N70-76197
RA-006-013-1A

OFFICE OF MANNED
SPACE FLIGHT

APOLLO PROGRAM

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

AUGUST 1966

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON, D.C. 20546

36

N70-76197

RA-006-013-1A

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

August 1966

Prepared by
Apollo Reliability and Quality Assurance Office
National Aeronautics and Space Administration
Washington, D.C. 20546

# PREFACE

This document is an official release of the Apollo Program Office. Many of the procedures and methods are already being carried out. The extent to which this guideline should be implemented at the present stage of program matrurity should be evaluated by comparing the benefits to be derived therefrom with the problems of implementation, including cost.

The principal criteria in judging the value of applying all the procedures of this guideline are the need for these procedures to accomplish identification and ranking of potential failures critical to hardware performance and crew safety. Other considerations, such as, design/development testing, noncriticality of the equipment to system operational success, past experience, and reliability analyses, may preclude the need to perform all the procedures of this guideline.

Willis J. Willoughby
Acting Director
Apollo Reliability and Quality

# TABLE OF CONTENTS

Paragraph Title Page

## SECTION 1—INTRODUCTION

## SECTION 2—PROCEDURE FOR FAILURE MODE AND EFFECTS ANALYSIS

## SECTION 3—PROCEDURE FOR CRITICALITY ANALYSIS

## SECTION 4—SUMMARY OF FMEA AND CA

## TABLE OF CONTENTS (Cont.)

# LIST OF ILLUSTRATIONS

# SECTION 1

# INTRODUCTION

## 1.1 PURPOSE

This document provides guidelines for the accomplishment of Failure Mode, Effects, and Criticality Analysis (FMECA) on the Apollo program. It is a procedure for analysis of hardware items to determine those items contributing most to system unreliability and crew safety problems.

## 1.2 SCOPE

This document is applicable to all NASA activities with cognizance over design, development, and test of Apollo flight, ground, and related equipment which have major impact on mission success. It may be invoked in equipment contracts in whole or in part, where design or development is involved, as a portion of the reliability engineering and as the guideline for carrying out the activity, predicated on budget considerations, equipment criticality, schedules, and other factors.

The ground rules for the use of FMECA may call for substitute overstress tests on structural parts or for other design/development tests of the system in place of the FMECA, or these rules may not require an FMECA on those parts of the system that are established by preliminary FMECA to be noncritical to system operational success.

## 1.3 DEFINITION OF FMECA

Failure Mode, Effects, and Criticality Analysis is a reliability procedure which documents all possible failures in a system design within specified ground rules, determines by failure mode analysis the effect of each failure on system operation, identifies single failure points, i.e., those failures critical to mission success or crew safety, and ranks each failure according to criticality category of failure effect and probability of occurrence. This procedure is the result of two steps: the Failure Mode and Effect Analysis (FMEA), the Criticality Analysis (CA). In performing the analysis, each failure studied is considered to be the only failure in the system.

## 1.4 OBJECTIVES OF FMECA

The FMECA provides:

a. The design engineer with a method of selecting a design with a high probability of operational success and crew safety.

b. Design engineering with a documented method of uniform style for assessing failure modes and their effect on operational success of the system.

c. Early visibility of system interface problems.

d. A list of possible failures which are ranked according to their category of effect and probability of occurrence.

e. Identification of single failure points critical to mission success or to crew safety.

f. Early criteria for test planning.

g. Quantitative and uniformly formatted data input to the reliability prediction, assessment, and safety models.

## 1.5 USE OF FMECA

The FMECA is normally accomplished before a reliability prediction is made to provide basic information. An 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. This analysis may also be used to provide a model for analyzing already-built systems.

An updated FMECA is a major consideration in the design reviews, inspections, and certifications defined in NASA Apollo Program Directive No. 6, Office of Manned Space Flight, August 12, 1965, subject, "Sequence and Flow of Hardware Development and Key Inspection, Review and Certification Checkpoints."

An FMECA should be performed initially at the highest system level feasible. The purpose of this analysis should be to determine the criticality ranking of the major system elements so FMECA program effort may be scoped and allocated for subsystems and equipments critical to system operational success.

## 1.6 FMECA RELATION TO THE RELIABILITY PREDICTION, ASSESSMENT AND CREW SAFETY MODELS

(See "Apollo Reliability Estimation Guidelines", RA 006-007-1.)

FMECA is a simplified reliability estimation tool. It cannot substitute for the reliability prediction and assessment or for crew safety models and their analysis.

FMECA provides quick visibility of the more obvious reliability problems ranked according to their importance to system operational success. Changes made in the system to remove or reduce these more obvious reliability problems will usually restructure major parts of the system. This will make the more detailed analysis of the reliability models an inefficient process for upgrading system reliability during the early stages of design when changes are being made rapidly; hence, the FMECA is particularly appropriate during this period. The FMECA should be reviewed by the designer on a timely basis.

After a satisfactory system design based upon estimates has been obtained, a detailed reliability analysis of the system design is made using the reliability mathematical models. This verifies quantitative reliability goals, verifies the adequacy of redundancy or other failure preventive means built into the system, and discloses subtle reliability problems involving multiple concurrent failures in the system.

Where the detailed analysis results in a redesign of portions of the system, a repetition of the FMECA on these redesigned portions and those portions affected by the redesigned portions is accomplished. The FMECA insures that the design engineers have considered all conceivable failure modes in the new design and their effect on system operational success. Also, the FMECA provides design engineering judgment input to the reliability models.

## 1.7 PROCEDURE OF FMECA

FMECA is performed in two basic steps: (1) Failure Mode and Effects Analysis (FMEA) and (2) Criticality Analysis (CA). The combination of these two steps provides: (3) Failure Mode Effects and Criticality Analysis (FMECA). Section 2 provides step-by-step procedures for FMEA; Section 3 provides step-by-step procedures for CA; and Section 4 combines the FMEA and CA into the FMECA.

# SECTION 2

# PROCEDURE FOR FAILURE MODE AND EFFECTS ANALYSIS

## 2.1 SYSTEM DEFINITION

### 2.1.1 ACCOMPLISHMENT

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

a. Define the system to be analyzed. Obtain all descriptive information available on the system to be analyzed. This 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 such as feasibility or reliability studies of the system being analyzed and of past similar systems.

b. Construct a reliability logic block diagram of the system to be analyzed, similar to that shown in Figure 2-1, for each equipment configuration involved in the system's use.

The diagrams are developed starting at the top level of the system and extending downward to the lowest level of system definition at the time of analysis. These reliability logic block diagrams are not descriptive block diagrams of the system that show the interconnection of equipments. 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.

All redundancies or other means for preventing failure effects should be shown as functional blocks or notes.

Where certain functions are not required in an operational time phase, the information may be shown by a dotted block as in the case of component 05 in Figure 2-1 or by other suitable means.

c. At the lowest level of system definition, as developed from the top down, analyze each failure mode of the system component and its effect on the system. Where system functional definition has not reached the level 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 giving the general type of hardware envisioned as the basis for system design.

Four basic conditions of component or functional failure should be considered:

- Premature operation.
- Failure to operate at a prescribed time.
- Failure to cease operation at a prescribed time.
- Failure during operation.

The FMEA assumes that only the failure under consideration has occurred. When redundancy or other means have been provided in the system to prevent undesired effects of a particular failure, the redundant element is considered operational and the failure effects terminate at this point in the system. When the effects of a failure propagate to the top level of a system and cause the system to fail, the failure is defined as a critical failure in the system.

When an FMEA is being performed on an already-built system, the analyst may find cases where redundancies or other means of preventing failure effects do little to improve the failure situation or where the redundancies may actually worsen it. These cases should be reported for the next higher level. Where the scope of the FMEA program permits, the redundancy or other failure effects preventive means should not halt the continuation of the failure effects analysis toward the top level of the system.

d. Document each potential failure mode of each system component and the effects of each failure mode on the system by completing an FMEA format similar to that shown in Figure 2-2. Instructions for filling out the FMEA format are given on pages 2-6 through 2-10.

## 2.1.2 DOCUMENTATION

The following documentation is representative of the information required for system definition and analysis:

### 2.1.2.1 System Technical Development Plans

To define what constitutes and contributes to the various types of system failure, the technical development plans for the system should be studied. The plans will normally state the system objectives and specify design requirements for operations, maintenance, test, and activation. Detailed information in the plans will normally provide a mission or operational profile and a functional flow block diagram showing the gross functions that the system must perform. Time diagrams and charts used to describe system functional sequence will aid the analyst to determine the time feasibility of various means of failure detection and correction in the operating system. Also required is a definition of the operational and environmental stresses that the system is expected to undergo and a list of the acceptable conditions of functional failure under these stresses.

### 2.1.2.2 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 should explain the design compromises and operating conditions agreed upon.

### 2.1.2.3 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, are required for construction of the FMEA reliability logic block diagrams. A reliability logic block diagram as used in the FMEA and as described in paragraph 2.1.1.6 shows the functional interdependencies within the system and permits the effects of a failure to be traced. System descriptions and specifications usually include either or both functional and equipment block diagrams 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.

### 2.1.2.4 Equipment Design Data and Drawings

Equipment design data and drawings identify the equipment configuration performing each of the system functions.

Where functions shown on a reliability functional block diagram depend on a replaceable module in the system, a separate FMEA may be performed on the internal functions of the module. The effects of possible component failure modes in the module on module inputs and outputs then describe the failure modes of the module when it is viewed as a system component.

### 2.1.2.5 Coding Systems

For consistent identification of system functions and equipment, an approved coding system should be adhered to during the analysis. Use of coding systems common to the overall program are preferable.

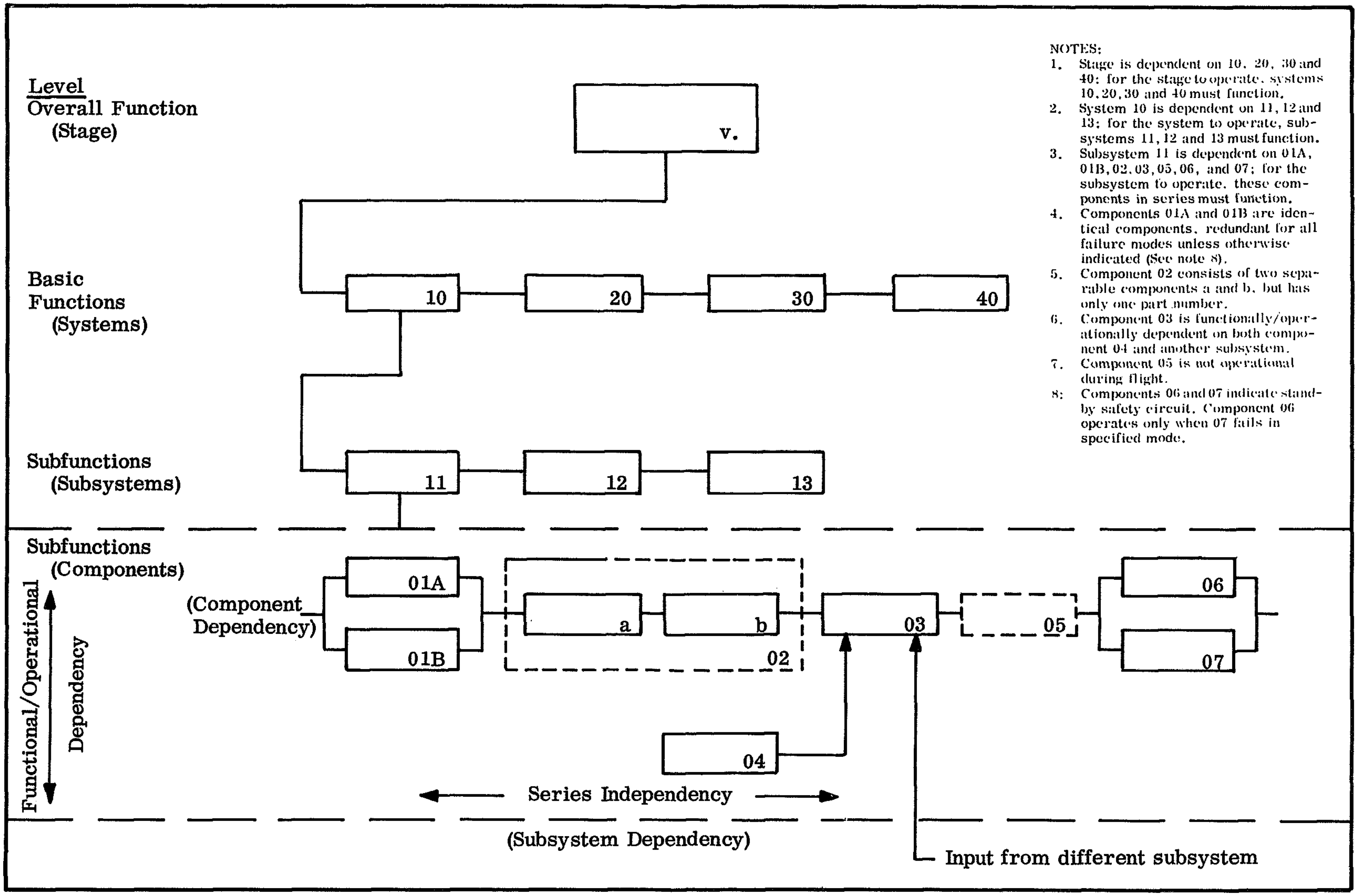
### 2.1.2.6 Test Results

Tests run on the specific equipment under the identical conditions of use are desired. When such test data are not available, the analyst should collect and analyze the data obtained from studies and tests performed during current and past programs on equipment similar to those in the system and under similar use conditions.

## 2.2 RELIABILITY LOGIC BLOCK DIAGRAM

The next step of the FMEA procedure is the 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 Figure 2-1. 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 may be diagrammed 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



NOTES:

1. Stage is dependent on 10, 20, 30 and 40: for the stage to operate, systems 10, 20, 30 and 40 must function.
2. System 10 is dependent on 11, 12 and 13; for the system to operate, subsystems 11, 12 and 13 must function.
3. Subsystem 11 is dependent on 01A, 01B, 02, 03, 05, 06, and 07; for the subsystem to operate. these components in series must function.
4. Components 01A and 01B are identical components, redundant for all failure modes unless otherwise indicated (See note 8).
5. Component 02 consists of two separable components a and b, but has only one part number.
6. Component 03 is functionally/operationally dependent on both component 04 and another subsystem.
7. Component 05 is not operational during flight.
8: Components 06 and 07 indicate standby safety circuit. Component 06 operates only when 07 fails in specified mode.

Figure 2-1. General Reliability Logic Block Diagram Scheme

next higher system level. This procedure ultimately leads to an FMEA for the stage, the space vehicle, and space system.

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

## 2.3 FAILURE MODE AND EFFECTS ANALYSIS

The FMEA and its documentation are the next steps of the procedure. These are accomplished by completing the columns of an FMEA format similar to that given in Figure 2-2 as follows:

Column Number — Explanation or Description of Entries

(1) Name of system function or component under analysis for failure modes and effects. Breakdown of a system for analysis should normally be down to the lowest practicable level 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 listing its parts.

(2) Drawing number by which the contractor identifies and describes each component or module. These drawings should include configuration, mechanical, and electrical characteristics.

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

(4) Identification number of FMEA reliability logic block diagram and of the function.

(5) Concise statement of the function performed.

(6) Give the specific failure mode after considering the four basic failure conditions:

- Premature operation.
- Failure to operate at a prescribed time.
- Failure to cease operation at a prescribed time.
- Failure during operation.

## FAILURE MODE AND EFFECTS ANALYSIS

System ____________
Subsystem ____________
Equipment ____________ Flight ________
Module ____________ GSE ________

Page ______ of ______ Pages
Date ____________
By ____________
Approved ____________

| Item Identification | | | | Function | Failure Mode and Cause | Mission Phase | Failure Effect On | | | Failure Detection Method | Corrective Action Time Available/Time Required | Useful Life |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Ident. Number | Drawing Reference Designation | Reliability Logic Diagram Number | | | | Component/ Functional Assembly | Subsystem | System | | | |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) |
| | | | | | | | | | | | | |

Figure 2-2. General Format for Failure Mode and Effects Analysis

2-7.2.5

Preceding page blank

2-8

Column Number — Explanation or Description of Entries

(6) (Cont.) For each applicable failure mode, describe the cause including operational and environmental stress factors, if known.

(7) Phase of mission in which critical failure occurs, e.g., Prelaunch: checkout, countdown; Flight: boost phase, earth orbit, translunar, lunar landing, etc. Where the subphase, event, or time can be defined from approved operational or flight profiles, the most definitive timing information should also be entered for the assumed time of critical failure occurrence. The most definitive time information that can be determined should also be given for the failure effects under the columns titled "Failure Effects On."

(8) A brief statement describing the ultimate effect of the failure on the function or component being analyzed. Examples of such statements are component rendered useless, component's usefulness marginal, or structurally weakened to unacceptable reliability level. Timing information as described under (7) should be given.

(9) A brief description of the effect of the failure on the next higher assembly. Timing information as described under (7) should be given as to time of failure effect.

(10) A description of the effect of the component failure on the system. For the major systems of the overall space system, these effects are divided into failures affecting mission success and failures affecting crew safety. Examples of failures affecting mission success are abort, limited mission, degrade mission objectives, and vehicle loss, scrub, or hold, etc. Examples of failures affecting crew safety are total loss of crew, partial loss of crew, and loss of redundancy. For lower level systems where effects on the overall space system are unknown, the effects of a failure on the system under analysis may be described as loss of system inputs or outputs. Examples of such effects are loss of signal output, loss of output pressure, and shorted power input. Timing information as described under (7) should be given.

(11) A description of the methods by which the failure could be detected. Identify which of the following categories the failure detection means falls under:

- On-board visual/audible warning devices.
- Automatic abort-sensing devices.
- Ground operational support system failure-sensing instrumentation.

Column Number — Explanation or Description of Entries

(11) (Cont.)

- Flight telemetry, ground support equipment console display, etc.
- None.

Timing information as described under (7) should be given with respect to the reaction time available between time of component failure, time of detection, and time of critical failure effect.

(12) A description of what corrective actions that the flight crew and the ground crew could take to circumvent the failure. If applicable, the time available for effective action and the time required should be noted.

(13) State the useful life of item under given environmental conditions.

# SECTION 3

# PROCEDURE FOR CRITICALITY ANALYSIS

## 3.1 CRITICALITY PROCEDURE

The Criticality Analysis (CA) is reliability procedure which determines a system component's magnitude of criticality to system operational success.

The CA is performed in two steps:

a. Identify critical failure modes of all components in the FMEA for each equipment configuration in accordance with the categories listed in paragraph 3.2. For FMEA's of lower level systems where the effect of failure modes on mission success or crew safety cannot be determined, the critical failure modes will be those that cause failure of one or more of the system's inputs or outputs.

   The specific type of system failure is expressed as a unique loss statement. For major Apollo systems, example loss statements are crew loss, abort, and vehicle scrub. For lower level systems, example loss statements are output signal loss, input power shorted, and loss of output pressure.

b. Compute Critical Numbers ($C_r$) for each system component with critical failure modes. The method is given in paragraph 3.3, and a format for the data is shown in Figure 3-1.

   The $C_r$ for a system component is the number of system failures of a specific type expected per million missions due to the component's critical failures modes.

   Where the factors involved in the calculation of system component criticality numbers vary with mission time, the mission is divided into mission phases such that the change in the factors are negligible. A criticality number is computed for each mission phase for a given loss statement.

The analyst responsible for the CA at the next higher system level continues the analysis using lower level CA's. Where the loss of an input or output of a lower level equipment is critical to equipment operational success at his system level, action should be taken to design the criticality out of the system or to reduce its criticality to an acceptable level by improvements in basic reliability, redundancy, or other means.

## 3.2 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 higher levels in the overall space system should be identified according to approved nonambiguous loss statements. The following categories, according to Reference 5, Appendix A, paragraph 3.3.3, may be used:

### HARDWARE CRITICALITY CATEGORIES FOR FLIGHT HARDWARE

Category 1—Hardware, failure of which results in loss of life of any crew member. This includes normally passive systems, i.e., emergency detection system, launch escape system, etc.

Category 2—Hardware, failure of which results in abort of mission but does not cause loss of life.

Category 3—Hardware, failure of which will not result in abort of mission nor cause loss of life.

### HARDWARE CRITICALITY FOR GROUND SUPPORT EQUIPMENT

Category A—Hardware, failure of which results in the loss of life of any crew member or ground crew member.

Category B—Hardware, failure of which results in abort of mission but does not cause loss of life.

Category C—Hardware, failure of which will not result in abort of mission nor cause loss of life.

At the lower system level where it is not possible to identify critical failure modes according to loss statements under the six categories above, approved loss statements based upon loss of system inputs or outputs should be used (See paragraph 3.1a.). Kennedy Space Center loss statements can be found in Reference 9 of Appendix A. Marshall Space Flight Center loss statements can be found in Reference 8 of Appendix A.

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 represents the analyst's judgment as to the conditional probability that the loss will occur given that the failure mode has occurred.

## 3.3 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 $C_r$ for a system component is the number of system failures of a specific type expected per million missions 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 3.2.

For a particular loss statement and mission 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.

$j$ = Total number of critical failure modes in the system component under loss statement.

$\beta$ = Conditional probability that the failure effects of the critical failure mode occur given that the critical failure mode has occurred.

$\alpha$ = Fraction of all failures (or $\lambda_G$) experienced by a component and that are due to the particular failure mode under consideration.

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

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

$\lambda_G$ = 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.

n = An index of summation for critical failure modes in the system component that fall under a particular loss statement.

The factor $\beta$ is the probability of loss discussed in paragraph 3.1, and should be limited to the following values:

| Failure Effects | Value of Beta |
|---|---|
| Actual Loss | 100 Percent |
| Probable Loss | > 10 Percent to < 100 Percent |
| Possible Loss | 0 Percent to 10 Percent |
| None | 0 Percent |

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 part of $C_r$ due to each of the component's critical failure mode under the loss statement, these parts are summed for all critical failure modes as indicated by

$$\sum_{n=1}^{j} .$$

A failure mode failure rate is represented in the formula for $C_r$ by the product of the terms $\alpha$, $K_E$, $K_A$, and $\lambda_G$. These terms should be replaced by actual failure mode failure rates determined from the test program as they become available. A sample calculation is given on the following page.

### 3.3.1 $C_r$ CALCULATION EXAMPLE

For a given mission phase:

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

$K_A = 10, \quad K_E = 50,$

$\alpha = 0.30$ for one critical failure mode under loss statement, and

$\alpha = 0.20$ for the second critical failure mode under the same loss statement.

Let $\beta = 0.50$ and $t = 10$ hours.

Find: $C_r$ for this system component during this mission phase.

Solution:

For the first critical failure mode, i.e., for n = 1

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

For the second critical failure mode; i.e., for n = 2

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

$j = 2$ and

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

### 3.3.2 FORMAT FOR $C_r$ CALCULATION

The columns of the format for $C_r$ calculations shown in Figure 3-1 should be filled out as follows:

| Column Number | Explanation or Description of Entries |
|---|---|
| (1) - (7) | These columns duplicate the information given in the same columns of the FMEA format shown in Figure 2-2 and are explained in paragraph 2.3. |

| Column Number | Explanation or Description of Entry |
|---|---|
| (8) | Failure effects given for the highest system level on the FMEA. |
| (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. |
| (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 mission phase and loss statement. |

System ______________

Subsystem ______________

Equipment ______________ Flight ________

Module ______________ GSE ________

CRITICALITY ANALYSIS

Page ______ of ______ Pages

Date ______________

By ______________

Approved ______________

| Item Identification | | | | Critical Failures | | | | Criticality Evaluation | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name<br>(1) | Ident. Number<br>(2) | Drawing Reference Designation<br>(3) | Reliability Logic Diagram Number/ Function Number<br>(4) | Function<br>(5) | Failure Mode and Cause<br>(6) | Mission Phase<br>(7) | Failure Effects<br>(8) | Reliability Data Source Code<br>(9) | Probability of Failure Effects $\beta$<br>(10) | Failure Mode Ratio $\alpha$<br>(11) | Environ-mental Ratio $K_E$<br>(12) | Operational Ratio $K_A$<br>(13) | Generic Failure Rate Failures/ Hour or Cycle $\lambda_G$<br>(14) | Operating Time Hours or Cycles $t$<br>(15) | Critical Failure Mode Contribution $(\beta \alpha K_E K_A \lambda_G t \cdot 10^6)$<br>(16) | Component Criticality Number, $C_r$ $\sum_{n=1}^{j} (\beta \alpha K_E K_A \lambda_G t \cdot 10^6)_n$<br>(17) |
| | | | | | | | | | | | | | | | | |

Figure 3-1. General Format for Criticality Number Calculation

Preceding page blank

# SECTION 4

# SUMMARY OF FMEA AND CA

## 4.1 PREPARATION OF FMECA SUMMARY

The procedure is a method for combining the criticality values by mission phase to develop an overall summary.

Preparation of the FMECA summary is developed from the FMEA and CA analysis discussed in Sections 2 and 3 and is accomplished by completing a form similar to that given in Figure 4-1. Instructions for completing the form are given below.

A criticality list is prepared. Critical system components are grouped according to loss statement and are listed in the groups in descending order according to the magnitude of their total criticality number for the particular loss statement. A system component's total criticality number for a particular loss statement is computed from the FMECA summary information. Examples of ground rules for this are given below.

A general FMECA summary form is shown in Figure 4-1. The columns are completed as follows:

| Column Number | Explanation or Description of Entries |
|---|---|
| (1) - (5) | Identification and function of the system component with critical failure modes is the same as are those for the FMEA format in Figure 2-1 which is described in paragraph 2.3. |
| (6) | For each system component, enter its critical failure modes and, if known, their cause. |
| (7) - (9) | If the critical failure mode has an effect during Phase I of the mission, its effect on the system is given in column (7) with mission time or event. The approved loss statement for the effect is given in column (8). The portion of the total criticality number calculated for the critical failure mode according to the example given in paragraph 3.3.1 is entered in column (9). |

Column Number — Explanation or Description of Entries

(10) - (12) Where the critical failure mode has an effect during Phase 2 of the mission, columns (10)-(12) are completed in the same manner as in columns (7)-(9). This format should be extended to include all mission phases.

(13) A total criticality number may be computed for each system component according to approved ground rules. An example of ground rules is as follows:

a. Each criticality number in the mission phase columns shall be multiplied by an approved importance weighting factor for its particular loss statement.

   Example for stage/module level FMECA: Kills Crew = 1.0, Causes abort = 0.5, Launch scrub = 0.4, Launch delay = 0.3.

   Example for subsystem level FMECA: Loss of critical output or input which could lead to crew loss = 1.0, Loss of noncritical input or output = 0.2, Annoyance failure = 0.1.

   These examples are given only to convey the intent. A lengthy list of statements of actual loss may be ranked in <u>relative</u> importance by this means.

b. A given critical failure mode in a system component shall occur only once during the mission; therefore, the largest weighted criticality number for a critical failure mode will be selected from among the mission phase columns for calculation of the component's total criticality number.

c. A component's total criticality number for a particular loss statement shall be the sum of the weighted criticality numbers with the same loss statement selected from the mission phase columns according to ground rule b, preceding.

d. Each total criticality number with loss statement for a system component as calculated by ground rule c. above shall be entered in column (13) of the FMECA summary format.

## 4.2 CRITICALITY LIST

The last step of the FMECA is the preparation of the criticality list. Critical system components are grouped according to loss statement and are listed in the groups in descending order according to magnitude of their total criticality number

System ______ Subsystem ______ Equipment ______ Flight ______ Module ______ GSE ______

FMECA SUMMARY

Page ______ of ______ Pages
Date ______
By ______
Approved ______

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Item Identification | | | | Function | Failure Mode and Cause | Mission Phase Criticality | | | | | | System Component Total Criticality Number |
| | | | | | | Phase 1 | | | Phase 2 | | | |
| Name | Ident. Number | Drawing Reference Designation | Reliability Logic Diagram Number/ Function Number | | | Failure Effect | Loss Statement | Criticality Number | Failure Effect | Loss Statement | Criticality Number | |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) |
| | | | | | | | | | | | | |

Figure 4-1. General FMECA Summary Format

Preceding page blank

4-4

for the loss statement. A system component may appear in more than one of the groups. Appropriate supporting information and recommendations should be given for each of the listed components.

# APPENDIX A

## REFERENCE DOCUMENTS

1. NASA Reliability Publication NPC 250-1, July 1963, "Reliability Program Provisions for Space System Contractors," paragraph 3.4.

2. NASA Quality Publication NPC 200-2, April 1962, "Quality Program Provisions for Space System Contractors," paragraph 4.3.1.

3. NASA Publication M-D MA 500, MA 001.000-1, January 1966, "Apollo Program Development Plan," paragraphs 10.5.3 and 10.5.4.

4. NASA Publication NHB 5300.1, October 1965, "Apollo Reliability and Quality Assurance Program Plan," paragraphs 2.2.3.d, 2.2.4.g, 4.1.a, 4.2.b.(5), 4.7, 5.2.2, 5.2.4, 5.3.1, 5.4, and 5.5.

5. NASA Publication NPC 500-10, 20 May 1964, "Apollo Test Requirements," paragraphs 3.3.3, 3.4.1, 3.5.4.2.c (3), 3.6.2.1.n, and 4.4.1.

6. NASA Publication NHB 5320.2, October 1965, "Manual for Evaluating Apollo Contractor Reliability Plans and Performance," Activity Area 3.4.

7. NASA Apollo Program Directive No. 6, Office of Manned Space Flight, 12 August 1965, "Sequence and Flow of Hardware Development and Key Inspection, Review and Certification Checkpoints."

8. NASA Marshall Space Flight Center Drawing No. 10M30111, Revision A, 26 June 1964, "Procedure for Performing Systems Design Analysis."

9. NASA Kennedy Space Center Publication KSC-STD-118(D), 3 February 1965 "Failure Effect Analysis of Ground Support Equipment."

10. NASA Kennedy Space Center document TR-4-49-3-D, Revised 1 July 1964, "Determination of Criticality Numbers for Saturn I, Block Vehicle Ground Equipment (Launch Complex 37B)."

11. NASA Publication RA 006-007-1, June 1966, "Apollo Reliability Estimation Guidelines".

12. NASA Publication SP-7, "Dictionary of Technical Terminology for Aerospace Use", 1st Edition 1965.

13. NASA Publication SP-6001, "Apollo Terminology," August 1963.

# APPENDIX B

## DEFINITIONS

These definitions, as given below, have been taken from:

a. NASA Publication SP-7, "Dictionary of Technical Terminology for Aerospace Use," 1st Edition, 1965.

b. NASA Publication SP-6001, "Apollo Terminology," August 1963.

APOLLO—A term generally used to describe the NASA Manned Lunar Landing Program but specifically used to describe the effort devoted to the development test and operation of the space vehicle for long duration, Earth orbit, circumlunar, and lunar landing flights.

ABORT—1. To cut short or break off an action, operation, or procedure with an aircraft, space vehicle, or the like, especially because of equipment failure; as to abort a mission, the launching was aborted. 2. An aircraft, space vehicle, or the like that aborts. 3. An act or instance of aborting.

ASSEMBLY—A number of parts or subassemblies or any combination thereof joined together to perform a specific function.

CHECKOUT(C/O)—A test or procedure for determining whether a person or device is capable of performing a required operation or function. When used in connection with equipment, a checkout usually consists of the application of a series of operational and calibrational tests in a certain sequence, with the requirement that the response of the device to each of these tests be within a predetermined tolerance. For personnel, the term checkout is sometimes used in the sense of a briefing or explanation to the person involved, rather than a test of that person's capability.

COMPONENT—An article which is a self-contained element of a complete operating unit and which performs a function necessary to the operation of that unit.

COMPONENT AND PART RELIABILITY—A component or part is reliable when it will operate to a predetermined level of probability under the maximum ratings at most severe combination of environments for which it was designed and for the length of time or number of cycles specified.

COMPONENT STRESS—The stresses on component parts are those factors of usage or test which tend to affect the failure rate of these parts. This includes voltage, power, temperature, frequency, rise time, etc; however, the principal stress, other than electrical, is usually the thermal-environmental stress.

COUNTDOWN—1. A step-by-step process that culminates in a climactic event, each step being performed in accordance with a schedule marked by a count in inverse numerical order; specifically, this process is used in leading up to the launch of a large or complicated rocket vehicle, or in leading up to a captive test, a readiness firing, a mock firing, or other firing test. 2. The act of counting inversely during this process.

In sense 2, the countdown ends with T-time; thus, T minus 60 minutes indicates there are 60 minutes left except for holds and recycling. The countdown may be hours, minutes, or seconds. At the end, it narrows down to seconds, 4-3-2-1-0.

CREW—A group of ground and flight specialists who perform simultaneous and sequential duties and tasks involved in the accomplishment of an assigned operation.

CREW SAFETY—Safe return of all three flight crew members whether or not the mission is completed.

CREW SAFETY PROBABILITY—The probability of flight crew return without exceeding prescribed emergency limits.

CREW SAFETY SYSTEM (CSS)—Consists of the necessary sensors, test equipment, and displays, aboard the spacecraft to detect and diagnose malfunctions and to allow the crew to make a reasonable assessment of the contingency. For emergency conditions, the CSS is capable of initiating an abort automatically.

CRITICAL DEFECT—A defect that judgment and experience indicate could result in hazardous or unsafe conditions for individuals using or maintaining the product or could result in failure in accomplishment of the ultimate objective.

CRITICALITY—Assignment of relative importance to hardware or systems.

CRITICALITY PARTS LIST—A listing of those parts whose failure would cause a degradation in mission success or crew safety.

DESIGN REVIEW—A progressive review, starting after the design study and continuing through the prototype stage. Provides an assessment of reliability and reliability trends by use of applicable tests and prediction techniques.

ENVIRONMENT—The aggregate of all the conditions and influence which affect the operation of equipments and components.

EQUIPMENT—One or more assemblies, or a combination of items, capable of independently performing a complete function.

EQUIPMENT FAILURE—When an equipment no longer meets the minimum acceptable specified performance and cannot be restored through operator adjustment of controls.

FAILURE—The inability of a system, subsystem, component, or part to perform its required function.

FAILURE MECHANISM—The physical process which results in a part or equipment failure.

FAILURE MODE—The physical description of the manner in which a failure occurs, the operating condition of the equipment at the time of the failure.

FAILURE RATE—Rate at which failures occur as a function of time. If the failure rate is constant, it is frequently expressed as the reciprocal of mean-time-between-failure (MTBF).

FEASIBILITY STUDY—The phase during which studies are made of a proposed item or technique to determine the degree to which it is practicable, advisable, and adaptable for the intended purpose.

FLIGHT—1. The movement of an object through the atmosphere or through space, sustained by aerodynamic, aerostatic, or reaction forces, or by orbital speed; especially, the movement of a man-operated or man-controlled device, such as a rocket, a space probe, a space vehicle, or aircraft. 2. An instance of such a movement.

FLIGHT CREW—The Apollo flight crew consists of three men who are cross-trained to be capable of manning any of the Command Module (CM) duty stations. The three crewmen are designated commander, navigator, and systems manager. The CM commander is also the Lunar Excursion Module (LEM) commander.

FLIGHT MISSION—Within a project, the specific technical or scientific objective to be accomplished by a given launching of a space vehicle or launch vehicle.

GROUND OPERATIONAL SUPPORT SYSTEM (GOSS)—Those equipments, exclud-the launch vehicle, spacecraft, and launch complex, required to be in operation for direct support of the mission being accomplished. These equipments shall include those used to provide or support mission control, guidance and navigation, tracking, telemetry, communications, logistics, and recovery operations.

GROUND SUPPORT EQUIPMENT (GSE)—That equipment on the ground, including all implements, tools, and devices (mobile or fixed) required to inspect, test, adjust, calibrate, appraise, gage, measure, repair, overhaul, assemble, disassemble, transport, safeguard, record, store, or otherwise function in support of a rocket, space vehicle, or the like, either in the research and development phase or in an operational pahse, or in support of the guidance system used with the missile, vehicle, or the like.

The GSE is not considered to include land or buildings; nor does it include the guidance-station equipment itself, but it does include the test and checkout equipment required for operation of the guidance-station equipment.

HOLD—During a countdown, to stop counting and to wait until an impediment has been removed so that the countdown can be resumed, as in T minus 40 and holding.

INTERFACE—1. A common boundary between two parts of a system, whether material or nonmaterial. 2. Specifically, in a rocket vehicle or other mechanical assembly, a common boundary between two components.

LAUNCH—1. The action taken in launching a rocket from the surface. 2. The resultant of this action, i.e., the transition from static repose to dynamic flight by the rocket. 3. The time at which this takes place. 4. The action of sending forth a rocket, probe, or other object from a moving vehicle, such as an aircraft or spacecraft.

MAINTENANCE—The function of retaining material in or restoring it to a serviceable condition.

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

MISSION ANALYSIS—A comprehensive evaluation of all the parameters which affect the events of a mission.

MISSION PROFILE—A graphic or tabular presentation of the flight plan of a spacecraft showing all pertinent events scheduled to occur.

MISSION SUCCESS—The attainment of all or a major part of the scientific objectives of the flight with no crew injury or loss of life. It has sometimes been defined as the safe return of all three astronauts from a completed lunar landing mission.

MISSION TASK—The specified purpose for which a device must perform.

MODULE—1. A self-contained unit of a launch vehicle or spacecraft which serves as a building block for the overall structure. The module is usually designated by its primary function as command module, lunar landing module, etc. 2. A one-package assembly of functionally associated electronic parts, usually a plug-in unit, so arranged as to function as a system or subsystem; a block box. 3. The size of some one part of a rocket or other structure, as the semidiameter of a rocket's base, taken as a unit of measure for the proportional design and construction of component parts.

OPERATING TIME—The time period between turn-on and turn-off of a system, subsystem, component or part during which time operation is as specified. Total operating time is the summation of all operating time periods.

PART—1. One of the constituents into which a thing may be divided. Applicable to a major assembly, subassembly, or the smallest individual piece in a given thing. 2. Restrictive. The lease subdivision of a thing; a piece that functions in interaction with other elements of a thing but is itself not ordinarily subject to disassembly.

PRELAUNCH—The phase of operations, beginning with the arrival of space vehicle elements at the launch site and ending with the start of the launch countdown.

REDUNDANCY—The existence of more than one means for accomplishing a given task where all means must fail before there is an overall failure to the system. (NPC 250-1)

Parallel redundancy applies to systems where both means are working at the same time to accomplish the task and when either of the systems is capable of handling the job itself in case of failure of the other system. Standby redundancy applies to a system where there is an alternative means of accomplishing the task that is switched in by a malfunction sensing device when the primary system fails.

RELIABILITY—Of a piece of equipment or a system, the probability of specified performance for a given period of time when used in the specified manner.

RELIABILITY ASSESSMENT—An analytical determination of numerical reliability of a system or portion thereof without actual demonstration testing. Such assessments usually employ mathematical modeling, use of available test results, and some use of estimated reliability figures.

SCRUB—To cancel a scheduled firing either before or during countdown.

SPACE SYSTEM—A system consisting of launch vehicle, spacecraft, ground support equipment, and test hardware used in launching, operating, and maintaining the vehicle or craft in space.

SUBSYSTEM—A major functional subassembly or grouping of items or equipment which is essential to operational completeness of a system.

SYSTEM—1. Any organized arrangement in which each component part acts, reacts, or interacts in accordance with an overall design inherent in the arrangement. 2. Specifically, a major component of a given vehicle such as a propulsion system or a guidance system. Usually called a major system to distinguish it from the systems subordinate or auxiliary to it.

The system of sense 1 may become organized by a process of evolution, as in the solar system, or by deliberate action imposed by the designer, as in a missile system or an electrical system.

In sense 2, the system embraces all its own subsystems including checkout equipment, servicing equipment, and associated technicians and attendants. When the term is preceded by such designating nouns as propulsion or guidance, it clearly refers to a major component of the missile. Without the designating noun, the term may become ambiguous. When modified by the word major, however, it loses its ambiguity and refers to a major component of the missile.

TEST—1. A procedure or action taken to determine under real or simulated conditions the capabilities, limitations, characteristics, effectiveness, reliability, or suitability of a material, device, system, or method. 2. A similar procedure or action taken to determine the reactions, limitations, abilities, or skills of a person, other animal, or organism.