Work Instruction

Failure Modes and Effects Analysis (FMEA), Critical Items List (CIL), and Fault Tree Analysis (FTA)

Approved by:

_____

Gary G. Kelm., Chief
Program and Project Assurance Division

NASA - Glenn Research Center
Cleveland, OH 44135

Point of Contact: Jose A. Cruz/(216) 433-3122

Change Record

Rev.	Effective Date	Description
Basic	Dec. 3, 1998	Initial Issue
A	Aug 27, 1999	CR006: Add quality records section, clarification of approval process, technical corrections, add definitions/acronyms, update organizational names, additional info for tools & training
B	Feb. 11, 2000	CR026: Change 6.6, 6.7 and add Table 1 to add criticality numbers
	May 15, 2006	Document Review by P.O.C. no changes required - document updated to reflect organizational names plus new AFS numbering. Rev. change not required.
C	Aug 3, 2008	CR 130: This revision adds interim reviews of analyses by members of an IPT that is defined as containing disciplines such as Systems Engineering, Risk Management, System Safety, and Probabilistic Risk Assessment (PRA). The process flow charts were revised and the explanation for process steps was expanded. Flow-down of requirements from NPRs is incorporated. Change title from Failure Modes, Effects and Criticality/Fault Tree Analyses. Confirm document number change from GRC-W0510.060.
D	Apr. 13, 2010	CR148: Replace Space Assurance Requirements and Guidelines (GLM-QE-8700.2) with Space Assurance Requirements (GLPR 7120.5.30).

1.0 PURPOSE

To define a process at Glenn Research Center for performing Failure Modes and Effects Analysis (FMEA), developing the Critical Items List (CIL), and Fault Tree Analysis. These analyses are applied as required by NASA Programs and Projects. These analyses identify failure modes and faults in hardware for flight projects at Glenn Research Center.

2.0 REFERENCES

Document Number	Document Title
NPR 7120.5	NASA Space Flight Program and Project Management Requirements
NPD 8700.1	NASA Policy for Safety and Mission Success
NPD 8720.1	NASA Reliability and Maintainability (R&M) Program Policy
NASA-STD-8729.1	Planning, Developing, and Managing an Effective Reliability and Maintainability Program
NPR 8000.4	Agency Risk Management Procedural Requirements
NPR 8705.5	Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
NPR 8715.3	NASA General Safety Program Requirements
NASA/SP-2007-6105	NASA Systems Engineering Handbook
n/a	NASA Fault Tree Handbook with Aerospace Applications
GLPR 8700.4	Product Assurance
GLP-QE-8700.1	Roles, Responsibilities and Interrelationships of SMAD/SSQRD Support to GRC Programs/Projects
GLM-QE-8700.1	Product Assurance Manual
GLPR 7120.5.30	Space Assurance Requirements
CxP 70043	Constellation Program Hardware Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL) Methodology

2.1 Quality Records and Forms

The Failure Modes and Effects Analysis (FMEA), Critical Items List (CIL), and Fault Tree Analysis reports are the responsibilities of the P/P/S and become part of the P/P/S Configuration Management System. However, analysis reports written by Program and Project Assurance Division will be archived in the PPAD office archive.

2.2 Definitions and Acronyms

FMEA	Failure Modes and Effects Analysis (FMEA) - Study of a system and the working relationships of its elements to determine ways in which failure can occur (failure modes) and the effects of each potential failure on the system element in which it occurs, on other system elements, and on the

success of the system's mission.

(a) Hardware FMEA - A FMEA that is taken to the lowest hardware level required (typically the Line Replacement Unit [LRU]/component level) to identify all critical failure modes and their causes, in order to identify sufficient controls to minimize their probability of occurrence. Also, the term Hardware FMEA is sometimes used to indicate that a FMEA is mainly concerned with hardware, as opposed to Process FMEA's and Software FMEA's that are not.

(b) Functional FMEA - A higher-level FMEA that is done at the subsystem level and reports the failure modes that could result in loss of functions and the effects from those failures.

FTA	Fault Tree Analysis (FTA) can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety or reliability standpoint), and the system is then analyzed in the context of its environment and operation to find all realistic ways in which the undesired event (top event) can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, software errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, the top event of the fault tree.
GMIPs	Government Mandatory Inspection Points.
Item	An "Item" as documented in the Failure Modes and Effects Analysis worksheet refers to a particular hardware component, assembly, or device associated to a particular failure mode.
SMAD	Safety and Mission Assurance Directorate
IPT	Integrated Product Team: The Integrated Product Team is the team responsible for the Systems Engineering, hardware components design and selection, System Safety, Reliability and Maintainability, Probabilistic Risk Assessment, Risk Management, and Software Product Assurance (SPA) on the Program, Project, or Sub-project.
CSO	Chief Safety and Mission Assurance Officer
RAMEs	Reliability, Availability, and Maintainability Engineers
PM	Project Manager
P/P/S	Program/Project/Subproject
PPAD	Program and Project Assurance Division

3.0 SAFETY PRECAUTIONS

Not Applicable

4.0 TOOLS, EQUIPMENT AND MATERIALS

A sample FMEA/CIL worksheet (Excel spreadsheet) and/or Fault Tree should be available from PPAD Reliability & Maintainability. The spreadsheet format should be tailored to meet Program FMEA/CIL or FTA requirements.

Fault tree analysis computer programs are available from NASA or commercial sources.

5.0 PERSONNEL TRAINING AND/OR CERTIFICATION

NASA Professional Development Initiative Course SMA 511 - Failure Modes and Effects Analysis (FMEA)/Critical Items List (CIL).

NASA Safety Training Center Course: Design for (RAM) Reliability, Availability, and Maintainability.

6.0 INSTRUCTIONS – FMEA

6.1 **Define the Scope of the FMEA:** The P/P/S Systems Engineering and RAMEs agree upon whether the FMEA should be a detailed Hardware FMEA or a Functional FMEA. The P/P/S Systems Engineering defines the boundaries of the system to be analyzed.

6.2 **Develop Mission Timeline:** The P/P/S Systems Engineering provides an explanation of the mission, and mission phases. The best estimates are made for the duration of mission phases and planned operating times for subsystems. A timeline showing major mission events and environmental threats is developed.

6.3 **System Familiarization:** Design Description is acquired from the P/P/S Systems Engineering. The P/P/S develops the system documentation. This documentation describes the design and operation of the system and may consist of the Baseline Concept Document, a functional description, drawings, schematics, parts lists, materials, hardware map, specifications, and interface descriptions. The P/P/S determines the component interfaces. If sufficient documentation is not available to perform detailed failure mode analysis, the RAMEs interview the engineers supporting design for the P/P/S. They develop the best possible description that they can for the design based on interview notes.

6.4 **Develop Functional Flow Block Diagram (FFBD):** The RAMEs work with the P/P/S Systems Engineering to develop a functional flow block diagram. The P/P/S and RAMEs also trace the flow of energy and commands through the system.

6.5 **Develop Reliability Block Diagram**: The RAMEs work with the P/P/S Systems Engineering to develop the reliability block diagram. This provides a representation of the redundancy in the system and provides an important input to reliability prediction analysis as well.

6.6 **Review Hazards Analysis:** If a Hazard Analysis has been or is in the process of being developed it can be reviewed at this point as an aid to determining failure modes whose effects may impact safety. Even if a Hazard Analysis has not been developed design information and the reliability block diagram can be reviewed with system safety to assure mutual understanding of the system and its internal redundancy.

6.7 **Identify Failure Modes**: At the lowest level of system design required for the analysis (such as the line replaceable unit [LRU] level or component level) the P/P/S and RAMEs

identify the different ways in which the component may fail (possible and credible failure modes). Failure modes will be postulated after consideration of the following four basic failure conditions:

a) Premature operation
b) Failure to operate within specification or at a prescribed time
c) Failure during operation, including failure to contain or store energy or fluids
d) Failure to cease operation at a prescribed time

In addition, the P/P/S and RAMEs will consult the NASA Lessons Learned data base to identify experience based information that could lead to the identification of possible failure modes and effects that could have been unanticipated by the analyst.

6.8 **Identify Failure Mode Effects**: For each postulated failure mode, the P/P/S and RAMEs will describe the credible failure effects at the following indenture levels:

Immediate Effect - The failure effect on the item under analysis, the assembly it is associated with (if appropriate), and its interfaces.

Next Effect - The failure effects at the next higher assembly level, typically the subsystem/system.

End Effect - The failure effects at the integrated vehicle level, including effects on the mission and crew.

As a minimum, the worst case effect at these levels will be documented; however, it is recommended that the most likely effects also be documented.

6.9 **Assign Criticality to Failure Modes and Effects:** The P/P/S and RAMEs will assign a criticality category for each failure mode on the basis of worst-case potential failure effect, assuming the loss of all redundancy (where applicable). This worst case criticality is then annotated with the available design redundancy (if applicable) to yield the final criticality ranking. This will include possible catastrophic effects as well as the effects of loss of hardware functions. The criticality categories are defined as follows in Table 1.

6.10 **IPT Review:** The Preliminary FMEA is submitted for review by the **IPT.** This review enables the IPT to take the Failure Modes and Effects into account in the development of their designs and other analysis products. The IPT also reviews the failure modes and effects with respect to the **Requirement Screens** (Table 2). All items, except those determined to be criticality 3, will be assessed for compliance with the **requirement screens** on a PASS/FAIL basis. Any item which fails a screen or which does not meet fault tolerance requirements (two fault tolerant for criticality 1/1R items, or one fault tolerant for criticality 2/2R items) will be indicated as not meeting requirements.

6.11 **Review of IPT Comments:** The RAMEs review the recommended additions, corrections, and deletions. These are discussed with originators. The draft FMEA is revised as appropriate.

6.12 **Incorporate Changes:** As a result of IPT review, additions, deletions, and corrections are made to the FMEA.

6.13 **Complete all other FMEA worksheet data elements:** Consult Program requirements for specific FMEA worksheet data elements and complete remaining elements. (Examples may be Failure Detection method, Time-to-Detect, Time-to-Effect, Corrective Action, Ref. Designators, LRU identification, etc.)

6.14 **Submit FMEA to Review Board.**

6.15 **Is the analysis approved?** Yes: Go to 6.16. No: Review Failure Modes and Effects Analysis and make corrections to the analysis. Coordinate with IPT.

6.16 **Distribute Preliminary (and Approved) FMEA Report**.

6.17 **Go To 7.0: Procedure for Critical Items List (CIL).**

7.0 INSTRUCTIONS – CIL

7.1 **The RAMEs and Design Engineers review each failure mode** and criticality.

7.2 **Could the failure mode (should it occur) result in loss of life, vehicle, or mission?** (Y/N) If the answer is Yes, Go to Step 7.3. If the answer is No, then the failure mode does not go on the Critical Items List.

7.3 **Can the failure mode be designed out of the system?** (Y/N) If the answer is Yes, the failure mode is designed out. If the answer is No, then Go to Step 7.4.

7.4 **The failure mode is documented on a Critical Items List (CIL**) with all data elements as defined for the CIL items as per Program FMEA/CIL Requirements. Components and Systems Engineering, and other members of the IPT cooperate to develop the Retention Rationale. (Design Features, Operational Workarounds, Testing, Inspections, Flight History, and Maintainability, to show that the probability of occurrence for the worst case effect of the failure mode has been minimized.)

7.5 **The CIL is reviewed/checked by the IPT.**

7.6 **The RAMEs and Design Engineers review** IPT comments.

7.7 **The RAMEs and Design Engineers** make changes: Additions, Corrections, and deletions.

7.8 **The CIL is submitted to the Review board.**

7.9 **Is the CIL Approved?** If Yes: Go to 7.10. If No: Go to 7.3

7.10 **The CIL Returns to the IPT** for development of the Government Mandatory Inspection Points (GMIPs). All members of the IPT may be involved in developing the GMIPs but they shall be developed principally by the Design Engineering Groups.

7.11 **The GMIPs are submitted to the Review Board** for approval.

7.12 Are the GMIPs approved? If Yes, Go to 7.13. If No, then Go to 7.10.

7.13 The RAMEs and P/P/S publish the FMEA/CIL and GMIPs Report. The P/P/S writes the preliminary report.

7.14 The Report is sent to the P/P/S and PPAD Report Archives.

8.0 INSTRUCTIONS – FTA

8.1 **Define Application:** The P/P/S and RAMEs define the application for the Fault Tree Analysis. In this step, it is decided if the analysis is intended to be applied as a safety assessment (hazard analysis), or as a reliability analysis (such as a comparison for alternative design concepts). In this step it will become apparent if the analysis is to be qualitative only (to better understand the casual relationships between possible faults and conditions) or if it must also encompass quantification (estimates of probability and uncertainties).

8.2 **Define Top Level Event or Events:** The P/P/S and RAMEs define the Top-Level Event (or Events) for the Fault Tree. (Examples: Loss of Crew (LOC), Loss of Mission (LOM), Loss of Vehicle (LOV), Loss of Science (LOS) or other events.)

8.3 **Determine System Boundary:** The P/P/S defines the boundaries of the system to be analyzed and the relevant interfaces that should be considered.

8.4 **Develop Mission Timeline and Environment:** The P/P/S defines the mission phases, the major events within mission phases, and estimates the duration of mission phases. A separate Fault Tree may need to be developed for various mission phases depending upon the mission events possible in that phase and the environment. In this step, the analyst must also determine the environment that the system under analysis will be subjected to.

8.5 **System Familiarization:** Design Description is acquired from the P/P/S Systems Engineering. The P/P/S develops the system documentation. This documentation describes the design and operation of the system and may consist of the Baseline Concept Document, a functional description, drawings, schematics, parts lists, materials, hardware map, specifications, and interface descriptions. The P/P/S determines the component interfaces. If sufficient documentation is not available to perform a fault tree analysis, the RAMEs interview the engineers supporting design for the P/P/S. They develop the best possible description that they can for the design based on interview notes.

8.6 **Review HA, FMEA/CIL, and RBD analysis:** If a hazard analysis (HA), FMEA, CIL, or reliability block diagram (RBD) reliability analysis has already been performed for the system, it should be reviewed.

8.7 **Construct FFBD:** The RAMEs work with the P/P/S Systems Engineering to develop a functional flow block diagram (FFBD). The P/P/S and RAMEs also trace the flow of energy and commands through the system.

8.8 **Determine Intermediate Events and Logic:** Immediately below the top-level event, the analysts (RAMEs or RAMEs with P/P/S) will determine the set of events which when occurring alone or in combination are necessary and sufficient to bring about the occurrence of the Top Level Event. The logic (OR gate or AND gate) will follow.

8.9 **Analyze to Lowest Level:** The analysis is continued for each intermediate event using the same process in 8.8 above extending to the lowest level of the Fault Tree. The lowest level of analysis may be determined by:

1. Extent of design and operational information available
2. Extent of information available on failure or fault possibilities
3. Up-front decision by P/P/S and RAMEs on admissible complexity of analysis
4. Probability Cut-Off: Events with probability of occurrence that falls below a specified threshold are neglected

8.10 **IPT Review:** The Fault Tree is submitted for review by the **IPT.** This review enables the IPT to take the Fault Tree into account in the development of their designs and other analysis products. The IPT also reviews the Fault Tree with respect to the design to determine if additions, corrections, or deletions are recommended.

8.11 **Review IPT Comments:** The RAMEs review the recommended additions, corrections, and deletions. These are discussed with originators. The draft Fault Tree is revised as appropriate.

8.12 **Implement Changes:** The draft Fault Tree is revised as appropriate.

8.13 **Check the Fault Tree:** All events and Logic gates are checked to be sure that all changes have been correctly made.

8.14 **Submit to Review Board.**

8.15 **Is the Fault Tree approved?** If Yes: Go to 8.16. If No: Go to 8.10.

8.16 **Distribute Preliminary Report.**

8.17 **Go To Procedure for Quantification.**

Procedure for Quantification

8.18 **Is Quantification Required? (Y/N)** If Yes: Go to 8.19, If No: Go to 8.30

8.19 **Data Search:** RAMEs and P/P/S engineers develop a list of basic events and conduct a data search for frequency data or probability of occurrence on these basic events. For unique devices or first time designs, the first priority should be to acquire data that is based upon heritage if possible, otherwise surrogate data may be used. (Preferred order of data selection: 1.) Very similar design and similar mission, 2.) Very similar design under test conditions, 3.) Similar equipment field data or test data from manufacturers, 4.) Expert elicitation based on an understanding of the functionality and failure mode, 5.) Reliability handbook data.)

8.20 **Estimate Input Data Uncertainties:** Occurrence data for basic events is statistically analyzed by the RAMEs with inputs from the P/P/S. This analysis should result in:

1. Assigning a time dependent distribution to the basic event
2. Estimates of the distribution parameters
3. Estimates of the uncertainty in the distribution parameters

Note: Judgment may have to be exercised here because the nature and quality of the data may not allow a statistical determination of (1), (2), and (3) above. Thus, some engineering judgment and/or expert opinion may have to be used.

8.21 **Review of Data by Engineering and/or Technology Experts:** Occurrence rate data for basic events is reviewed by project engineers and/or technology experts at this stage of the analysis.

8.22 **Data and Uncertainty Adjustments:** Due to experience based real-world knowledge, it may be necessary to adjust some of the occurrence rates. This is a valid adjustment (change of values) because it is based on experience and engineering judgment.

8.23 **INPUT to Fault Tree: Data and Uncertainty for Basic Events.**

8.24 **Cut Sets, Probabilities, Importance Measures, and Uncertainty in probability of occurrence for Top-Level Event are computed.**

8.25 **IPT Review:** The results of the Quantitative analysis are submitted for review by the **IPT.** This review enables the IPT to take the quantitative Fault Tree Analysis results into account in the development of the designs and other analysis products. The IPT also reviews the results with respect to the design to determine if additions, corrections, or deletions are recommended in the data.

8.26 **Review IPT Comments:** The RAMEs review the recommended additions, corrections, and deletions. These are discussed with originators.

8.27 **Implement Changes:** The Fault Tree analysis is revised as appropriate.

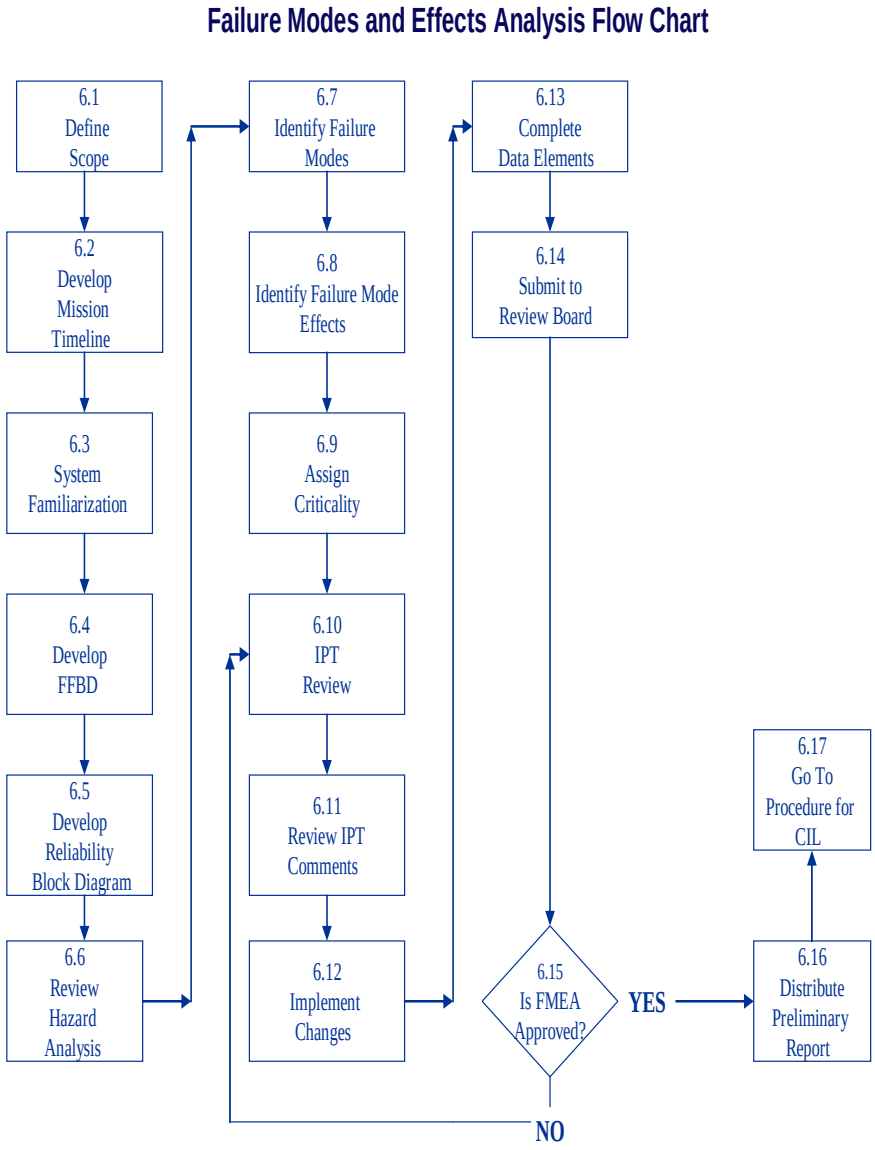
8.28 **Prepare Results and Submit for Review at Board.**

8.29 **Is FTA Approved? Y/N. If YES, Go to 8.30. If NO, Go to 8.25.**

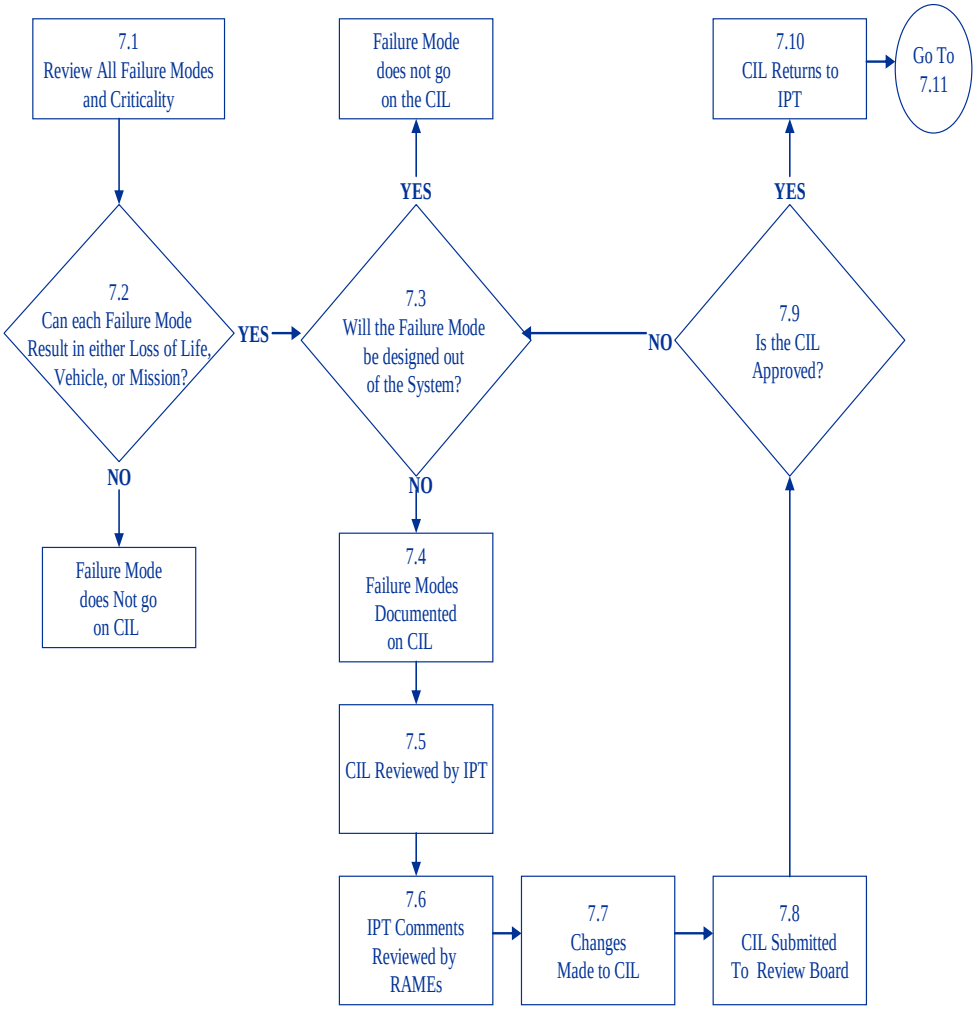
8.30 **Write Fault Tree Report and Publish.**

8.31 **Send Fault Tree Report to P/P/S and PPAD Archives.**

FLOW DIAGRAMS

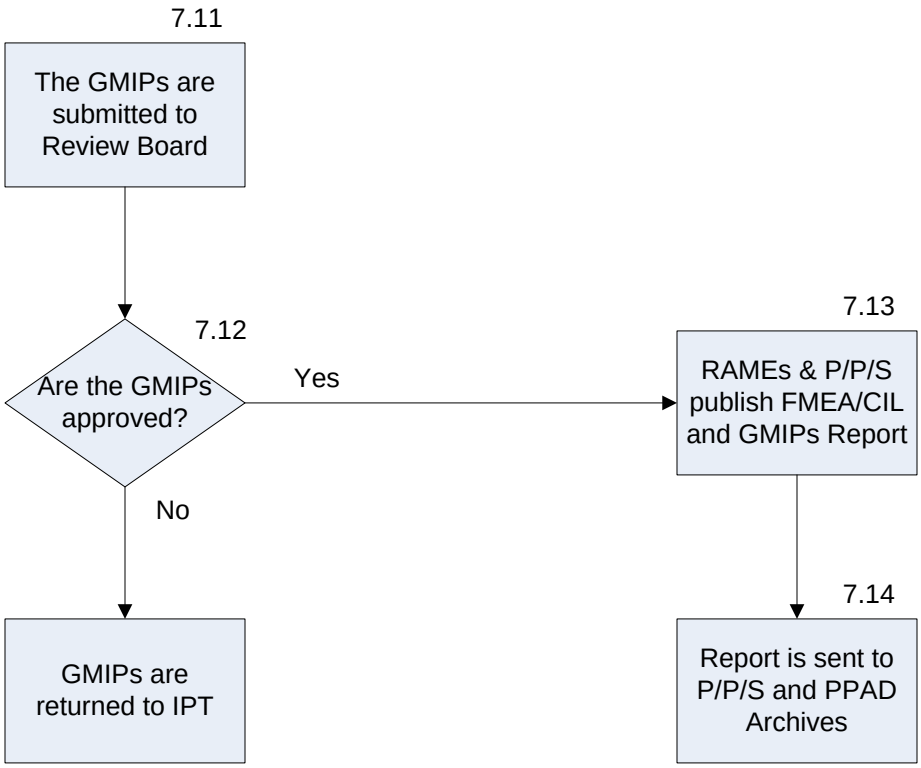


Critical Items List Flow Chart



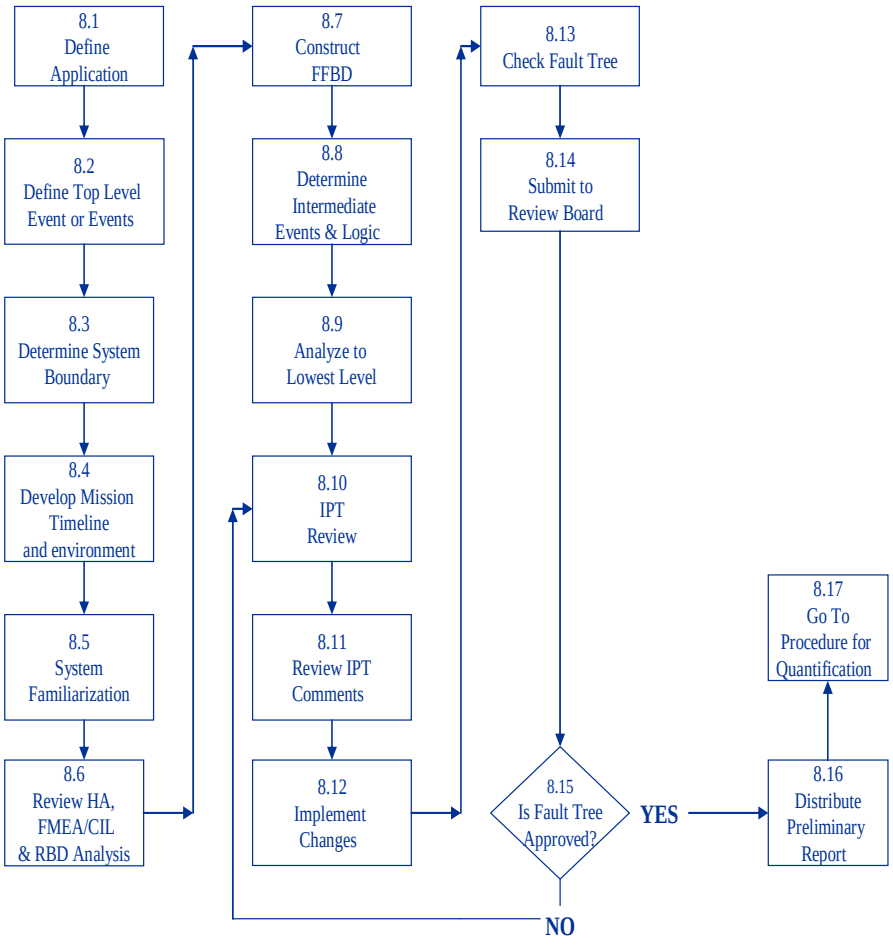
2

Critical Items List Flow Chart (Continued)



3

Fault Tree Analysis Flow Chart



4

Fault Tree Analysis Flow Chart (Continued)

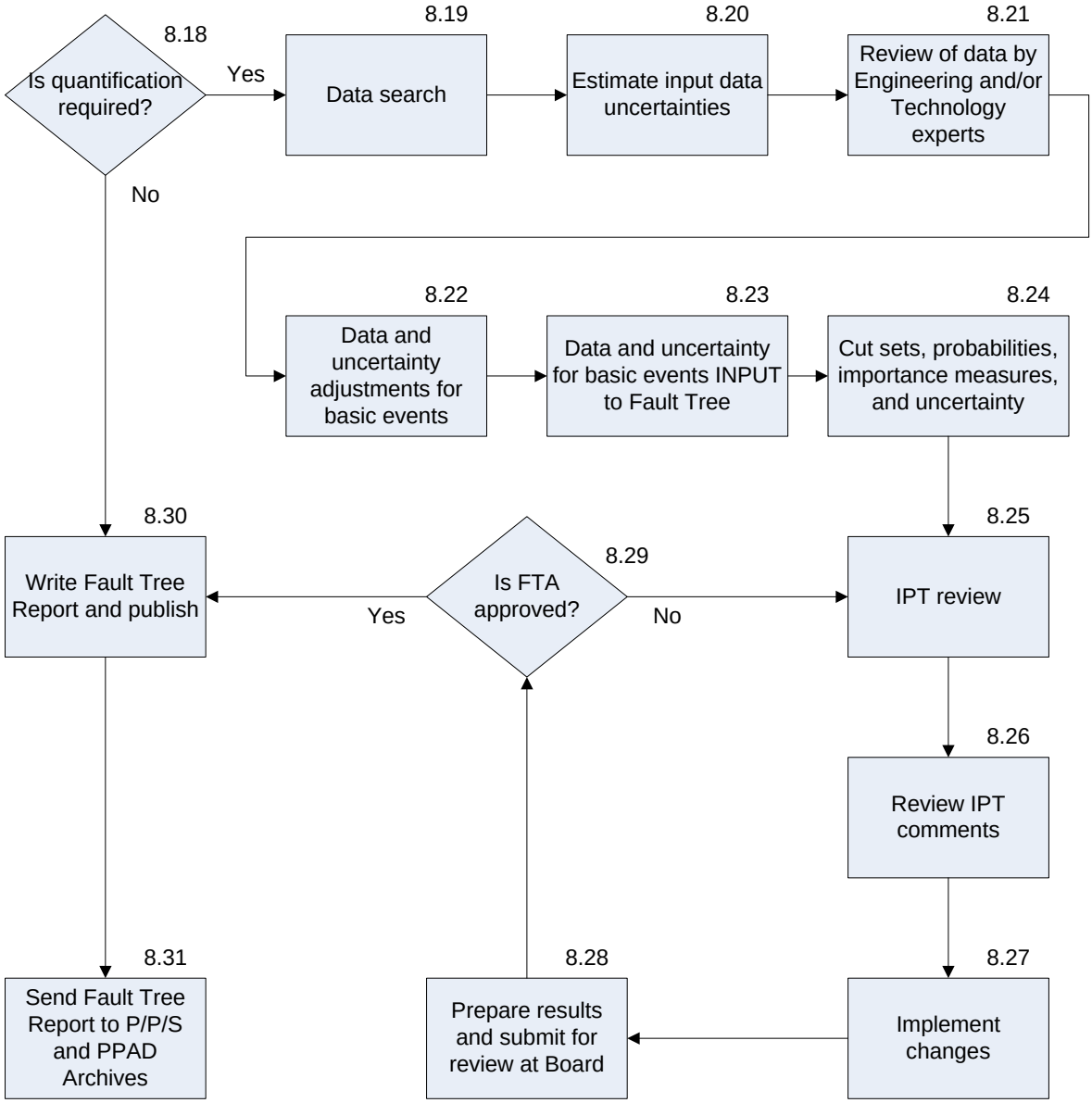


Table 1: Failure Mode Criticality Categories

Criticality	Criticality Definition
1	Single failure that could result in loss of life or vehicle.
2	Single failure that could result in a loss of mission.
1R#	Redundant hardware item, which if all failed, could cause loss of life or vehicle. A number is used to indicate the number of redundant paths or strings (e.g. 1R3 – a triple redundant item).
1S	Failure in a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous condition, potentially resulting in loss of life or vehicle.
2R	Redundant hardware items, which if all failed, could cause a loss of mission.
3	All other failures.

Table 2: Requirement Screens

Screen	Screen Definition (Answers: Yes= Pass, No=Fail)
A	Is the Item capable of being functionally verified during normal ground processing?
B1	Is the failure mode under analysis detectable by flight and ground crew?
B2	If the criticality of the failure mode under analysis is higher than 3, can the system isolate the failure and provide recovery?
C	Can a single failure result in the loss of redundant functions? (For example, consider loss of a function receiving power from two independent power sources through redundant wire harnesses connected by a single connector so that failure of the connector would result in loss of the function.)