FLIGHT ASSURANCE PROCEDURE

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

1.0 PURPOSE

This procedure establishes guidelines for conducting a Failure Modes and Effects Analysis (FMEA) on GSFC spacecraft and instruments.

2.0 REFERENCE

a.	NHB 5300.4	Reliability Program Requirements for Aeronautical and Space System Contractors
b.	CR 5230.9	Payload and Experiment Failure Model and Effects Analysis and Critical Items List Groundrules
c.	MIL-STD 1629	Procedures for Performing a Failure Modes, Effects, and Criticality Analysis

3.0 DEFINITIONS

a. Failure Mode - A particular way in which an item fails, independent of the reason for failure.

b. Failure Mode and Effects Analysis (FMEA) - A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed to determine the effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

c. Indenture Levels - The hierarchy of hardware levels from the part to the component to the subsystem to the system, etc.

d. Redundancy - More than one independent means of performing a function. There are different kinds of redundancy, including:

(1) Operational - Redundant items, all of which are energized during the operating cycle; includes load-sharing, wherein redundant items are connected in a manner such that upon failure of one item, the other will continue to perform the function. It is not necessary to switch out the failed item or switch in the redundant one.

3.0 DEFINITIONS (cont.)

(2) Standby - Items that are inoperative (have no power applied) until they are switched in upon failure of the primary item.

(3) Like Redundancy - Identical items performing the same function.

(4) Unlike Redundancy - Nonidentical items performing the same function.

4.0 SCOPE

Typical ground rules for an FMEA are given along with an overview of the technique, principal, step-by-step instructions, sample work sheets, and work sheet data entries. Specific projects must, of course, add to, delete and otherwise tailor the procedures to conform with their needs, objectives, and contractual requirements. That is particularly true of safety issues or workaround operational methods. Although software analysis is outside the scope of an FMEA, the effects of failure modes at both software and hardware-software interfaces are included.

5.0 INSTRUCTIONS

5.1 GENERAL

5.1.1 Objective of the FMEA

The objective of an FMEA is to identify the way failures could occur (failure modes) and the consequences of the failures on spacecraft performance (failure effect) and the consequences on mission objectives (severity assignment). It is based on the usual case on which failure effects, which are expressed at the system level, are caused by failure modes at lower hardware levels. The procedure herein, does not quantify the probability for failure occurrence; rather a qualitative assessment of the failure effect is gained by assigning the failure mode to a severity category.

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

The results of the analysis are used to improve system performance by initiating corrective action, usually design changes; they are also useful in focusing product assurance procedures and identifying operational constraints. The FMEA is updated as necessary to include design changes and operational revisions.

5.1.2 Methodology

A bottom-up methodology, the FMEA is initiated by selecting the hardware at the lowest level of interest (e.g., component module, circuit, part). The various failure modes that can occur for each item at that level are tabulated. The corresponding failure effect, in turn, is interpreted as a failure mode at the next higher functional level. Successive iterations result ultimately in identification of the failure effects up to the highest system level. It is a process of inductive synthesis.

5.1.3 Timing

The effectiveness of the FMEA in the design process is dependent upon its early use in the identification of problems and the communication of the information gained to project personnel who can initiate changes before design becomes fixed. Therefore, the FMEA should be initiated as soon as preliminary design information is avai lable and then applied at greater depth as the design takes shape.

5.1.4 Preliminary Subsystem Analysis

During the conceptual phase of system development, when design information is limited to block diagrams, a “functional approach” is appropriate for identifying design problems. Failures are postulated for the major subsystems (the subsystems can also be broken down into lower-level blocks). The effects are assessed, and conceptual design changes are made as necessary. The identified failures are assigned to a severity category (defined in 5.1.8) with emphasis given to catastrophic and critical failures for which possible workaround procedures can be planned.

5.1.5 Detailed Hardware Analysis

Detailed hardware analysis is conducted when hardware items, signal lines, and power lines have been assigned. Using schematics and assembly drawings, failure modes are

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

postulated and their effects assessed. The failure modes are defined at the component interface, based on knowledge of the internal design and the effects are assessed at the component level are upward to higher hardware levels of assembly. The hardware level at which analysis begins is included in the project's Statement of Work, which usually requires analysis to the component level. The analysis is often extended to the part level as needed; that is especially true for safety considerations. At the part level, failure modes are defined for the parts within a component and the effect is assessed at the component interface.

5.1.6 Failure Modes

All the ways that a failure may occur at the har dware indenture level are identified. All probable, possible, or credible modes of failure are postulated; they include failure mechanisms that have been observed historically and whose mechanisms have been described in accordance with sound engineering reasoning.

The identification of the failure modes is based on a knowledge of the component, functional specifications, interface requirements, schematics, or failure modes of the piece parts associated with the interface. Failure modes at interfaces typically involve electrical connectors. Failures within the unit appear as short to ground, short to a voltage or open, for both signal and power lines. The analysis is for the purpose of detecting potential interface failures o riginating within the unit; the failure modes internal to the connectors are not considered.

Although it is not necessary to understand circuitry adjacent to connectors in order to identify a generic set of failure modes, such an understanding will help rule out certain failure modes and thereby reduce the amount of analytical work that has to be done.

5.1.6.1 Failure modes that occur within a unit, be it electrical or mechanical, are manifested at the interface by one of the following failure conditions:

a. Premature operation,

b. Failure to operate at a prescribed time,

5.0 INSTRUCTIONS (cont.)

c. Failure to cease operation when required.

d. Failure during operation.

5.1.7 The Hardware-Software Interface

Although software analysis is outside the scope of an FMEA, the hardware-software interfaces are examined from two perspectives:

a. Failures of the hardware that result in improper or lack of response to the software.

b. Failures in the software that affect hardware operations.

The results are brought to the attention of software designers and analysts for their consideration and possible corrective action. Examples of failures in the software that affect hardware operation follow:

a. Commands are too early.
b. Commands are too late.
c. Failure to command.
d. Commands erroneously.

5.1.8 Failure Effect Severity Categories

To provide a qualitative measure of the failure effect, each failure mode is assigned to a severity category. Safety issues and impact to other systems or property are reflected in the selection of the severity category.

The failure effect is assessed first at the hardware level being analyzed, then the next higher level, the subsystem level, and so on to the system or mission level. In selecting the severity category, the worst case consequence, considering all levels, are assumed for the failure mode and effect being analyzed.

Severity categories are defined below. Specific projects may require expanded definitions depending, for example, on the amount of degradation that is allowable in the return of scientific data.

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

a. Category 1, Catastrophic - Failure modes that could result in serious injury or loss of life, or damage to the launch vehicle.

b. Category 1R, Catastrophic - Failure modes of identical or equivalent redundant hardware items that, if all failed, could result in Category 1 effects.

c. Category 2, Critical - Failure modes that could result in loss of one or more mission objectives as defined by the GSFC project office.

d. Category 2R, Critical - Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed.

e. Category 3, Significant - Failure modes that could cause degradation to mission objectives.

f. Category 4, Minor - Failure modes that could result in insignificant or no loss to mission objectives.

5.1.9 Ground Rules and Assumptions

The ground rules off each FMEA include a set of project-selected procedures; the assumptions on which the analysis is based; the hardware that has been included and excluded from the analysis and the rationale for the exclusions. The ground rules also describe the indenture level of the analysis, the basic hardware status, and the criteria for system and mission success. Every effort should be made to define all ground rules before the FMEA begins; however, the ground rules may be expanded and clarified as the analysis proceeds.

A typical set of ground rules (assumptions) follows:

a. Only one failure mode exists at a time.

b. All inputs (including software commands) to the item being analyzed are present and at nominal values.

c. All consumables are present in sufficient quantities.

d. Nominal power is available.

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

e. All mission phases are considered in the analysis; mission phases that prove inapplicable may be omitted.

f. Connector failure modes are limited to: connector disconnect.

g. Special emphasis will be directed towards identification of single failures that could cause loss of two or more redundant paths.

5.2 THE FMEA PROCESS

The following paragraphs present a typical procedure for conducting an FMEA. The sample series of tasks can be modified in keeping with the space project's operational requirements and mission concerns. The procedure is summarized in Figure 1 and as follows:

5.2.1 Define the system to be analyzed. A complete system definition includes identification of internal and interface functions, expected performance at all indenture levels, system restraints, and failure definitions. Also state systems and mission phases not analyzed giving rationale for the omissions.

5.2.2 Indicate the depth of t he analysis by identifying the indenture level at which the analysis is begun.

5.2.3 Identify specific design requirements that are to be verified by the FMEA.

5.2.4 Define ground rules and assumptions on which the analysis is based. Identify mission phases to be analyzed and the status of equipment during each mission phase.

5.2.5 Obtain or construct functional and reliability block diagrams indicating interrelationships of functional groups, system operation, independent data channels, and backup or workaround features of the system.

5.2.6 Identify failure modes, effects, failure detection and workaround features and other pertinent information on the worksheet.

5.2.7 Evaluate the severity of each failure effect in ac cordance with the prescribed severity categories.

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

5.2.8 Identify hardware designs (or operations) that are candidates for corrective action and recommend specific corrective measures.

5.2.9 Document the analysis and summarize the results.

5.3 ANALYZING EACH FAILURE MODE

The FMEA tasks listed in 5.2 are performed once for each analysis. Tasks 5.2.6 and 5.2.7 are performed once for each failure mode. The sample procedure for analyzing each failure mode is as follows:

5.3.1 Select part or interface circuit for analysis.

5.3.2 Identify item R1, C1, C2, or J05 pin 1, etc.

5.3.3 Postulate a single failure, including mode of failure.

5.3.4 From knowledge of part/circuitry, identify a possible cause of failure.

5.3.5 From knowledge of circuit performance in the presence of the postulated failure, assess the local effect.

5.3.6 Assess the failure effect at the next higher level and upward to the highest system level of interest, i.e., the mission.

5.3.7 Assign a severity category in accordance with definitions in paragraph 3.5.

5.3.8 Provide remarks on how the failure would be detected and what action could be taken to restore operation. If not detectable, so state.

5.3.9 Provide remarks on application of redundancy reconfiguration to workaround a failure, or any other relevant information.

5.4 FILLING OUT THE WORKSHEET

Figure 2 presents a sample worksheet form that is used to compile the results of the FMEA. Sample entries are included. Wording should be brief and clear. Acronyms and abbreviations may be used providing they appear on the space project’s acronym list. The Header Items are illustrated by

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

Figure 2, but an explanation is given below for each column entry. The following is the minimum information that should be entered.

5.4.1 Worksheet Line Item Information

Failure Mode Number - Unique identifier for each failure mode evaluated. Enter in numerical order.

Identification of Item/Function - For functional analysis, enter a concern description of the function performed. For a hardware analysis, enter unique identifier, i.e., nomenclature, drawing/schematic refe rence designator, or block diagram identifier. If possible, use identifiers that are consistent with program usage.

a. Failure Mode; b. Failure Cause - Identify the specific failure mode after considering the four basic failure conditions below:

1. Unscheduled operation.
2. Failure to operate when required.
3. Failure to cease operations when required.
4. Failure during operation.

For each application hardware failure mode, list the major cause(s), e.g., separated connector, capacitor short, capacitor open, resistor short to ground, resistor short to voltage.

Failure Effects - List failure effect for each of the hardware levels being considered. List in column by a, b, c, as below:

a. Local Level - Enter a brief description of the failure effect at the subdivision level being analyzed.

b. Next Higher Level - Enter the failure effect at the hardware level above the level of the analysis.

c. System or Mission Level - Enter the effect of the failure mode on the mission. (If the failure has no effect, enter none.)

Severity Category - Assign a severity category number (see paragraph 5.1.8 for definition).

SUBJECT:	PERFORMING A FAILURE MODE AND EFFECTS ANALYSIS	NUMBER: P-302-720 REV. : Original

5.0 INSTRUCTIONS (cont.)

Remarks - Enter any pertinent information, references or comments. Specifically enter:

a. How the failure would be detected in the data.

b. Redundant or work around features of the design.

5.5 THE FMEA REPORT

Preliminary or interim reports are usually made available for each design review. An analysis of the system at the functional level should be ready for the Preliminary Design Review. Interim reports should contain all failure modes and identified problem areas with the proposed corrective actions.

Following are the major topics covered in the final report:

a. Detailed description of system with reliability block diagrams.

b. The indentured levels analyzed.

c. Summary of the results.

d. Summary of ground rules and assumptions.

e. Identification and discussion of the failure modes that are potential problem areas.

f. List of items exempted from the FMEA a nd the rationale for exemption.

g. Worksheets arranged from system level to the lowest unit analyzed

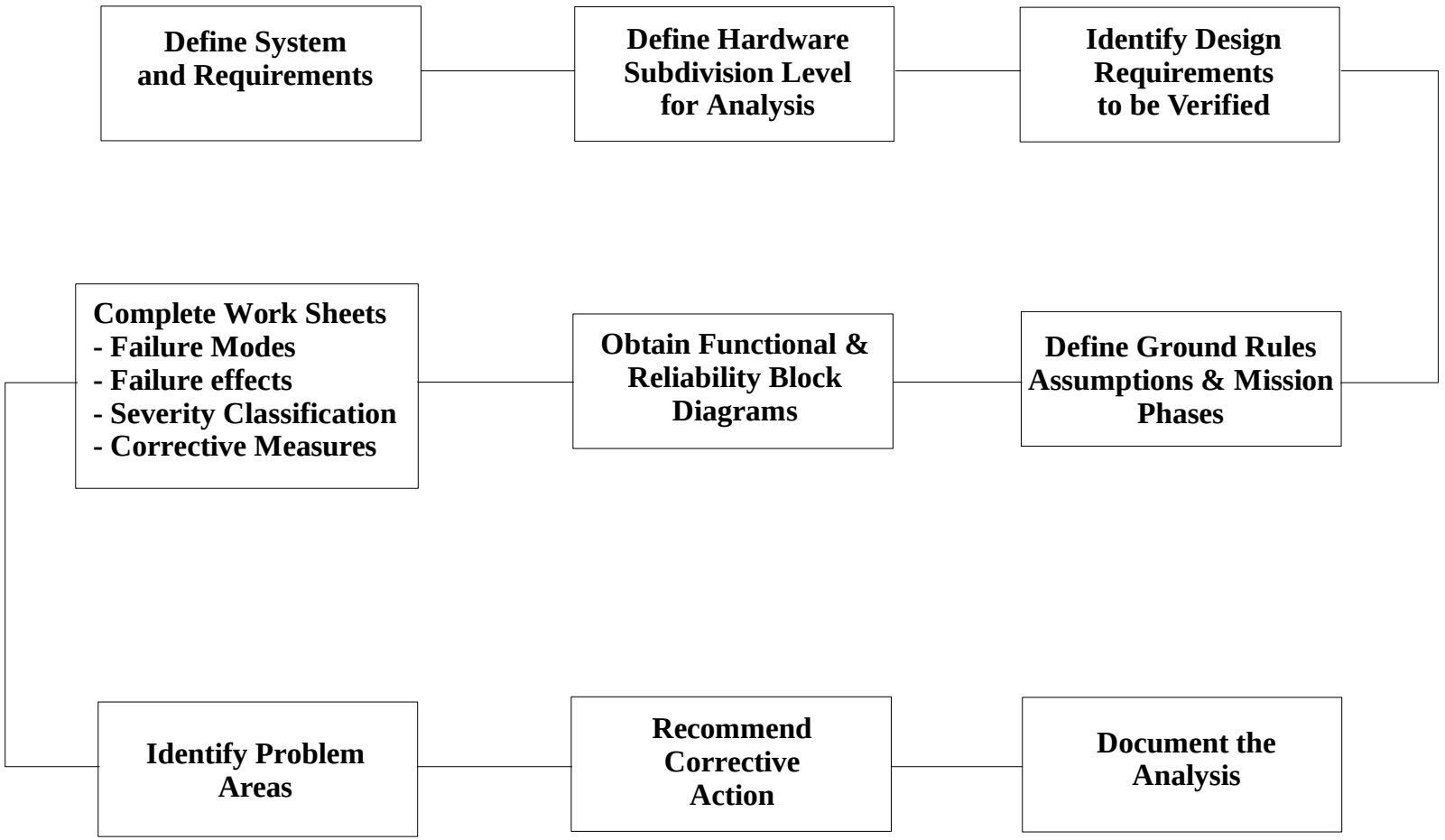

Figure 1. FMEA Flow Diagram

Figure 2. FAILURE MODE AND EFFECTS ANALYSIS

Mission DTF - 1
System FTS
Subsystem/Instrument 3.13
Component Wrist Actuator
Mission Phase Orbit

Date 8-10-96
Prepared by Ron Smith
Approved by RHB

Failure Mode Number	Identification of Item or Function	a. Failure Mode b. Failure cause	Failure Effects a. Local or Subsystem b Next Higher Level - System c. End Effect - Mission	Severity Category	Remarks a. Failure Detection Method b. Compensating Features/Action c. Other
3.13.6	Wrist actuator, roll provides motion in roll (x) axis	a. Loss of motor control b. Part failure in motor drive circuit	a. Loss of wrist roll motion and torque b. Cannot continue FTS task and mission c. None at Orbiter mission	2R	a. Position sensor & torque sensor displayed at DAC b. Backup hardware to put arm in safe position. Good arm can put arm in safe position.