AEROSPACE
RECOMMENDED PRACTICE

SOCIETY OF AUTOMOTIVE ENGINEERS, Inc. 485 Lexington Ave., New York, N. Y. 10017

ARP 926

Issued 9-15-67
Revised

DESIGN ANALYSIS PROCEDURE FOR FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

1. INTRODUCTION

1.1 Definition - Failure Mode, Effects and Criticality Analysis (FMECA) is a design evaluation procedure which documents all conceivable potential failures in a system or component design, determines by single failure analysis the effect of each failure on system operation, identifies failures critical to operational success or personnel safety, and ranks each potential failure according to the combined influence of failure effect severity and probability of occurrence.

1.2 Purpose - FMECA provides:

a. The design engineer with a method of selecting a design with high reliability and high personnel safety potential during early design phase,

b. An additional method to insure that all conceivable failure modes and their effect on operational success of the system have been considered,

c. A list of potential failures which are ranked according to the magnitude of their effect and probability of occurrence,

d. Early criteria for test planning and the design of the test and checkout systems,

e. A basis for quantitative reliability analysis,

f. Historical documentation for future reference to aid in analysis of field failures and/or consideration of design changes,

g. Input data for trade-off studies,

h. A basis for establishing corrective action priorities, and

i. Assistance in the objective evaluation of design requirements related to redundancy, failure detection systems, fail safe characteristics and automatic and manual override.

1.3 Scope - FMECA is normally accomplished before, and provides basic information to, a reliability prediction. FMECA should be initiated as an integral part of the early design process of system functional assemblies and should be periodically updated to reflect design changes. An updated FMECA should be a major consideration in the design reviews, inspections and certifications.

1.4 General Procedure - FMECA is performed in two basic steps:

(1) Failure Mode and Effects Analysis (FMEA)
(2) Criticality Analysis (CA)

1.4.1 Failure Mode and Effects Analysis (FMEA) is a study of the results or effects of single independent component failure in a system. The FMEA procedure is basically a single failure analysis. That is, each failure, as its effects are studied, is considered to be the only failure in the system.

Accomplishment of a FMEA on a system consists of the following general steps:

(1) Define the system to be analyzed, and obtain all descriptive information available on this system. The information should include such documents as functional block diagrams, system descriptions, specifications, drawings, system component identification coding, operational profiles, environmental profiles, and reports bearing on reliability (e g., feasibility or reliability studies of the system and other similar systems).

Representative input information is discussed in paragraph 2.1. The definition of the system interfaces is particularly important.

(2) Construct a reliability logic block diagram of the system to be analyzed (similar to that shown in Fig. 1, page 9), for each equipment configuration involved in the system.

The diagrams are developed starting at the top level of the system, extending downward to the lowest level of system definition at the time the analysis is made. These reliability logic block diagrams are not descriptive block diagrams of the system that show the interconnection of equipment. The reliability logic block diagrams used for an FMEA show the functional interdependencies between the system components so that the effects of a functional failure may be readily traced through the system.

(3) For each system component, at the lowest level of system definition, analyze each potential failure mode of the component and its effect on the system. Where system definition has not reached the piece part level, the system component will be an assembly. Where system hardware definition has not reached the stage of identification of the system functions with the specific type of hardware that will perform these functions, the FMEA should be based upon failure of the system functions, stating the general type of hardware envisioned as the basis for system design.

Four typical modes of component or functional failure to be considered include:

a. Premature operation
b. Failure to operate at a prescribed time
c. Failure to cease operation at a prescribed time
d. Failure during operating

(Other unique failure modes should be considered as applicable.)

The FMEA assumes that only the failure under consideration has occurred. When safety or back-up devices exist, this assumption should be broadened to include the failure conditions which resulted in the need for back-up function.

(4) Document each potential failure mode of each system component and the effects of each failure mode on the system by completing a FMEA format similar to that shown in Fig. 2, pages 10 & 11. Instructions for completing the FMEA format are given in paragraph 2.3.

1.4.2 The Criticality Analysis (CA) is a procedure which determines a system component's criticality relative to a defined loss statement such as crew loss, operation loss, etc. The CA is performed in two steps:

(1) Identify each component's critical failure modes in the FMEA for each equipment configuration.

The critical failure modes in major systems are those that affect the defined loss parameter - for example, operational loss or crew loss.

(2) Compute Criticality Numbers (C_r) for each system component with critical failure modes. The method is given in paragraph 3.2 and a format for the data is shown in Fig. 3, page 12.

The criticality number for a system component is the number of system failures of a specific type expected per some predefined appropriate number of operations,* due to the component's critical failure modes.

*Per million was used in this document. If a different number of operations is used the criticality formula must be changed accordingly.

The specific type of system failure is expressed as a unique loss statement. For major systems, example loss statements are: loss of life, failure to maintain operational status, failure to become operational, and failure causing excessive maintenance.

For lower level systems, example loss statements are: output signal loss, input power shorted, and loss of output pressure.

2. PROCEDURE FOR FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

2.1 System Definition - The first step in accomplishment of the FMEA is definition of the system to be analyzed. The following documentation is representative of the information required for system definition and analysis:

2.1.1 System Technical Development Plans and Specifications - To define what constitutes and contributes to the various types of failure, the technical specifications, requirements, and development plans for the system should be studied. These will normally state the system objectives and specify the design requirements for operation, maintenance, test and activation. Detailed information in the plans will normally provide operational profiles and functional flow block diagrams showing the gross functions the system must perform for successful operation and are usually included at the system level. Time diagrams and charts used to describe system functional sequence will aid the analyst in determining the time-stress as well as feasibility of various means of failure detection and correction in the operating system. 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.

2.1.2 Trade-Off Study Reports - To determine the possible and more probable failure modes and causes in the system, trade-off study reports should identify the areas of marginal design and explain the design compromises and operating conditions agreed upon.

2.1.3 System Description and Specifications - The descriptions and specifications of the system's internal and interface functions starting at the highest system level and progressing to the lowest level of system development to be analyzed is required for construction of the FMEA reliability logic block diagrams. A reliability logic block diagram used in the FMEA portrays the functional interdependencies within the system so the effects of a failure may be traced. System descriptions and specifications usually include either or both functional and equipment block diagrams or schematics that facilitate the construction of the reliability logic block diagrams required for the FMEA. In addition, the system descriptions and specifications give the limits of acceptable performance under specified operating and environmental conditions.

2.1.4 Equipment Design Data and Drawings - Equipment design data and drawings identify the equipment and the equipment configuration that perform each of the system functions.

Where functions shown on a reliability functional block diagram are performed by a replaceable module in the system, a separate FMEA is performed on the internal functions of the module, viewing the module as a system. The effects of possible internal failures in the module then describe the failure modes of the module when it is viewed as a component of the system of which it is a part.

2.1.5 Coding Systems - For consistent identification of system functions and equipment, an approved coding system should be adhered to during the analysis.

2.1.6 Reliability Data - The determination of the possible and probable failure modes requires an analysis of reliability data on the equipment that could perform each of the internal functions of the system or the equipment that the designer has 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, and with the tests performed under the identical conditions of use. When such test data are not available, the analyst should collect and analyze the reliability data that are available from operational experience and tests that have been performed during current and past programs on equipment similar to those in the system under similar use conditions.

The acquisition and correct interpretation of reliability data on the equipment involved in system interfaces should be given particular attention.

2.2 Reliability Logic Block Diagram - The second step of the FMEA procedure is construction of a reliability logic block diagram of the system to be analyzed. The general reliability logic block diagram scheme for a system is shown in Fig. 1, page 9. This example system is for a space vehicle stage and the notes given explain the functional dependencies of the stage components.

A system component at any level in the stage system may be treated as a system and diagramed in like manner for failure mode and effects analysis. The results of the component's FMEA would define the failure modes critical to the component's operation: i.e., those that cause loss of component inputs or outputs. These failure modes will then be used to accomplish the FMEA at the next higher system level. This procedure ultimately leads to a FMEA for the uppermost system.

All system redundancies or other means for preventing failure effects are shown in the reliability logic block diagram since, by definition of single failure analysis, when a means exists to prevent a single failure's effects, the failure cannot be a critical failure above the system level where the preventive means are effective.

It should be pointed out that for a given system, a separate logic diagram may be required for each operational phase or mode since both component use and criticality may vary with the phase or the mode of operation.

2.3 Failure Mode and Effects Analysis - The failure mode and effects analysis and its documentation are the next steps of the procedure. They are accomplished by completing the columns of a FMEA format similar to that given in Fig. 2,* pages 10 & 11, as follows:

(1) Name of system function or component being analyzed for failure mode and effects. Breakdown of a system for analysis should normally be down to the lowest level of system development at the time of the FMEA. In special cases such as electronic systems using integral modular units as system building blocks, the modules may be listed rather than its parts.

(2) Drawing number or code by which each component or module is identified.

(3) Reference designation used to identify component or module or schematic. Applicable schematic and wiring drawing numbers should also be listed.

(4) Identification number of FMEA Reliability Logic Block Diagram and of function on the diagram that the component or module applies to.

(5) Concise statement of the function performed.

(6) Consider at least the four typical failure modes: 1. Premature operation; 2. Failure to operate at a prescribed time; 3. Failure to cease operation at a prescribed time; and 4. Failure during operation.

(7) Individual phase or mode of operation in which critical failure occurs. Where the subphase, event or time can be defined from approved operational profiles, the most definitive timing information should also be entered for the assumed time of critical failure occurrence.

(8) A brief statement describing the ultimate effect of the failure on the function or component being analyzed. Examples: (a) Component rendered useless; (b) Component's usefulness marginal; (c) Structurally weakened.

(9) A brief description of the effect of the failure on the next higher level of the functioning entity within the system. This level may be typified by such items as batteries, fuel tanks, communication receivers, transmitters, engines, inertial units, etc.

*Figure 2 has been partially completed with typical information and serves as an example of the type information expected in this format.

(10) A description of the effect of the component failure on the uppermost system. For major systems, these effects are divided into two groups: 1. failures affecting operational success (examples: operation ended, limited operation, degrade operational objectives, delay, fail to start operation, etc.); and 2. personnel safety (examples: total loss of life, personnel injury, etc.). For lower level systems where effects on the overall system are unknown, a failure's effects on the system under analysis may be described as loss of system inputs or outputs (examples: loss of signal output, loss of output pressure, shorted power input).

(11) A description of the methods by which the failure could be detected. Identify which of the following categories the failure detection means fall under, such as: on-board visual/audible warning devices; automatic sensing devices; ground operational support system failure - sensing instrumentation; flight telemetry, ground support equipment console display, or None.

(12) Identification of both time required for corrective action and time available to take corrective action. The time required for corrective action compared to time available is a significant criticality factor in some types of systems involving either humans in the system loop or automatic corrective action means.

(13) A description of design provisions or compensating means to prevent failure mode or minimize criticality.

(14) This column may be used to identify pertinent information not included in the other columns.

3. PROCEDURE FOR CRITICALITY ANALYSIS (CA)

3.1 Critical Failure Mode Identification

The first step of CA is the identification of critical failure modes from the FMEA's on the system.

Critical failure modes at the higher levels in the overall system should be identified according to approved nonambiguous loss statements similar to the following categories:

Category 1 - Failure which results in potential loss of life.
Category 2 - Failure which results in potential mission failure.
Category 3 - Failure which results in delay or loss of operational availability.
Category 4 - Failures which result in excessive unscheduled maintenance.

At the lower system levels where it is not possible to identify critical failure modes according to loss statements under the four categories above, approved loss statements based upon loss of system inputs or outputs should be used.

The loss statement used to identify a critical failure mode in a system should be prefixed with the word "actual," "probable," "possible," or "none" which represent the analyst's judgment as to the conditional probability that the loss will occur given that the failure mode has occurred. The judgment should be based upon an established set of ranges for probability of loss such as the following:

Effect of Component Failure	Probability of Loss
Actual Loss	100%
Probable Loss	> 10 to <100%
Possible Loss	> 0 to 10%
None	0%

3.2 Criticality Number Calculation:

The second step of the CA procedure is the calculation of Criticality Numbers (C_r) for the system components with critical failure modes.

A criticality number for a system component is the number of system failures of a specific type expected per million* operations due to the component's critical failure modes. The specific type of system failure is expressed by the critical failure mode loss statement discussed in paragraph 3.1.

For a particular loss statement and operational phase, the C_r for a system component with critical failure modes is calculated with the following formula:

$$C_r = \sum_{n=1}^{j} (\beta\alpha\, K_E K_A \lambda_G t \cdot 10^6)_n \qquad n = 1, 2, 3, \ldots, j$$

where:

C_r = Criticality Number for the system component on losses per million trials.

n = The critical failure modes in the system component that fall under a particular loss statement.

j = Last critical failure mode in the system component under loss statement.

λ_G = Generic failure rate of the component in failures per hour or cycle.

t = Operating time in hours or number of operating cycles of the component per mission.

K_A = Operational factor which adjusts λ_G for the difference between operating stresses when λ_G was measured and the operating stresses under which the component is going to be used.

K_E = Environmental factor which adjusts λ_G for difference between environmental stresses when λ_G was measured and the environmental stresses under which the component is going to be used.

NOTE: For simplified uses, omit K_E, K_A, and use λ_G as estimated failure rate for the given failure mode and operating condition.

α = Failure mode ratio of critical failure mode. The failure mode ratio is that fraction of λ_G attributable to the critical failure mode.

β = Conditional probability that the failure effects of the critical failure mode occur, given that the critical failure mode has occurred.

10^6 = Factor which transforms C_r from losses per trial to losses per million trials so C_r will normally be greater than one.

*Per million was used in this document. If a different number of operations is used the criticality formula must be changed accordingly.

The factor β is the probability of loss and should be selected from an established set of ranges.

Failure Effects	Typical Value of Beta
Actual Loss	100%
Probable Loss	> 10% to < 100%
Possible Loss	> 0% to 10%
None	0%

The expression $(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)$ is the portion of C_r for the component due to one of its critical failure modes under a particular loss statement. After calculation of the portion of C_r due to each of the component's critical failure modes under the loss statement, these portions are summed as indicated by $\sum_{n=1}^{j}$

C_r Calculation Example:

Given: System component with $\lambda_G = 0.05$ failures per 10^6 operating hours;

$K_A = 10$; $K_E = 50$; $\alpha = 0.30$ for first critical failure mode under loss statement; $\alpha = 0.20$ for second and last critical failure mode under same loss statement; $\beta = 0.50$; $t = 10$ hours.

Find: C_r for this system component.

Solution: For first critical failure mode:

$$(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_1 = (0.50)(0.30)(50)(10)(0.05 \times 10^{-6})(10)(10^6) = 38$$

For second and last critical failure mode:

$$(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_2 = (0.50)(0.20)(50)(10)(0.05 \times 10^{-6})(10)(10^6) = 25$$

$$C_r = \sum_{n=1}^{2} (\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_n = 38 + 25 = 63$$

3.2.1 Format for Criticality Number Calculation

The columns of the format for criticality number calculations shown in Fig. 3* should be completed as follows:

(1) - (7) These columns duplicate the information given in the same columns of the FMEA format shown in Fig. 2, and are explained in paragraph 2.3.

(8) Failure effects given for the highest system level on the FMEA using a category code similar to that shown in paragraph 3.1.

(9) The source of reliability information used for each calculation should be identified in this column.

(10) - (16) Enter the information required for the calculation of the portion of the component's criticality number due to each of its critical failure modes.

*Figure 3 has been partially completed with typical information and serves as an example of the type of information expected in this format.

(17) Enter the component's criticality numbers in this column. This is the sum of the portions of the criticality number entered in column (16) due to a particular operational phase and loss statement.

3.3 Criticality Analysis Summary

A summary list of critical items can be made from the information derived from the Criticality Analysis. There are several methods to accomplish this list and the method used should be customed to the needs in each case. Generally, this list will include groups of critical items with each group in descending order of criticality number for a given loss statement.

PREPARED BY
COMMITTEE G-11,
AEROSPACE RELIABILITY

NOTES:

1. Stage is dependent on 10, 20, 30 & 40. For the stage to operate, systems 10, 20, 30 & 40 must function.
2. System 10 is dependent on 11, 12 & 13. For the system to operate, subsystems 11, 12 & 13 must function.
3. Subsystem 11 is dependent on 11.01, 11.02, 11.03, 11.04A or 11.04B and 11.05. For the subsystem to operate, the four components in series and one of the parallel components must function.
4. Components 04A and 04B are identical components, redundant for all failure modes.

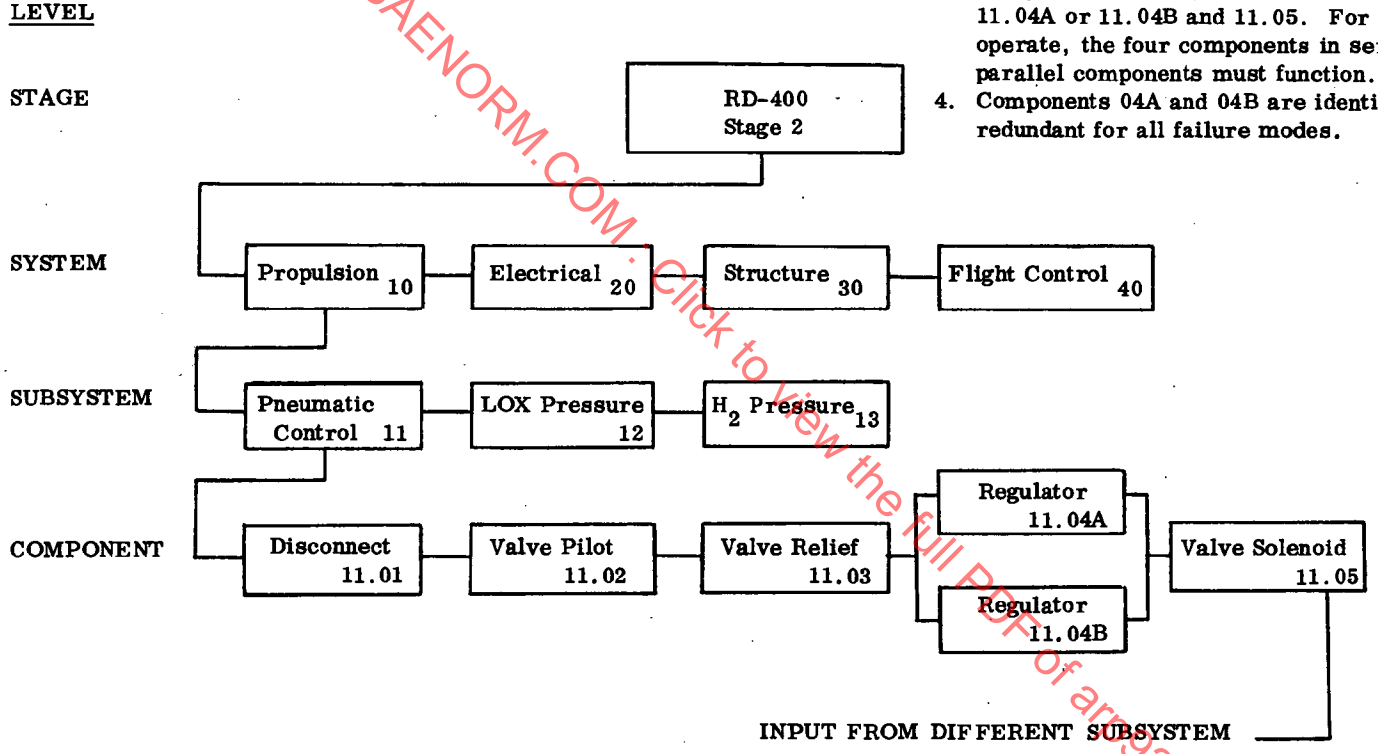

Figure 1 - General Reliability Logic Block Diagram Scheme