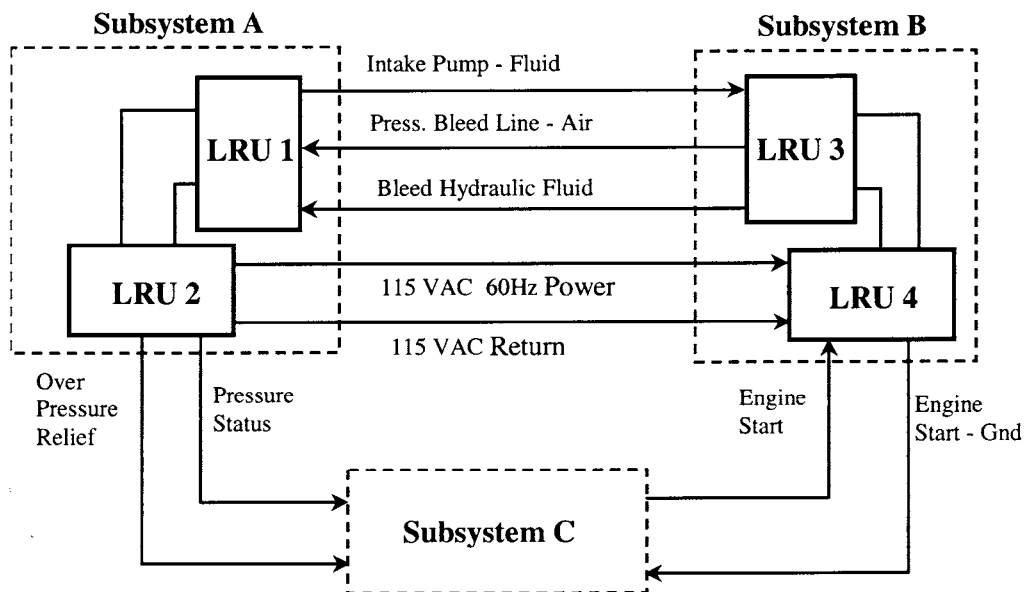


FIGURE 3 - Interface FMEA Examines the Interfaces Between Subsystems

3.1.2 (Continued):

For large systems the system integrator must ensure that the analysis is complete. The subsystem owner or designer is responsible for assessing the effects of all inputs to the subsystem. The system integrator uses the results of the subsystem owners' assessments and applies the results to the interface architecture accounting for all fan-in and fan-out conditions.

- 3.1.3 Detailed FMEA: A Detailed FMEA is performed in the same manner as the corresponding Functional FMEA to verify that the design complies with requirements for failures that can cause loss of end-item functions, single point failures, fault detection, and fault isolation. Components representing the implemented design provide the basis for the postulated failure modes. In a hardware Detailed FMEA the components comprise the physical system design. In a software Detailed FMEA the components are from the software source code.

A Detailed FMEA is the process of determining and documenting characteristics of the failures of each component within the individual system elements (piece-parts, functional part groupings, and as-implemented software). A Detailed FMEA is initiated as the design of each element matures and the detailed design schematics, parts lists, and detailed software design documents and source code become available. This analysis can be performed on the engineering model and revised for changes reflected in the system operational model. An established set of failure modes is essential for performing the detailed analysis correctly. Any single-point or undetected failures that have undesired consequences are reviewed with the respective design discipline. Deficiencies found are corrected by the appropriate design group and the analysis is revised accordingly.