



**GODDARD TECHNICAL
HANDBOOK**

**Goddard Space Flight Center
Greenbelt, MD 20771**

GSFC-HDBK-8004

**Approved: 08-20-2024
Revalidation Date: 08-20-2029**

**GUIDELINE FOR FAILURE MODES AND EFFECTS ANALYSIS
AND RISK ASSESSMENT**

**THIS STANDARD HAS BEEN REVIEWED FOR EXPORT CONTROL RESTRICTIONS;
APPROVED FOR PUBLIC RELEASE
DISTRIBUTION IS UNLIMITED**

Prepared By:

**Nancy
Lindsey**

Digitally signed by Nancy
Lindsey
Date: 2024.07.22
11:02:20 -04'00'

Nancy J. Lindsey
Subject Matter Expert, Reliability
Maintainability, and Availability (Code 370)
NASA Goddard Space Flight Center

Endorsed By:

**Charles
Knapp**

Digitally signed by
Charles Knapp
Date: 2024.07.29
15:17:33 -04'00'

Charles Knapp
Branch Head, Reliability Maintainability,
and Availability Assessment (Code 371)
NASA Goddard Space Flight Center

Approved By:

**TRISTRAM
HYDE**

Digitally signed by
TRISTRAM HYDE
Date: 2024.08.09
13:35:42 -04'00'

Tristram T. Hyde
Chief Engineer
NASA Goddard Space Flight Center

Maria Nowak

Digitally signed by Maria
Nowak
Date: 2024.08.14
11:34:57 -04'00'

Thomas V. McCarthy
Director of Engineering and Technology
NASA Goddard Space Flight Center

**DEIRDRE
HEALEY**

Digitally signed by
DEIRDRE HEALEY
Date: 2024.08.20
10:19:08 -04'00'

Deirdre Healey
Director of Safety and Mission Assurance
NASA Goddard Space Flight Center

NASA GODDARD SPACE FLIGHT CENTER
Greenbelt, Maryland 20771

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Baseline	-	08-20-2024	Initial Release

FOREWORD

This handbook is published by the Goddard Space Flight Center (GSFC) to provide uniform engineering and technical implementation guidance for processes, procedures, practices, and methods that have been endorsed as standard for NASA programs and projects, including mission assurance methodologies.

This handbook defines a consistent approach for performing Failure Mode, Effects, and Criticality Analysis (FMECA) on GSFC missions for risk assessment.

Requests for information, corrections, or additions to this handbook should be submitted via “Contact Us” on the GSFC Technical Standards website at <http://standards.gsfc.nasa.gov>.

Michael
Viens

Digitally signed by
Michael Viens
Date: 2024.07.29
13:22:32 -04'00'

Michael J. Viens
Technical Standard Program Manager
NASA Goddard Space Flight Center

TABLE OF CONTENTS

SECTION	PAGE
DOCUMENT HISTORY LOG	3
FOREWORD	4
TABLE OF CONTENTS.....	5
LIST OF FIGURES	6
LIST OF TABLES.....	6
1. SCOPE	7
1.1 Purpose	7
1.2 Applicability	7
1.3 Safety.....	8
2. APPLICABLE DOCUMENTS.....	8
2.1 General	8
2.2 Order of Precedence.....	8
3. ACRONYMS AND DEFINITIONS.....	9
3.1 Acronyms and Abbreviations.....	9
3.2 Definitions.....	9
4. Failure Mode, Effects, and Criticality Analysis (FMECA).....	12
4.1 General	12
4.2 Roles and Responsibilities	14
4.3 Analysis Methodology	18
4.3.1 FMECA Approaches.....	18
4.3.2 Failure Mode Analysis.....	19
4.3.3 Critical Item and SPF Identification	34
4.3.4 Common Cause Susceptibility Identification	35
4.3.5 Risk Assessment	37
4.4 Data Incorporation.....	38
4.4.1 Legacy Analysis.....	40
5. COMMUNICATION, MONITORING, AND REPORTING	43
5.1 Communication/Monitoring.....	43
5.2 Reporting.....	47
APPENDIX A – RECOMMENDED RELIABILITY PROGRAM PLAN WORDING.....	49
APPENDIX B – FAILURE RISK CONTROL PLANS	50
APPENDIX C – FMECA CREDIBILITY DETERMINATION ASSISTANT	54

LIST OF FIGURES

FIGURE	PAGE
Figure 1 - FMECA Process and Data Flow Diagram	17
Figure 2 - FMECA Worksheet Example	24
Figure 3 - Failure Mode Cause Identification Process Example	27
Figure 4 - FMECA Causal Data Capturing from Legacy/Subordinate FMECAs	29
Figure 5 - FMECA Effect Correlation from Superior FMECAs and Additional Sources.....	30
Figure 6 - Occurrence Value Documentation Formatting Examples.....	31
Figure 7 - FMECA Effect D/P Capturing from Legacy/Subordinate FMECAs	32
Figure 8 - CIL and SPF Table Templates	36
Figure 9 – Example of Common Cause Susceptibility Table for Risk Generation	37
Figure 10 - Summary Failure Modes, Effects and Criticality Analysis Worksheet Example	42
Figure 11 - Threat Criticality Matrices	44
Figure 12 - RPN Criticality Matrices.....	45
Figure 13 - D/P Criticality Matrices	45
Figure 14 - D/P Matrix.....	46

LIST OF TABLES

TABLE	PAGE
Table 1: GSFC FMECA Risk Priority Number (RPN) Table	23
Table 2: Potential Data Incorporation Flows	39

1. SCOPE

1.1 Purpose

This handbook provides a uniform approach for performing Failure Mode, Effects, and Criticality Analysis (FMECA) concurrently with development efforts as a living risk assessment document for GSFC missions and infrastructure. It also conveys methods for updating of FMECAs as designs, materials, operational parameters, processes, and operations are refined or additional knowledge is attained.

FMECA is an inductive analysis performed to identify failure modes and their likelihood, effects, and mitigations throughout a system's life and provides the following project benefits:

- Identifies where there is the potential for irreversible physical and/or functional damage/change (locally and globally) or risk within a system.
- Assesses risk/impact of a failure and creates a composite picture of the system's susceptibilities, including Single Point Failures (SPFs), Critical Items (CIs), propagation risks, and mitigation effectiveness.
- Assists with Fault Detection, Isolation, and Recovery (FDIR) design definition and sufficiency evaluation.
- Identifies the need for and recommends/verifies recovery/mitigation strategies (e.g., safing, exception handling, FDIR).
- Verifies predictive monitoring (or detection) designs/strategies.
- Verifies redundancy (switching/independence/cross-strapping) effectiveness and robustness.
- Supports design trades, testing, and operations planning.
- Provides testing and operations anomaly diagnosis and recovery data.

A proper FMECA greatly reduces the risk of a failure impacting mission success and/or inducing lengthy downtimes in test/operations. It also enables designers and system stakeholders to adjust hardware/software designs, operations, and maintenance; prepare for exigency operations; and extend or modify operational concepts with confidence while optimizing fault tolerance and system sustainment.

1.2 Applicability

The guidance set forth in this document provides the baseline approach for FMECAs on all missions, infrastructure, spacecraft, instruments, ground systems, systems, subsystems, and components developed by, contracted by, or manufactured by GSFC and/or any subsidiary entity/organization.

This handbook may be cited in contract, program, project, and other Agency documents to provide technical guidance. This handbook was developed mainly with the intent of improving the reliability of flight systems. It can be tailored to be as quantitative as necessary ([4.3.2.3 - likelihood subsection](#)).

1.3 Safety

Failure modes identified as affecting safety should be reported to the cognizant project safety manager for inclusion in the appropriate safety analysis.

2. APPLICABLE DOCUMENTS

2.1 General

Documents listed in this section contain provisions that constitute underlying requirements related to the implementation guidance provided in this handbook. When imposed, it is expected that the latest issuances of the cited documents will be used unless otherwise approved by the applicable Technical Authority. The applicable documents are accessible via the NASA Technical Standards System at <http://standards.nasa.gov>, directly from the standards developing organizations, or from other document distributors.

GPR 7120.4	Goddard Procedural Requirements (GPR) for Risk Management
GPR 8705.4	Risk Classification Guidelines and Risk-Based SMA Practices GSFC Payloads and Systems
N/A	GSFC Single Point Failure (SPF) Policy
SAE J1739	Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery (Machinery FMEA)
NPR 8000.4	Agency Risk Management Procedural Requirements
NASA-STD-8729.1	Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems
MIL-STD 1629	Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis

2.2 Order of Precedence

When applied internally or imposed by contract on a program or project, the technical requirements in NASA and GSFC directives (or other requirements documents) take precedence over implementation guidance provided in this handbook.

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

CDR	Critical Design Review
CI	Critical Item
CIL	Critical Items List
CSO	Chief Safety and Mission Assurance Officer
D/P	Detection/Prevention
DNH	Do No Harm
FDIR	Fault Detection, Isolation, and Recovery
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
GOLD	Goddard Open Learning Design
GSFC	Goddard Space Flight Center
GPR	GSFC Procedural Requirement
HDBK	Handbook
I&T	Integration & Test
LRU	Line Replaceable Unit
MOA	Mission Operations Assurance
NPR	NASA Procedural Requirement
ORR	Operational Readiness Review
ORU	Operational Replaceable Unit
PDR	Preliminary Design Review
P _f	Probability of Failure
PSA	Part Stress Analysis
R&M	Reliability and Maintainability
RPN	Risk Priority Number
SEEA	Single Event and Effects Analysis
SPF	Single Point Failure
STD	Standard
SMA	Safety and Mission Assurance
TRL	Technical Readiness Level
TRR	Test Readiness Review
WCA	Worst Case Analysis
WI	Work Instruction

3.2 Definitions

Scope	The breadth of systems/processes considered in the analysis (e.g., observatory, spacecraft, instrument, subsystem, component, capture, launch).
-------	---

Common Cause Failure	Multiple failures, damage, or potential latent defects that have the same origin, where the origin is a single or repeated external event, this includes impact, vibration, temperature, contaminants, miscalibration, improper workmanship/manufacturing, maintenance, radiation, Electromagnetic Interference (EMI), Micrometeoroid and Orbital Debris (MMOD), etc.
Common Mode Failures	Failures that are inherent in the design of the system/process that can occur in any identical instantiation at that can occur simultaneously or at different times because of a design issue or defect.
Credible	Failure modes that represent a <i>plausible risk</i> or have likelihood of failure greater than 0.1% ($P_F > 0.001$ or occurrence rating = 1-5) per 300-PG-7120.4.2.
Criticality Rating	A relative measure of risk from Very, Very Low to Very High (0-5) derived for each failure mode's technical consequence (derived from failure severity/type), likelihood of occurrence, and Detection/Prevention (D/P) provisions.
Critical Item (CI)	Items (parts, components, units, logic, procedures, etc.) that have a failure mode that is assessed with having failure type labels of 1, 1SC, 2S or 2 (See Table 1).
Design Maturity	The level to which the concept of an object, code, or process has solidified and has proven its ability to meet performance expectations. See also NASA TRL levels
Detection	Means or methods by which a failure mode can be discovered [or symptoms/signatures that would trigger mitigations or action (flight operations, software, hardware, etc.); captured in the FMECA as part of D/P value/rating and description.
Detection/Prevention Value	A quantitative criticality rating of the identified detection/prevention provision, ranging from 1 to 5.
Failure Effect	The consequence(s) a failure mode has on the operation, function, or status of an item. Failure effects should consider redundancy and are classified at the local, next higher, and system levels.
Failure Cause	The physical or chemical processes, design (hardware or software) defects/features, quality defects, part misapplication, or other processes that are the basic reason for failure, or that initiate the mechanism that proceeds to failure.
Failure Mechanism	The means (e.g., open, short) through which the failure induces the failure mode.
Failure Mode	The manner (or observable state) of failure or undesired outcome that occurs within a system or operation.
Failure Type	The classification (e.g., Critical and SPF, Critical, Significant, Minor) and qualitative label (e.g., 1, 1SC, 2S, 2, 3, 4, 4T, and 5) assigned to the failure mode based on the worst potential consequences resulting from the failure.
Indenture Level	The degree of system or process decomposition/hierarchy/segmentation (e.g., black box, first active component, piece-part, task) being analyzed (aka the depth of the analysis).

Mission Success	The achievement of a system's/process' desired purpose regardless of whether it is for a space-mission, support system, or infrastructure.
Mitigation	An action (e.g., impact lessening/preventative measure, FDIR, but not redundancy since that is already considered in consequence) taken to reduce the cause or effect of a failure mode; captured in the FMECA as the D/P rating and description.
Non-Credible	Failure modes that are <i>Highly Implausible</i> or have a likelihood of failure of less than or equal to 0.1% ($P_F \leq 0.001$ or Occurrence Rating = 0).
Occurrence Value	The probability or likelihood that a <u>failure mode and its effects</u> will transpire based on qualitative assessment, failure rate data, or test/performance data; captured in the FMECA as Likelihood of Occurrence Rating/Value.
Occurrence Rating	A quantitative criticality rating of the identified failure mode likelihood, ranging from 1 to 5, based on the occurrence value captured in the FMECA under Likelihood of Occurrence (Rating & Value).
Prevention	An action taken to reduce the likelihood of a failure mode/cause (e.g., preventative measure, fault avoidance); captured in the FMECA as part of D/P rating and description.
Retention Rationale	Justification for keeping a failure mode or item that includes information on mitigation steps taken/planned (e.g., design, tests, inspections) and their effectiveness, as well as mission need, design margins, and failure/operational history.
Risk	The combination of 1) the probability (qualitative or quantitative) that an organization will experience an undesired event such as cost overrun, schedule slippage, or failure to achieve a required outcome; and 2) the worst-case consequences or impact of the undesired event were it to occur.
Severity Value	A quantitative criticality rating of the identified failure mode severity, ranging from 1 to 5, based on failure type (e.g., 1 and 1SC are mapped to a rating of 5; 2S and 2 are mapped to a rating of 4; 3 is mapped to a rating of 3; 4 and 4T are mapped to a value of 2; and 5 is mapped to a value of 1).
Single Point Failure	The failure of an item (or cause of the failure of other dependent items) that would prevent achievement of required functionality of the system/process (failure types - 1SC and 1) and is not compensated for by redundancy, alternative operational procedure, or other means.
Subordinate Analysis	Analysis that provides source data for the FMECA. It can take the form of a vendor/legacy FMECA, a specific system, scenario, or lower indenture level FMECA, or other reliability or design analysis.
Success Criteria	The minimum set of measures that establish the accomplishment of predefined goals and objectives for a given activity or undertaking. Within the practice of risk management, it usually refers to the establishment of goals and objectives for risk mitigation activities.

4. FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS (FMECA)

4.1 General

Failure mode identification and risk assessment is begun during the design and development phases by reliability engineering (at GSFC) together with design engineering and software/parts engineering. A FMECA identifies system, component, part, or process failure modes that could lead to adverse consequences. The goal of the analysis is to determine how any single failure can impact a system's or any associated system's functionality and performance, while identifying likelihood, detection, mitigations, and causes. To provide the best value, a FMECA is best performed collaboratively in early design or conceptualization and is updated throughout a process/system's development and test/operations phases, reflecting the current performance, status, and operational usage of the process/system and its constituent pieces.

The FMEA/FMECA process (See [Figure 1](#)) and its resulting failure modes (with likelihood, causes, severity, effects, detection, and mitigation assessments), CI identification, and SPFs highlighting provide product insights and risks assessments that promote improved product robustness throughout its life by identifying:

- the potential for irreversible physical and/or functional damage;
- how/if damage/failures propagate;
- how damage/failures impact the system (locally and globally);
- the means available for failure detection, isolation, and compensation;
- the symptoms and causes of failure for anomaly investigation;
- predictive monitoring and redundancy strategy validity and viability;
- recovery strategies (determination and optimization of contingency operations and autonomous recovery/safing plans) prior to failures;
- the risk/effectiveness of corrective action implementation plans;
- the risks to mission success and safety architectures;

and inspiring concurrent/subsequent design/operations changes (e.g., predictive monitoring, exigency procedures, optimized FDIR). In addition, FMECA's support product operational robustness with anomaly diagnostic and recovery strategy data for the development/execution of corrective actions and increasing maintenance/servicing optimization.

A FMECA also assists in verification of the following requirements and objectives:

- GOLD Rules (GSFC-STD-1000):
 - 1.05: *Single point failures (SPF) items that prevent the ability to fully meet minimum mission success requirements shall be identified, and the risk associated with each shall be characterized, managed and tracked and the system trades necessary to determine the need and effectiveness of mitigation efforts (e.g., redundancy, selection of robust parts, etc.) commensurate with mission class shall be conducted and documented.*

- GPR 8705.4

Table 1 Follow guidance from NASA-STD-8729.1 for Class A – D. For Ground System: Focus on availability and maintainability of ground system from NASA-STD-8729.1 based on mission classification; For 7120.8 Follow guidance from NASA-STD-8729.1 for Class D; For Do No Harm (DNH) - Tall pole/criticality analysis guides focused reliable design efforts. Reliability analysis should help delineate between high value-added requirements and those that do not entail credible risk. Interface FMEA; For Hosted Payloads: Host practices and demonstrated reliability.

- NPR 8705.4

Goal: Fault tolerance and graceful degradation designed and implemented addressing all critical items or processes whose failure would result in failure to meet mission objectives, injury to personnel, or collateral damage.

Obj: The top-level objective of R&M activities in NASA support systems programs and projects is to ensure that systems perform as required over their lifecycles to satisfy mission objectives including safety, reliability, maintainability, and quality assurance requirements as defined in the references listed in Appendix D. Programs and projects are expected to address this objective by conducting analysis and testing activities and making the necessary design and operational choices to limit the likelihood of faults and failures, and to provide mitigation and restoration capabilities as needed to maintain an acceptable level of functionality considering those safety, performance, and reliability objectives. Accordingly, the top-level objective is decomposed into the following four subobjectives: The system conforms to the design intent (interfaces and/or functions) and performs as planned under nominal and failed conditions. The system and its elements remain functional for the intended lifetime, environment, operating conditions, and usage. The system is tolerant to faults, failures, and other anomalous internal and external events.

- NASA-STD-8729.1A:

2.A.2 System or its elements are not susceptible to common-cause failures, subobjective a: The system and its elements remain functional for the intended lifetime, environment, operating conditions, and usage.

3.A.1 System has multiple means of accomplishing functions that are critical to mission objectives including safety, subobjective a: Provide similar or dissimilar functional redundancy

*3.A.2 Separate redundant paths functionally and physically. subobjectives a-c: Separate redundant paths functionally and physically
Isolate and contain faults
Evaluate and control shortest path to worst-case effects (e.g., hazardous events)*

- 3.A.3 *System is able to recover from anomalies affecting functions that are important to top-level expectations, subobjective a:*
Provide fault management (detection, active isolation, recovery) capabilities
- 3.A.4 *System can degrade or lose functions without significantly impacting top-level expectations (through contingency operations), subobjective a:*
Plan contingency or other off nominal operations

4.2 Roles and Responsibilities

Development of FMECAs requires a detailed understanding of the parts/elements, components, systems, functions, and functional dependencies that are utilized within the system/process for operational success. FMECA development is a process (See [Figure 1](#)) of investigating potential failures, consequences, and proposed mitigations, which are refined/updated based on design/operations improvements made during or implemented based on the investigation. This process requires the involvement of not only all Product Design Leads (PDLs) but also Safety and Mission Assurance (SMA) personnel, systems engineering, and Integration and Test (I&T) project team members to ensure failure implications are understood and mitigations are implemented appropriately. It is important for these members of the project to have a good understanding of what items are associated with failure risks and knowledge of the item's management and risk control plan so that continuous risk management of failure risks is accomplished.

Roles and responsibilities are as follows:

Responsible Engineer (RE) [Reliability Engineer for GSFC analyses]:

- a. Has overall responsibility for the FMECA(s) (See [Appendix A](#) for recommended reliability program plan wording).
- b. Assesses or calculates likelihood of a failure mode being realized.
- c. Provides summary and itemized (worksheets) failure analysis results with failure modes, causes (direct or from subordinate FMECAs or other analyses), consequences, detection-signatures, mitigations, and FDIR-responses.
- d. Performs, integrates vendor/subordinate analyses, and documents the analysis.
- e. Communicates the risks (e.g., candidate risk statements, risk matrices) and recommendations (e.g., mitigations, testing, sensor optimization, redundancy, FDIR, operational changes) identified in the analysis.
- f. Provides CI and SPF identification with retention rationale and control information.
- g. Recommends actions for fault tolerance improvement and reanalysis update opportunities.
- h. Provides analysis results as inputs to safety, systems engineering, and other reliability analyses.
- i. Keeps the analysis, risks, and recommendations up to date with design, implementation (e.g., FDIR/mitigation verifications or nonverifications, build/integration variations from design), safing, compliance, testing issues/results, and performance/operational changes.

- j. Utilizes FMECA results when supporting operations/testing and anomaly examinations.

Design/Systems Team:

- a. Provides (and updates) the necessary design information (e.g., block diagrams, design elements, element functions, mechanical/circuit/code design, exception handling, safing/operational needs) and dependencies (e.g., data, mechanical, power, thermal) to the RE.
- b. Assists in the identification of failure modes, causes, consequences, detection-signatures, mitigations, and FDIR-responses.
- c. For items being life or performance tested, provides the test reports/data.
- d. Reviews and concurs with FMECA.
- e. Works with the RE to determine which failure mode, SPF, and CI risks should be formally proposed to/managed by the project risk management board.
- f. Uses analysis data and results to formulate tests and design/operational compensations to mitigate identified risks.
- g. Uses analysis data and results to diagnose and mitigate the consequences of issues that occur during operations and testing, while sharing issues with RE.
- h. Incorporates analysis results into any maintenance/refurbishment planning.

Chief Safety and Mission Assurance Officer (CSO) or Mission Operations Assurance (MOA):

- a. Reviews and concurs with the FMECAs.
- b. Shares vendor-provided FMECA deliverables with RE for use/incorporation and acceptability determination.
- c. Facilitates direct communication with FMECA providers, including vendor analysts.
- d. Ensures that processes are in place to facilitate and verify failure preventions and mitigations.
- e. Works with the RE to determine which failure mode, SPF, and/or CI, risks should be formally proposed to the project risk management board as risks.
- f. Uses analysis data and results to assist with quality/noncompliance disposition decisions (e.g., Use-As-Is) and ensures sharing of those decisions with RE.
- g. Uses analysis data and results to diagnose and mitigate the consequences of issues (including operational condition exceedances) in operations and testing, while ensuring those issues are shared with RE.

I&T Team:

- a. Uses analysis data and results to diagnose and mitigate the consequences of issues (including operational condition exceedances) in testing, while sharing issues with RE.
- b. Uses analysis data and results to formulate and prepare for tests by incorporating warnings, mitigations, and controls/monitors relative to failure mode consequence avoidance.

- c. Shares testing issues/results with the CSO and RE for potential FMECA updates.
- d. Incorporates analysis results into any maintenance/refurbishment planning.

Operations Team:

- a. Uses analysis data and results to diagnose and mitigate the consequences of issues during operations (including exceedances in usage or operational conditions), while sharing issues with RE.
- b. Uses analysis data and results to formulate and prepare for operations and contingency operations by incorporating warnings, mitigations, and/or controls/monitors relative to failure mode consequence avoidance.
- c. Shares operations issues/results with the CSO/MOA for potential RE FMECA updates.
- d. Incorporates analysis results into maintenance/refurbishment planning.

Quality Assurance:

- a. Assists with and verifies that processes/systems/hardware are generated and operated in accordance with designs/specifications, including pertinent conditions and parts/material inclusion, while sharing issues with RE.
- b. Identifies quality/noncompliance issues and makes disposition decisions (e.g., Use-As-Is) and shares those decision with RE.
- c. Uses analysis data and results to assist with quality/noncompliance disposition decisions (e.g., Use-As-Is).
- d. Uses analysis data and results to verify FDIR, detection, and mitigations provisions are implemented, as documented in the FMECAs.

Software Assurance:

- a. Assists with and verifies software is implemented and operated in accordance with designs/specifications, while sharing issues with RE.
- b. Identifies software quality/noncompliance or performance issues and makes disposition decisions (e.g., Use-As-Is) and shares those decision with RE.
- c. Uses analysis data and results to assist with quality/functionality noncompliance disposition decisions (e.g., Use-As-Is).
- d. Uses software failure mode criticality data to assist with and refine safety-critical software determination and assurance in accordance with NASA-HDBK-2203 and NASA-STD-8739.8.
- e. Uses analysis data and results to verify FDIR, exception handling, detection, and mitigations provisions are implemented, as documented in the FMECAs.

System Safety:

- a. Informs RE of the existence/addition of hazards, inhibits, controls so that updated mission success and inhibit failures (and inhibit configuration fault tolerance) can be assessed and characterized.

- b. Reviews and uses failure modes identified as affecting safety (Failure types – 1SC and 2S) for inclusion in appropriate safety analysis and procedural control development.

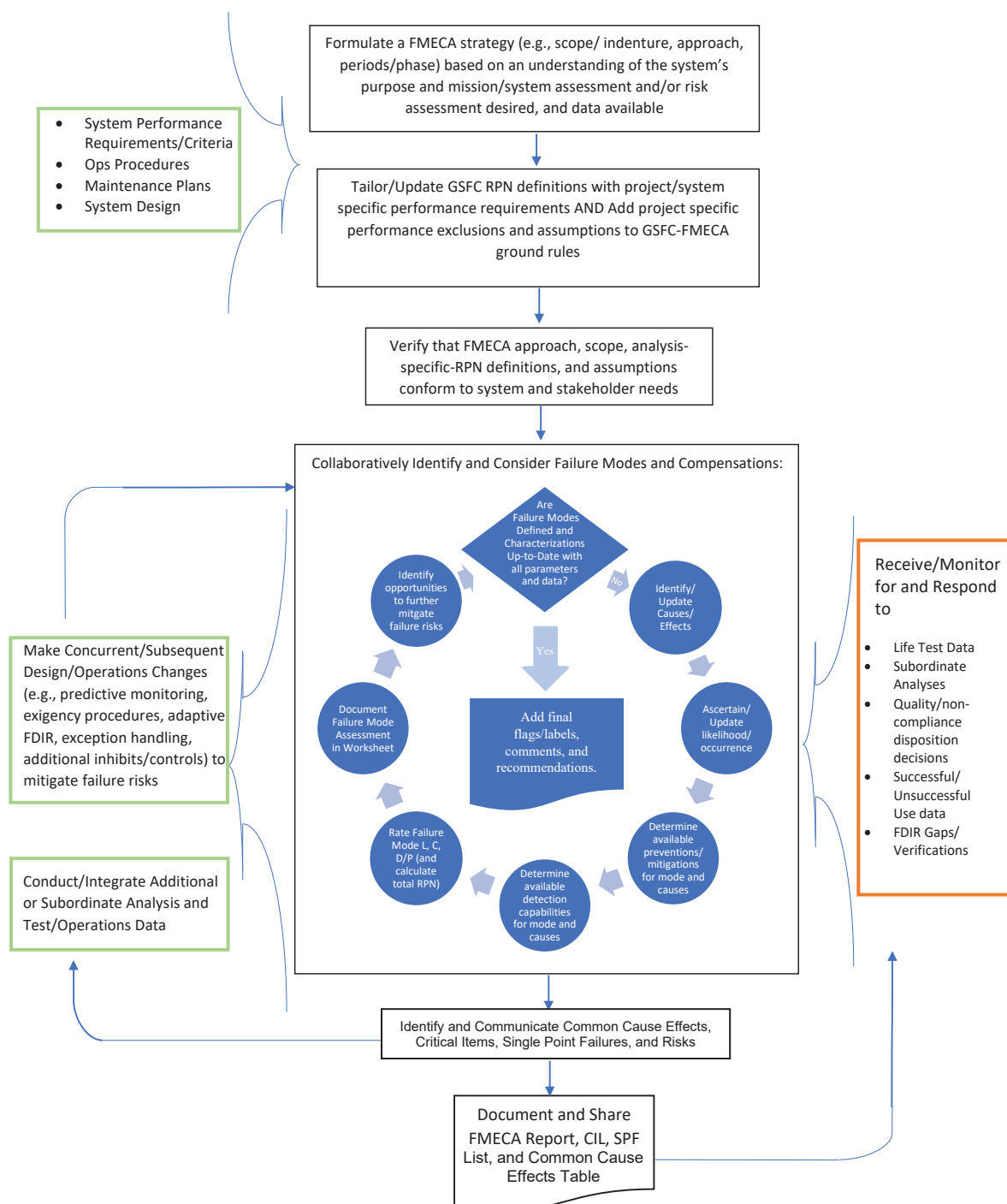


Figure 1 - FMECA Process and Data Flow Diagram
(Black Boxes – RE, Green Boxes Design/Systems/Ops Team, Orange Boxes – SMA Team)

4.3 Analysis Methodology

4.3.1 FMECA Approaches

There are five general approaches to FMECAs, which differ by mode-type and/or design-penetration that can be applied to hardware or software systems:

- (i) Functional (Usage) FMECA – An analysis of the loss, degradation, or erroneous performance of each system-element, that characterizes the impacts to itself up-through the system/mission, while identifying detection and mitigation provisions.
- (ii) Detailed (Design) FMECA – An analysis of the loss, degradation, or erroneous performance of each piece-part of a system-element that characterizes the impacts to itself up-through the system/mission, while identifying detection and mitigation provisions.
- (iii) Interface (Compatibility) FMECA – An analysis of the loss/degradation of required or expected interactions (e.g., mechanical, logical, power, data) of each system-element or erroneous interactions with coincident system-elements or support systems, that characterizes the impact to itself up-through the system/mission, including coincident systems, while identifying detection and mitigation provisions. This can be performed from the functional or piece/detailed part perspective to assess connection/ propagation risks and element/input/output compatibility.
- (iv) Process (Procedural) FMECA – An analysis of potential failure issues (including human error contributions) with each procedural (e.g., manufacturing, assembly, integration, maintenance/service, inspection) step or test/operational action/sequence, that characterizes the impact to itself up-through the system/mission while identifying detection and mitigation provisions, including human error controls.
- (v) Do No Harm (DNH) FMECA – An analysis of the loss/degradation of required or expected functionality or interactions (e.g., mechanical, logical, power, data, thermal, maintenance/service) of each system-element with coincident elements, that characterizes the impact to itself and looks for propagations/impacts to coincident-systems, while identifying detection and mitigation provisions. This can be performed from the functional, process, interface, or piece/detailed part perspective to assess propagation risks.

Desired assessment or risk determination, design maturity, variations in process or design complexity, and data availability will dictate the analysis type/scope that is used. In some cases, this may necessitate that the analysis be performed with combined approaches (e.g., interface and functional) to evaluate risks/failures effectively. In other cases, initial analysis findings or uncertainties may elicit or dictate the need for use of one of the other FMECA approaches or additional reliability analysis, to fully characterize risks. Additionally, if a legacy FMECA exists for the desired system/element/process that has the appropriate analysis type/scope it can be updated as described in [Section 4.4](#) ([and 5](#)).

To provide the best value, a FMECA is best performed as early in the design or conceptualization as possible but must have the appropriate data/design definitions to support the FMECA approach undertaken. Normally, there is sufficient data to perform functional, interface, or process FMECA's prior to Preliminary Design Review (PDR), while detailed FMECA's can be supported prior to Critical Design Review (CDR). Additionally, a FMECA provides continued fault-tolerance insights only if it is updated with design changes, operational changes (e.g., duty cycle, environment, movement, maintenance/refurbishment), test results (cause/mode additions or eliminations based on issues/verifications), and subordinate FMECA's or other reliability analysis (See [Section 4.4 and 5](#)).

4.3.2 Failure Mode Analysis

4.3.2.1 Formulate Failure Mode Analysis Strategy

Failure mode analysis (See [Figure 1](#)) begins with defining a FMECA strategy based on an understanding of the mission/system assessment and/or risk assessment desired.

FMECA strategies are established by the RE by selecting a FMECA approach (or approaches):

- (i) Functional (Usage) FMECA – Assesses system-robustness-to-failure (internal or externally induced) and mission success risks (and improves FDIR/exception handling).
- (ii) Detailed (Design) FMECA – Assesses detailed design-feature failures (internal or externally induced) for mission success risks and to identify design susceptibilities (and improves FDIR/exception handling).
- (iii) Interface (Compatibility) FMECA – Assesses system-to-system compatibility, safety, and failure propagation risks (and improves FDIR/exception handling).
- (iv) Process (Procedural) FMECA – Assesses production quality risks (defective/unreliable units) and damage risks to systems involved in the process and assesses fabrication/maintenance or operational/use procedures or sequences for error susceptibility to enable improvement quality controls, exception handling, and exigency operations planning.
- (v) DNH FMECA – Assesses system-to-system (nominally, system to system-to-be-protected, but could be bidirectional if desired) safety and failure propagation risks and assesses the potential for adverse interactions.

and analysis scope (i.e., the breadth of systems/processes included) and indenture/segmentation level:

- (a) Black-box – Covers the assessment of failure modes of elements/units of hardware (e.g., Line Replaceable Units [LRU], Operational Replaceable Units [ORU]), software, or processes (set of procedural steps) and their characterization, while failures in internal design attributes and steps are considered as mode causes not modes on their own.

- (b) First active component – Extends failure analysis to cover the assessment and characterization of the failure modes to the first active component on either side of an interface. For mechanical systems, these are components that move or rotate themselves or other components (e.g., pumps, valves, wheels, gears, hinges, toggle, non-explosive actuators); for electrical/electronic systems, these are those that are enabled by power and control or modify electrical signals/data for downstream use (e.g., integrated circuits, EEEE-parts, switch/relay); for software these are the first logic/code that performs a decision or initiates a course of action (this includes exception-handling but not set-up, loading, transmission-only or counting logic/code); and for processes, these robotic/human interface steps that initiate hardware or software action (e.g., opening, closing, deploying, powering on/off, rebooting/reloading).
- (c) Piece-part (physical, logical, or procedural) – Covers the failure assessment and characterization of internal failures of design attributes and steps, while associated impacts to elements/units of hardware (e.g., LRUs, ORUs), software, or processes (set of procedural steps) will be captured as effects/impacts and not modes or causes on their own.
- (d) Task (procedural or logic) – Covers the assessment and characterization of failure modes of logic/code or procedural steps (e.g., errors, incomplete/over execution, mistimed or non-actions), while associated hardware/software or system performance impacts are captured as effects and not modes or causes on their own (but may provide detection/prevention provisions as well).
- (e) Other analyst-specified level.

and operational periods/phase(s):

- (1) Testing – The interval of system or unit-level usage for performance, compatibility, and specification verification.
- (2) Fabrication/Integration – The interval or specific situations associated with manufacturing and joining system components.
- (3) Flight/Operations – The interval of nominal and extended system usage (duration, environment, and operations required) to meet success criteria.
- (4) Servicing/Maintenance – The interval or specific situations associated with refurbishing, replacing, and upkeeping system components.
- (5) Specific Operation(s) – The interval for a specific subset of nominal and extended system usage (scenario, environment, and operations required).

based on the performance and risk insights desired. Note: subordinate or more detailed analysis may be inspired by any strategy chosen.

Some examples (Project concern => recommended FMECA strategy) are:

Is it safe to test with specific GSE? => Perform an interface (GSE-to-test-article) FMECA or GSE DNH FMECA, at black box level or first active component for the testing phase..

Can the system harm host-system? => Perform an interface FMECA or DNH FMECA, at black box level, for (all or specific) operations phase(s).

Is there a failure of an instrument that can end the mission or cause loss of success? => Perform an instrument functional & interface (Instrument-to-spacecraft/host) FMECA, at black box level, for (all or specific) operations phase(s).

Could the planned process/action lead (operations/maintenance) to system or infrastructure harm? => Perform a process FMECA at task level, and/or interface FMECA (or update existing analysis) between systems involved in process/action, at black box level, for (specific or all) operations or servicing/maintenance phase(s).

Is the system single fault tolerant? => Perform functional or detailed FMECA, at box or piece-part level (stopping at the lowest level at which redundancy is implemented), for any period of interest.

Can the system perform mission (meet requirements) for planned life (or extended life)? => Perform functional & interface FMECA between all mission systems, at black box level, for any/all periods of interest.

Is there risk of using a particular component or design? => Perform detailed FMECA if possible, at piece part level during any/all periods of interest; or fallback to functional FMECA if detailed design data is unavailable, at black box level, for any/all periods of interest.

Can software induce a hardware failure and vice versa? => Perform functional & interface FMECA between all hardware-to-software interfacing systems, at black box level, for any/all periods of interest.

4.3.2.2 Define Failure Mode Analysis Ground Rules and Assumptions

The analyst will use the GSFC FMECA RPN definitions (See [Table 1](#)) and begin to define the analysis-specific assumptions and ground rules by using the GSFC-FMECA ground rules:

1. Only one failure mode exists at a time. Failures, degradations, and excessive performance are assumed to only happen one at a time and their effects and likelihood are not considered collaboratively (but may be duplicative). However, failure modes may be causes of other failure modes based on effects.
2. All items and systems (unless specifically stated otherwise) are as-designed, good-as-new, and conforming to usage limits, while consumables are present and in sufficient quantities for the use-case of the analysis.
3. All items, systems, and processes are capable of performing their intended purpose unless failed.
4. FMECA indenture level remains constant within an analysis. Therefore, redundancy will only impact a failure mode's consequence not its likelihood or detection/prevention.
5. Failure mode effects are listed specifically, individually, and at three levels (local, next level, ultimate) starting at the element itself.

6. Interface or signal issues can be considered failure modes at the source, but at the impacted hardware, these would be individual impacts or causes, not stand-alone failure modes.
7. Actions on the system that are not considered are sabotage, misuse, infrastructure/weather issues, or other noncredible scenarios.
8. Severity, likelihood, and D/P are assessed (and reassessed until all are considered, and their interactions are reflected in findings/values) as specified in the FMECA RPN Table ([Table 1](#)), which will have had each consequence level clarified with performance criteria and acceptable system unavailability at a minimum by the RE.

For example:

- Technical Consequence-3, ‘Moderate impact to full mission success criteria. Minimum mission success criteria are achievable with margin’ is appended and becomes ‘Moderate impact to full mission success criteria. Minimum mission success criteria are achievable with margin: *All Threshold Science is still achievable; Not all Baseline Science is achievable;*’ and Technical Consequence-4, ‘Minor impact to higher priority full mission success criteria’ is appended and becomes ‘Minor impact to higher priority full mission success criteria: *Degradation of Threshold Science Measurements or loss of all science data for one orbit period or less.*’
- In addition, others like Likelihood-3, ‘ $0.15 < P_F \leq 0.25$ ’ can also be enhanced/clarified if desired and appended as follows ‘ $0.15 < P_F \leq 0.25$ or $5.9 \times 10^{-6} < \lambda < 1.03 \times 10^{-5}$ for constant failure rate items and a mission duration of 3 years 60 days.’

In addition, the RE will need to convert any implicit assumptions being made to explicit ones and add any mission-specific assumptions or scope limitations being made in their analyses that are not covered in RPN clarifications. Adding these will formulate analysis-specific, explicit assumptions and ground rules, so that consistent consequence assessments can be made during failure mode characterization. These explicit additions may take the form of operational period inclusions/exclusions (e.g., launch, test), performance criteria definitions (e.g., what is degradation versus loss and temporary versus prolonged), or each specific common cause or passive structural failure inclusion or exclusion justification. For instance, if a mission says, ‘Strong spots are considered the most critical to science,’ the analyst might state the assumption that the loss of a strong spot is considered a failure not a degradation. Similarly, impacts to non-success related elements (e.g., student instrument) or the failure of a passive structure could be excluded by an added ground rule. Note: perfect manufacturing or workmanship is not normally assumed since these would be underlying causes of failure until verified as correct, but if it is assumed, then this will need to be stated explicitly and these causes eliminated from each failure mode. For example: ‘Workmanship/Calibration is excluded from this analysis based on quality assurance activities, testing, inspection, and assumed mature design and implementation processes.’

It is prudent to review the FMECA approach (or combined approaches), scope, analysis-specific-RPN definitions, and assumptions with system stakeholders before beginning an analysis to ensure results meet their needs.

Table 1 - GSFC FMECA RPN Table

Criticality Rating	Technical		Failure Type		Failure Severity	Detection/Prevention (Mitigations)
	Likelihood of Occurrence	Consequence				
5 Very High	$0.50 < P_F$	Minimum mission success criteria are not achievable.	Critical and SPF	1SC	Failures that could cause a catastrophic event such as the loss of life, permanently disabling injury to personnel, or facility loss/destruction.	None - Failure will not be detected and will not be prevented or mitigated.
				1	Failures (and failures with failure recoveries) that could result in mission loss or minimum mission success criteria not being achievable.	
4 High	$0.25 < P_F \leq 0.50$	Major impact to full mission success criteria. Minimum mission success criteria are achievable.	Critical	2S	Failures that could prevent detection, mitigation, or operations during a hazardous condition resulting in 1SC conditions, eliminate a hazard inhibit, or cause severe injury or occupational illness or major property damage.	Remote - Unlikely failure will be detected or prevented or mitigated.
				2	Failures (and failures with failure recoveries) that could result in loss of one or more mission objectives, including the substantial loss of data, loss of functionality, or reduction in life of the mission, but minimum mission success criteria are still achievable.	
3 Moderate	$0.15 < P_F \leq 0.25$	Moderate impact to full mission success criteria. Minimum mission success criteria are achievable with margin.	Significant	3	Failures (and failures with failure recoveries) that could result in loss of one mission objective, including the significant loss of data, loss of functionality, or reduction in life of the mission, but minimum mission success criteria are still achievable.	Low to Moderate - Failure may be detected and may be prevented or mitigated.
2 Low	$0.02 < P_F \leq 0.15$	Minor impact to higher priority full mission success criteria.	Minor	4	Significant failures that could cause degradation to full mission objectives and still meet minimum mission.	Moderate to High - Failure is likely to be detected before occurrence and has a good chance of being prevented or mitigated.
				4T	Failures that cause a temporary 1, 2S, or 2 consequence condition until an identical provision or equivalent provisions are used to resolve with no more than degradation to mission success.	
1 Very Low	$0.001 < P_F \leq 0.02$	Minor impact to lower priority full mission success criteria.		5	Minor failures that could result in insignificant or no loss to mission objectives.	Certain - failure will be detected and prevented or mitigated.
0 Very Very Low	$P_F \leq 0.001$	N/A – Highly Implausible or Noncredible				

Project_Name Failure Modes, Effects, and Criticality Analysis Worksheet														
Project:										Analyst:			Organization:	
System/Subsystem: Name (ABC)[Acronym]										Date:			Version:	
FMECA-Mode Identifier (Unique Ref. No.)	Element Name	Element Function or Purpose	Potential Failure Mode	Potential Failure Causes	Likelihood of Occurrence (Rating & Value)	Potential Effects of Failure			Failure Type	Severity Value	Mitigating Factors (with headings, as shown, or sub-columns for Detection/Prevention/Mitigation)	D/P Rating	RPN	Comments
						Local Effect	Next Level Effect	Ultimate Effect						
ABC_###	Name	Purpose_1 Purpose_2 Purpose_3 ... Purpose_n	Mode	Mechanism_1 Cause_1.1 Cause_1.2 Mechanism_2 Cause_2.1 Cause_2.2... Cause_2.n ... Mechanism_n Cause_n.1 ... Cause_n.n	# (0-5) ----- #.## x10# or 0.## or ##.## or Range from table 1	Effect_1 Effect_2 ... Effect_n	Effect_1 Effect_2 ... Effect_n	Effect_1 Effect_2 ... Effect_n	1, 1SC, 2S, 2, 3, 4, 4T, Or 5	1-5	Prevention: Pre-Ops- Rigorous Contamination Control Plan to prevent outgassing to prevent damage, High Quality Parts; and performance and workmanship verification In-Ops – FDIR Proc_ABC Detection: Pre-Ops- N/A In-Ops – sensor XYZ reading of ### and safing RSTZ_1 Mitigation: FDIR Proc_ABC triggered by sensor XYZ reading of ###	1-5	##	Loss of redundancy in ABC system, reduces margin from 3 of 5 to 3 of 4. Loss of inhibit for mechanical hazard ### Failure creates hazard of impact injury in I&T (See hazard ###) Update failure mode when workmanship vibe test is completed. Needs Verification of FDIR Proc_ABC Verifies Requirement science availability (SSN_###) Associated with Requirement science availability (SSN_###) ¹Assumes likelihood from TM_##### pred. report Single Point Failure (SPF) Critical Failure Mode is noncredible due to successful workmanship test.

Where (Non-Italics are template fields; Italics are example text):

- **FMECA-Mode Identifier:** A unique reference number or label for each failure mode.
- **Element Name:** A designated moniker for the item being analyzed and associated with the failure mode.
- **Element Function or Purpose:** The required action, task, or performance provided by the element.
- **Failure Mode:** The manner (or observable state) of a failure or undesired outcome occurs within a system or operation.
- **Failure Causes:** Failure mechanisms and causes (See definitions in Section 3.2) that lead to the failure mode.
- **Likelihood of Occurrence (Rating & Value):** A quantitative ranking of the probability of occurrence and the probability of occurrence (if known) of the identified failure mode (see Table 1). The ranking values range from 1 to 5, corresponding to very low to very high probability while the probability values are quantified between 0 and 1.
- **Effects of Failure:** The consequence(s) a failure mode has on the operation, function, or status of an item. See Section 3.2 for more detailed definition.
- **Failure Type:** The classification (e.g., Critical and SPF, Critical, Significant, Minor) and qualitative label assigned to the failure mode based on the worst potential consequences resulting from the failure per Table 1.
- **Severity Value:** A quantitative rating of the identified failure mode, ranging from 1 to 5, based on the corresponding to Failure Types per Table 1.
- **Mitigating Factors (Detection/Prevention/Mitigation):** An explanation of detection/prevention methods/provisions available for the identified failure mode. See Section 3.2 for definitions.
- **Detection/Prevention Rating (D/P Value):** A quantitative ranking of the effectiveness of the detection or prevention methods being implemented to mitigate or avoid the failure mode effects. The values range from 1 to 5, corresponding to very unlikely to very likely that the effects will be avoided or mitigated. See Table 1.
- **RPN:** This value is the product of the Likelihood, Severity, and D/P values (rankings). The RPN is used to determine the order in which recommended actions will be developed to address potential failure modes and causes to improve the reliability of the equipment.
- **Comments:** Remarks or notes/clarifications, (rationale, exclusion-reasoning, recommendations), update/verification flags/alert-text, criticality/effects notes or flags for searching (‘loss of redundancy’, sources, related requirements (‘Verifies’), notes/clarifications, and explanations of assessments made by the reliability engineer(s) or the design engineer(s) about the occurrence, effect, or control of the identified failure mode(s). As well as rationale for retention of a SPF for use in SPF/CI (if desired). Cross-reference identifiers/labels/subscripts/superscripts should be used to provide clarity and relationship to failure mode data.

Figure 2 - FMECA Worksheet Example

4.3.2.3 Perform Failure Mode Identification and Characterization

Since failure mode analysis is an inductive (bottom-up) process, it is assumed that one mode will happen at a time, and the effects of multiple failure modes are not considered collaboratively. Failure mode identification and characterization (See Consider Failure Modes Cycle in [Figure 1](#)) uses the understanding of the parts/elements, components, and systems, their purpose or functions, and performance dependencies to:

- Postulate all potential failure modes in accordance with ground rules. Consider grouping or repeating common mode failures for identical items for brevity and updating efficiency;
- Identify causes and effects/impacts of each failure mode;
- Determine and verify consistency of each failure mode's or cause's available prevention and/or mitigation strategies and detection capabilities;
- Ascertain likelihood of occurrence, consequence, and D/P (and total RPN) values using analysis-specific RPN definitions ([Table 1](#));
- Add flags/labels, comments, and recommendations as necessary and described below;

and record those in a FMECA worksheet as shown in [Figure 2](#).

Postulating Failure Modes: This is the process of listing all possible undesirable and discrete outcomes [from legacy analysis (See [Meta-SMACM](#)), failure mode dictionaries, vendor/subordinate FMECAs] textually for a system or process at the predetermined indenture level and phase(s). This listing could include those outcomes that are later considered noncredible (excluded) by likelihood, physical feasibility, operational phase, and/or control/mitigation; generated by cause and effect identifications in the FMECA process; or added/refined by design changes inspired by the FMECA process or information from testing/ operations and reliability analyses such as limited life analysis ([GSFC-HDBK-8010](#)), fault tree analysis ([371-WI-8720.0.1A](#)), and fishbone/Ishikawa diagramming. Note: Failure modes are single events not event sequences, but failure modes may need to be repeated if their behavior and parameters are dependent on specific nominal conditions/states or operational periods. These dependencies will need to be used to create discrete instances of the failure mode (e.g., FMA1 becomes FMA1.1 during launch, FMA1.2 during cruise, FMB10 becomes FMB10.1 under maintenance, FMB10.2 under operations).

- (i) For a Functional (Operations) FMECA, failure modes capture the loss of an element (hardware or software) or its failure to perform its desired behavior (e.g., gather/accept correct data/signal at the correct time, deliver the correct data/signal at the correct time, move or restrict movement, generate/dissipate energy, convert material or energy, facilitate/restrict material or energy flow, execute logic), the degradation of an element's desired behavior, and the excessively/disproportionately performed desired behavior. The failure of an element itself would be a cause for a failure mode in this type of FMECA, but not a failure mode, although it may be a failure mode in other FMECA types (i.e., detailed, DNH, combined).

- (ii) For a Detailed (Design) FMECA, failure modes capture the malfunction (loss, degradation, and over-performance) of each element (hardware or software) individually in accordance with the indenture level: (black-box) unit/equipment malfunctions; (task) procedural or logical subset malfunctions of unit/equipment; (piece-part) malfunctions of each individual constituent fragment of a design/unit; (first active component) malfunctions of only the first active individual constituent fragment in a design/unit.
- (iii) For an Interface (Compatibility) FMECA, failure modes capture the loss, degradation, and excessive exchanges of all expected and unexpected data, material, and/or energy from one element (hardware or software) to another. This FMECA's failure modes cover impacts to both sides of each interface. The failure of an element itself would be a cause for a failure mode in this type of FMECA but not a mode, although, it may be a failure mode in other FMECA types (i.e., detailed, DNH, combined).
- (iv) For a Process (Procedural) FMECA (PFMECA), failure modes capture each potential anomalous activity (dormancy, degradation, and over-performance) within a process/procedure individually. These would be postulated by considering automation and operator/procedural errors and the failure, degradation, or over-performance of each element (hardware or software) of the process or procedure.
- (v) For a DNH FMECA, failure modes capture the functional, interface, detailed design, and process FMECA failure modes (as described above) and assess their potential to propagate to or negatively impact a specific target system. This FMECA's failure modes differ from those of other FMECAs, since it only considers the impacts to the target and does not consider the failure modes of the target in the analysis.
- (vi) Combinations – If a combined-type FMECA is employed then failure modes will be captured in accordance with all types being combined as described above.

Note: Modes may need to be refined or excluded once controls/mitigations are identified (See [Determining Detection/Prevention Strategies](#)) or revised concurrently by design/systems teams. Mode identification should be considered incomplete until D/P provision updates are completed.

Identify Causes: This is the process of determining each failure mode's manifestation mechanism and causation factors behind its occurrence. A single failure mode may have a single or multiple failure mechanisms and each mechanism may have a single or multiple causes. A failure mechanism should capture the proximate cause of the failure mode and the failure causes should capture the causes of the mechanism(s) (See Example in Figure 3). Mechanisms and causes can be procedural, exposure/use, interface, hardware, or software related in any FMECA type and derived independently or from legacy analysis (See [Meta-SMACM](#)), failure mode dictionaries, vendor/subordinate FMECAs. Mechanisms are usually independent of other mechanisms but causes may need to be combined-logically (with Boolean logic) to initiate a mechanism of a fault/failure mode (e.g., hot weather AND loss of environmental temperature control would initiate the mechanisms of overheating an element).

No Bearing Motion	Bearing Seized	Lack of Lubrication Material Incompatibility (Wrong Lubricant) Thermal Stress/CTE mismatch Foreign objects &/or debris
	Bearing Fractured	Impact Load Wrong Material Mechanical Over-Stress Workmanship Issue
	Bearing Turned Off	Erroneous procedure/operator error Upstream power failure
	Bearing Worn (Aged)	Operating Time/Speed/procedures
Failure Mode	Failure Mechanism(s)	Failure Cause(s)

Figure 3 - Failure Mode Cause Identification Process Example

In some cases, only the failure mechanism and/or a limited set of causes is determinable by the FMECA analyst. In these cases, designers, operators, test results, and subject matter resources should be consulted, and other reliability analyses such as subordinate FMECAs (legacy, supplied, or performed-separately on hardware, software), limited life analysis ([GSFC-HDBK-8010](#)), fault tree analysis ([371-WI-8720.0.1](#)), Part Stress Analysis (PSA) ([371-WI-8720.0.2](#)), Worst Case Analysis (WCA) ([371-WI-8720.0.5](#)), and fishbone/Ishikawa diagramming should be leveraged to fully capture all potential causes so that the causes can be addressed to remediate anomalies in the future. Regardless of how a failure mode's causes and mechanisms are identified, the reasoning, source, and subordinate FMECA failure modes (if applicable) should be captured in the FMECA (See Figure 4 for an example of how to capture all causal data). Note: Mechanisms and causes for one element may be failure modes for another.

- (i) For a Functional (Operations) FMECA, failure mechanisms and causes capture the reasons for the faulty functionality identified in the failure mode. Since these relate to the functionality of a system element, they will include performance issues internal to the element and/or system and, depending on an element's dependencies, external stimuli. For example, a system may have a laser that needs to create a pulse of a prescribed rate and duration with a specific energy, and a functional fault would occur when the pulse is not realized as specified (failure mode – no laser pulse produced). This failure mode could have the failure mechanisms of 'Laser Amplifier Amplification Loss' and 'Laser Powered Off.' Each of these mechanisms would have specific causes and could be captured in the FMCEA as follows:

Laser Amplifier Amplification Loss
Amplifier Cracks
Transient Loads
Improper Installation
Intermetallic Material Growth

Laser Powered Off
Input/Command Error
Software Malfunction (SW-#)
Power Loss (EPS-#)
Single Event Bit Upset

- (ii) For a Detailed (Design) FMECA, failure mechanisms and causes capture the reasons for the malfunction (loss, degradation, and over-performance) of each design-element (hardware or software). Since these relate to the innate capabilities of an element, they will include internal impetuses to the element and/or system, depending on an element's dependencies, and in some cases external stimuli. For example, a design may have a resistor to supply a specific voltage to another circuit element, and a fault would occur when it does not provide that specific voltage (failure mode: resistance absent - resistor shorted). Or, software code in the design that should process all data, would have a fault occur when it loses data (failure mode: software input data corruption). Each of these would have specific mechanisms and causes that could be captured in the FMCEA as follows:

Resistance absent-resistor shorted:

*Improper Workmanship
Insufficient Cleaning
Bent Pins
Improper Installation
Tin Whiskers
Overheating*

Software input data corruption:

*Input Error
Radiation Exposure
Single Event Bit Upset*

- (iii) For an Interface (Compatibility) FMECA, failure mechanisms and causes capture the reasons for anomalous exchanges of expected and unexpected data, material, and/or energy from one element (hardware or software) to another. Since these relate to exchanges, the mechanisms are flow-related (e.g., lost, degraded/corrupted, and/or excessive), and the causes for these could be functional/design failure modes or mechanisms (previously or subsequently analyzed with a Detailed and Functional FMECA or other reliability analysis methods) from either side of the interface.
- (iv) For a Process (Procedural) FMECA, failure mechanisms and causes capture the related reasons for a process fault/failure mode. The mechanisms of a process fault/failure mode are the errors, misapplication (environmental, system, timing), and misuse of procedures/methods or equipment (hardware or software). These may have causes that are functional, interactional, systemic (e.g., documentation, user-focus, training, environmental controls), and/or competency/ability related and need to be thoroughly researched (potentially using previously or subsequently performed Interface and/or Functional FMECA, other reliability analyses, or problem reports) to accurately mitigate risks and employ controls/improvements.
- (v) For a DNH FMECA, failure mechanisms and causes capture the reasons for anomalous exchanges of each expected and unexpected data, material, and/or energy from one element (hardware or software) to another (as described above). However, the causal assessment would only be of the side of the interface that can do harm to the other. This may be unidirectional or bi-directional.

Note: Causes (mechanisms and causations) may need to be refined or excluded once controls/mitigations are identified (See [Determining Detection/Prevention Strategies](#)) or revised concurrently by design/systems teams, which will also potentially impact the corresponding

effects or render the cause(s) noncredible/excluded. Cause identification should be considered incomplete until D/P provision updates are completed.

Project Name Failure Modes, Effects, and Criticality Analysis Worksheet				
Project:				
System/Subsystem: Name (ABC) [Acronym]				
FMECA-Mode Identifier (Unique Ref. No.)	Element Name	Element Function or Purpose	Potential Failure Mode	Potential Failure Causes
ABC_###	Name	Purpose_1 Purpose_2 Purpose_3 ... Purpose_n	Mode	Subordinate Item (SI) Failure A:^a SI FMECA Ref #: M-1.2, N-7,8, R2.21, S-4.1 Mechanism_2 Cause_2.1 Cause_2.2... Cause_2.n ... Logic Failure RW in NJT:^b NJT SW FMECA Ref#: FSW-1.2 Mechanism_n Cause_n.1 ... Cause_n.n

...

Organization:
Version:
Comments
Loss of redundancy in ABC system, reduces margin from 3 of 5 to 3 of 4. Loss of inhibit for mechanical hazard ### Failure creates hazard of impact injury in I&T (See hazard ###) Update failure mode when workmanship vbe test is completed Needs Verification of FDIR Doc. 117 Verifies Requirement science availability (SSN_###) Associated with Requirement science availability (SSN_###) ¹Assumes likelihood from TM_##### pred. report Single Point Failure (SPF) Critical Failure Mode is noncredible due to successful workmanship test. a - Based on SI FMECA: Document ###-## b - NJT SW FMECA: Document ###-## c - PSA Exceedance for Z sec: Document ###-##

Figure 4 - FMECA Causal Data Capturing from Legacy/Subordinate FMECAs or Other Sources

Identify Effects/Impacts: This is the process of determining and capturing each failure mode's impact(s) to the element itself (local effect), to dependent systems/elements/processes (next level), and the end-item effect (ultimate or mission effect). These impacts could be functional, process, and/or interface related regardless of the FMECA approach used; therefore, it is prudent to consider the potential for each type of impact to discover all potential impacts at each level (including but not limited to 'Loss of Redundancy'). This can be done as part of the FMECA process or informed by testing, peer-consultation, and other reliability analyses such as superior-indenture-level (system/ mission) FMECAs (See [Figure 5](#)), fault tree analyses ([371-WI-8720.0.1](#)), and fishbone/Ishikawa diagramming. The impacts at each level may be singular or multiple for singular or multiple items, and consideration should not cease until all are captured as each may impact the next level. Impacts should be short textual statements that capture the specific consequences, which when warranted can be enhanced with cross-referencing to other failure modes. If needed the comment field of the FMECA worksheet can be used to capture effect-assertion rationales/sources. Once all impacts are captured, the end-item effect(s) is compared to the consequences and severities listed in the RPN table ([Table 1](#)), and a failure type classification (e.g., Critical and SPF, Critical, Significant, Minor), qualitative label (e.g., 1SC or 1, 2S or 2, 3, 4 or 4T, 5), and severity value (e.g., 5, 4, 3, 2, 1) are assigned per [Table 1](#) and used later for criticality assessment and RPN calculation. Note: Effects will likely need to be refined or excluded once controls/mitigations (See [Determining/Prevention Strategies](#)) are identified or revised concurrently by design/systems teams and will also potentially impact the corresponding failure type and severity value as well or render a cause(s) noncredible/excluded. Effects and severity value assessments should be considered incomplete until D/P provision updates are completed.

Impacts/effects may seem understated after considering available D/P provisions. Therefore, the analyst should clarify this for the stakeholder by adding phrases to the nominal effects statements (or comments), such as ‘Harsh_Effect if it weren’t for the redundancy B,’ ‘Assumes redundant side still available for use,’ ‘Assumes well-trained operator,’ or ‘Harsh_Effect if it weren’t for FDIR proc Z.’ It is important to note that this is in addition to stating the effects implied by the one failure alone. For example, if a system/process is redundant and either instantiation can achieve success at any instant, then the failure for the B side cannot assume the A side is failed or unavailable, otherwise its risk will be overestimated (and vice versa). However, if an analyst finds a circumstance where a system/process that has an alternate/redundant instantiation and has an ill-advised operational/design constraint to not return or use the primary instantiation once the alternate is employed, then the analyst should engage in further discussions to assess the veracity of the circumstance and resolve the usage limitation if possible. But if the circumstance persists, the analyst may consider the alternate’s failure effects by assuming the primary is unavailable (noting the constraint and assumption), which would likely be more severe than the primary failure effects.

In addition, effects could also imply the need for the addition or refinement of FDIR provisions or failure modes in subordinate FMECAs (e.g., software fault-responses to hardware/process erroneous states/data). Therefore, annotating and communicating these correlations is essential (See Sections 4.3.2.4 & 5 and Figure 1).

Project Name Failure Modes, Effects, and Criticality Analysis Worksheet								
Project:								
System/Subsystem: Name (ABC)[Acronym]								
Potential Effects of Failure			Failure Type	Severity Value	Mitigating Factors (with headings, as shown, or sub-columns for Detection/Prevention/Mitigation)	D/P Rating	RPN	Comments
Local Effect	Next Level Effect	Ultimate Effect						
Effect_1 Effect_2 ... Effect_n	Effect_1 Effect_2 ... Effect_n	Superior Effect_1 Superior Effect_2 ... Superior Effect_n ^a	1, ISC, 1S, 2, 3, 4, 4T, Or 5 ^a	1-5	Prevention: <i>Pre-Ops- Rigorous Contamination Control Plan to prevent outgassing to prevent damage, High Quality Parts; and performance and workmanship verification</i> <i>In-Ops – FDIR Proc_ABC^a</i> Detection: <i>Pre-Ops- N/A</i> <i>In-Ops – sensor XYZ reading of ### and safing RSTZ_1^a</i> Mitigation: <i>FDIR Proc_ABC triggered by sensor XYZ reading of ###^a</i>	1-5	##	<i>Loss of redundancy in ABC system, reduces margin from 3 of 5 to 3 of 4.</i> <i>Loss of inhibit for mechanical hazard ###</i> <i>Failure creates hazard of impact injury in I&T (See hazard ###)</i> <i>Update failure mode when workmanship vbe test is completed</i> <i>Needs Verification of FDIR Proc_ABC</i> <i>Verifies Requirement science availability (SSN_###)</i> <i>Associated with Requirement science availability (SSN_###)</i> ¹ <i>Assumes likelihood from TM_##### pred. report</i> <i>Single Point Failure (SPF)</i> <i>Critical Failure</i> <i>Mode is noncredible due to successful workmanship test.</i> <i>a - Based on System-ABC FMECA: Document #-#-#</i>

Figure 5 - FMECA Effect Correlation from Superior FMECAs and Additional Sources

Ascertain Mode/Cause Likelihood: This is the process of determining and capturing each failure mode’s occurrence potential based on the probability of failure or contributing causes occurring over the desired operational and non-operational life or engineering judgement based on historical performance or other knowledge. Since any particular fault/failure mode may have more than one contributing cause, it is essential that an appropriate probability or logical aggregation of accurate probabilities be generated to predict a mode’s likelihood. The generation of these probabilities can be completed using sources such as ‘System Reliability Center’s

*Failure Mode Distributions*¹, 'Quanterion Automated Databook (QuAD)'², 'EPRD-2014', 'NPRD-2016', 'FMD -2026', MIL-HDBK-217³, reliability analysis tools (e.g., GSFC's FIAT, Windchill's Quality Solutions, Weibull++), and other reliability analyses [e.g., limited life analysis ([GSFC-HDBK-8010](#)), fault tree analysis ([371-WI-8720.0.1](#)), and RBDs/predictions ([PD-AP-1313](#) or [371-WI-8720.0.7](#))].

Once a mode's likelihood is estimated or assumed, it is compared to the likelihood ranges shown in the RPN table ([Table 1](#)) and the matching occurrence value rating (0-5) is assigned to the mode. If the rating of '0' is assigned to a failure mode, that mode may need to be flagged as *noncredible/excluded* in the comments for that mode. Note: When documenting the occurrence value in the FMECA's worksheet, it is best to capture the estimated or assumed likelihood along with the occurrence rating and to provide a source, rationale, and/or update-flag in the comments area for substantiation and updating purposes (See examples in Figure 6). Also, Likelihoods (and occurrence rating) may need to be refined based on other analyses (e.g., PSA/ WCAs predict intolerable stress exposures that could increase likelihood), controls/mitigations identification (see [Determining Detection/Prevention Strategies](#)), or when design changes inspired by the FMECA or other processes are made. Therefore, likelihood assessments and occurrence value rating should be considered incomplete until these updates are completed.

Occurrence Rating/Value	Comments
2 ($P_F = 0.1246$) ^a	a – Based on prediction document in Report (filename/report number)
4 ($P_F = 25 - 30\%$) ^b or ($P_F = 30\%$) ^b	b – Estimated based on designer/SME (name/position) experience and knowledge.
0 ($P_F \leq 0.001$) ^c	c – Updated from 0.50 after vibration test verified workmanship (WOA-##).
4 ($P_F = 0.3123$) ^d	d – Probability of failure will be updated once action is complete (e.g., life testing XYZ, process training, performance (hardware/software/process) testing).

Figure 6 - Occurrence Value Documentation Formatting Examples

Determine Mode/Cause Detection and Prevention Strategies (Mitigation Factors/Options): This is the process of determining and capturing each failure mode's signatures, symptoms, inhibits, controls, and impact-avoidance provisions. These should be as specific as possible so that they can be used to diagnose (identify the failure mode in existence and its causes from the FMECA) or resolve issues during operations/process-execution in the specified performance period for the FMECA.

- For Detections, constant or situational observables are captured. These observables could be direct or indirect and include:
 - health-monitors (e.g., voltages, currents, temperatures, stresses, contamination),
 - data losses, corruption, or exceedances,

¹ <https://www.scribd.com/document/317640712/Part-Failure-Mode-Distributions>

² <https://extapps.ksc.nasa.gov/Reliability/QuAD.html>

³ <https://www.quanterion.com/wp-content/uploads/2014/09/MIL-HDBK-217F.pdf>

- functional and performance changes,
- system or process state changes (e.g., on/off, pause, reset/reboot),
- system and process configuration changes (e.g., autonomous safing and FDIR actions) .
- For Preventions, controls, assurances, and mitigations are captured and should be kept up to date with any changes. These could include:
 - screening,
 - inspections,
 - reviews/checkpoints,
 - training,
 - dry-runs/testing, fail-safes,
 - fault tolerance attribute(s) other than redundancy (e.g., FDIR, Safing, exception-handling).

Controls and assurances should cover before and during the specified performance period of the FMECA, while mitigations should only be those present during the specified performance period of the FMECA. Further, mitigations that are the cause of an observable (e.g., FDIR, Safing, or other feature/strategy) should be noted with the Detection and should include the specific feature/strategy reference so that implementation can be verified, and feature-updates reflected in the FMECA efficiently. For example, Switch of X, Y, and Z systems from A to B due to FDIR-Pointing Check; Instrument A turned off due to Instrument Thermal Protection Safing feature; Manufacturing process halted due to ABC sampling/fallout finding; Software RSL-code aborted due to exception handling MNL feature/routine.

Criticality Analysis Worksheet						
						Analyst:
						Date:
Potential Failure Causes	Likelihood of Occurrence (Rating & Value)	Potential Effects of Failure			Failure Type	Mitigating Factors (with headings, as shown, or sub-columns for Detection/Prevention/Mitigation)
		Local Effect	Next Level Effect	Ultimate Effect		
<i>Subordinate Item (SI) Failure_A^a</i> <i>SI FMECA Ref #s: M-1.2, N-7,8, R2.21, S-4.1</i> <i>Mechanism_2</i> <i>Cause_2.1</i> <i>Cause_2.2...</i> <i>Cause_2.n</i> ... <i>Logic Failure_RW in NJT^b</i> <i>NJT SW FMECA Ref#s: FSW-1.2</i> <i>Mechanism_n</i> <i>Cause_n.1</i> ... <i>Cause_n.n</i>	# (0-5) ^c ----- ### x10 [#] or 0.## or ##.## or Range from table 1	<i>SI_Effect_1^a</i> <i>Effect_2</i> ... <i>NJT_SW_Effect_n^b</i>	<i>Effect_1</i> <i>Effect_2</i> ... <i>Effect_n</i>	<i>Effect_1</i> <i>Effect_2</i> ... <i>Effect_n</i>	1, 1SC, 1S, 2, 3, 4, 4T, Or 5	Prevention: <i>Pre-Ops- Rigorous Contamination Control Plan to prevent outgassing to prevent damage, High Quality Parts; and performance and workmanship verification</i> <i>In-Ops – FDIR Proc_S1^{a,b}</i> Detection: <i>Pre-Ops- N/A</i> <i>In-Ops – sensor XYZ reading of ### and safing RSTZ_1</i> Mitigation: <i>FDIR Proc_S1^{a,b} triggered by sensor XYZ reading of ###</i>
...						
						Comments <i>Loss of redundancy in ABC system, reduces margin from 3 of 5 to 3 of 4.</i> <i>Loss of inhibit for mechanical hazard ###</i> <i>Failure creates hazard of impact injury in I&T (See hazard ###)</i> <i>Update failure mode when workmanship vbe test is completed.</i> <i>Needs Verification of FDIR Proc_ABC</i> <i>Verifies Requirement science availability (SSN' ###)</i> <i>Associated with Requirement science availability (SSN' ###)</i> <i>Assumes likelihood from TM_##### pred. report</i> <i>Single Point Failure (SPF)</i> <i>Critical Failure</i> <i>Mode is noncredible due to successful workmanship test.</i> <i>a - Based on SI FMECA: Document #-.-#</i> <i>b - NJT SW FMECA: Document #-.-.-#</i> <i>c - PSA Exceedance for Z sec: Document #-.-.-#</i>

Figure 7 - FMECA Effect D/P Capturing from Legacy/Subordinate FMECAs or Other Sources

If needed the comment field of the FMECA worksheet can be used to capture D/P-assertion rationales/sources (such as subordinate FMECA data, as shown in Figure 7). Once these

fault/failure mode D/P factors are captured (best captured in two separate lists in the failure mode's Mitigating Factors cell), they are compared to the D/P statements shown in the RPN table ([Table 1](#)), and the corresponding D/P value rating (1-5) is assigned to the mode. In addition, since these factors can impact modes, likelihood, and effects, it is prudent to assess if the D/P factors affect those items and refine/re-evaluate those given the D/P provisions identified.

Ascertain Total RPN: This is the process of calculating the RPN once the severity, occurrence, and D/P criticality rating values are ascertained, and evaluations are checked for completeness, inconsistencies, or errors. Any inconsistencies found will need to be reanalyzed, to determine which part(s) of the failure mode assessments (L, S, or D/P) or ratings/values are inappropriate, and remedied (e.g., the failure mode text or values updated).

For example, if a failure mode has been assigned a Likelihood of 2, Severity of 4, and a D/P of 1, it means that this failure mode has a 'Low' chance of occurring, 'Major impact to full mission success,' and 'will be detected and prevented or mitigated,' which are contradictory with each other. If the D/P assessment is accurate, then the failure mode could be certain of being prevented, and if so, the likelihood should be lower and revised to 0 or 1; and/or the failure mode could be certain of being detected and mitigated, and if so, the severity should be less and revised to a value from 0 to 2. Alternatively, if the L and S assessments are accurate, then the mode and effects can occur, and the D/P assessment should be higher and revised to a value from 3 to 5.

Once all evaluations are consistent (and FMECA findings revised) then the total RPN is calculated by multiplying all three together:

$$\text{Total RPN} = \text{Severity_Value} * \text{Occurrence_Rating} * \text{D/P_Value}$$

4.3.2.4 Failure Mode Annotation

As noted earlier, the comment field of each failure mode is an effective place to capture any FMECA assertion's source (See Figures [6](#) and [7](#)) or rationale/reasoning (including exclusion justification) and action/update statements/flags. To be effective:

- Rationale/reasoning statements should capture the basis, assumptions, clarifications, and failure mode exclusion justifications for any assertion in the FMECA;
- Action/update trigger statements should capture the stimulus and the action needed [such as verification (e.g., FDIR, design, workmanship, procedural), testing, reanalysis] as specifically (e.g., who, what, when) as possible; and
- Recommendation statements should capture suggestions for fault tolerance improvements, testing, controls, operation/design/process change (including FDIR), or other fault tolerance/risk mitigations based on any of the failure mode's assertions.

In addition, it is advisable to capture annotations for related requirements. These annotations could provide justification for an element's cited purpose/function if needed. But they are most useful in supporting requirement verification, criticality determination (e.g., per NASA-HDBK-2203 and NASA-STD-8739.8 for software), and final implementation refinement and coordination. Therefore, annotations also should include short flag or labelling phrases followed by statements that explain

the reason for the label. Further, it is recommended that consistent flag or labelling phrasing (with comment-to-FMECA assertion cross-reference labeling) be used to enable filtering/searching in comments (or other failure mode fields) such as:

Loss of redundancy in/on/of ...	Assumes ...
Loss of inhibit in/on/of ...	Data source is ...
Failure creates hazard in/on/of ...	Single Point Failure (SPF)
Update failure mode when/after ...	Critical Failure
Needs Verification of ...	Related to common cause ...
Mode is noncredible due to ...	Potential Hazard ...
Verifies Requirement ...	Common mode to identical item ...
Associated with Requirement ...	It is recommended that ...

However, the annotation in the comment field can also be used to capture analysis-assistance and SPF/CI retention notes during the FMECA process.

4.3.3 Critical Item and SPF Identification

CI and SPF identification (See [Figure 1](#)) begins with using the FMECA worksheets/results to gather those failure modes that have been assessed as critical (failure types - 1SC, 1, 2S, 2) and are flagged as critical or an SPF. This subset of failure modes is used to generate a list of elements (CIs – not the failure modes) associated with those modes and a SPF mode list (a subset of all critical failure modes that are failure types - 1SC or 1 and/or are flagged an SPF). The list elements should then be further refined to create a Critical Items List (CIL) - as shown in Figure 8 and described in NASA Reliability Practice NO. PD-ED-1240⁴, while the SPF mode list should be refined to a SPF table (as shown in Figure 8). Each of these lists will include retention rationales and control plan descriptions in addition to FMECA-item identifiers and data (that should be further detailed if possible). If desired, these lists can be split into multiple lists by type of system/process (e.g., hardware, software, bus, payload, maintenance, repair), but care should be taken to ensure that these smaller lists encompass all CIs and SPFs still.

Note: All SPFs have critical failure modes, but not all CIs will have an SPF failure mode.

Examples of rationales include:

- Lack of alternatives (parts, operations, and design/safety options)
- Extensive heritage for similar use
- Item reliability or redundancy [not affected by failure mechanism (standby redundancy)]
- Alternative operations
- Risk vs. cost/benefit of alternatives (trade study)
- Mitigations to be implemented.

⁴ NASA Reliability Practice NO. PD-ED-1240, Identification, Control, and Management of Critical Items List, [1240msfc.pdf \(klabs.org\)](http://standards.gsfc.nasa.gov)

Examples of control plans (See [Appendix B](#)) include:

- Quality Control Plan - describes the actions (measurements, inspections, quality checks or monitoring of acceptance parameters) required to control failure risk.
- Process Control Plan - describes the actions (measurements, inspections, restrictions, instructions/regulations (e.g., ESD, contamination, handling) and training required to control failure and error risks.
- Operations Control Plan - describes the usage limits and allowances (duty cycles, restrictions (e.g., temperature limits, limitation), detection) to control failure risk.
- Hazard Control Plan - describes the actions/methods needed to ensure maintenance of hazard-cause management and safety assurance.
- Risk Mitigation Plan (This can include some or all of the above) – describes actions taken to impact likelihood or effects and when acceptance is warranted.

4.3.4 Common Cause Susceptibility Identification

Common cause susceptibility identification (See [Figure 1](#)) is completed by using the FMECA worksheets/results to gather those failure modes that have been found to be caused by the common failure causes of interest. This subset of failure modes and the items associated with them can be gathered in a table as shown in [Figure 9](#) or other means and should be used to generate risks associated with each common cause (See Section [4.3.5](#)) and recommendations as applicable or to the extent prescribed in the applicable MAR.

Examples of mitigation/action plans to recommend include:

- Parts Controls – plans and processes to select and limits parts used based on testing, quality levels, or acceptance parameters.
- Process Controls - plans and processes to define testing (e.g., CPT, workmanship thermal vac and vibe), measurements, inspections, restrictions (e.g., ESD, contamination, software-loading, and training required to mitigate the realization of causes.
- Environmental Controls - plans and processes to define testing, measurements, inspections, restrictions (e.g., ESD, contamination), analysis, and training required to mitigate the realization of environmental causes.
- Handling Plan – an instruction set of the actions and controls for attaching, manipulating, and lifting items.
- Design Features – elements of the system/process that mitigate the effects of causes (e.g., shielding, over-voltage protection, filters, FDIR).

Critical Items List					
Critical Item	Used on?	Retention Rationale		Control/Action Plan	FMECA Mode Identifiers
		Technical	Safety		
Name	ABC	Required to meet Requirement 123; Likelihood of occurrence is very low and no historical failure have been recorded on similar items; Name is impractical to make redundant; FDIR Proc_ABC will switch to redundant Name; ...	N/A – Item failure does not result in a feasible safety risk. ...	Pre- Ops: Work Instruction XYZ doc No. ##### to ensure NNN; Rigorous Contamination Control Plan to prevent outgassing to prevent damage, Heightened parts assurance; and performance and workmanship verification Operations: Switch To Redundant Name; FDIR Proc ABC; sensor XYZ reading of ### and safing RSTZ_I	ABC_###, ABC_###

Single Point Failures (SPFs)									
Failure Mode Origination	Failure Mode Element	Summarized System Effect	Likelihood		Risk Statement Control Plan	Retention Rationale		FMECA Mode Identifier	Potential Causes
			Rating or Range	Failure Rate (λ)		Technical	Safety		
ABC	Name	<SPF Scenario > leading to <effects>	Very Low 0.001 <P _f ≤ 0.02	3.6 x10* < λ ≤7.3 x10 ⁷ Source: XXXX Engineering Assessment	Given that <SPF scenario>, has/have <likelihood of occurrence>, there is the possibility that <local/intermediate consequences – effect(s)>) will occur, resulting in <ultimate effect/severity or purpose related consequence statement> Pre- Ops: Work Instruction XYZ doc No. ##### to ensure NNN; Rigorous Contamination Control Plan to prevent outgassing to prevent damage; High Quality Parts; and performance and workmanship verification Operations: Switch To Redundant Name; FDIR Proc_ABC; sensor XYZ reading of ### and safing RSTZ_I	Required to meet Requirement 123; Likelihood of occurrence is very low and no historical failure have been recorded on similar items; Name is impractical to make redundant; FDIR Proc_ABC will switch to redundant Name; ...	N/A - Single point failure does not result in a feasible safety risk. ...	ABC_###	Mechanism_1 Cause_1.1 Cause_1.2 Mechanism_2 Cause_2.1 Cause_2.2... Cause_2. Mechanism_n Cause_n.1 ... Cause n.n

Where:

- **Control/Action Plan:** Listing of failure management action to be taken or references to all quality, process, operations, hazard, and risk / risk control plan(s)
 - **Critical Item:** The name of the element with a critical failure mode.
 - **Failure Mode Element:** The name of the element or item associated with the failure mode.
 - **Failure Mode Origination:** The location (next higher assembly, logic, or process) of the element or item associated with SPF.
 - **FMECA Mode Identifiers:** The unique reference numbers or labels of the failure modes that are SPFs or that make this element critical.
 - **Likelihood:** A quantitative ranking of the identified failure mode possibility, ranging from Very Very Low to Very High (or 0 to 5), per Table 1, and Failure rate for the mode if available.
 - **Potential Causes:** Failure mechanisms and causes (See definitions in Section 3.2) that lead to the failure mode.
- **Retention Rationale:** The rationale for acceptance of CI/SPF from a technical and safety perspective. These are normally based on need and mitigations including likelihood, design features, fault tolerance, tests and inspections planned/accomplished, usage constraints, and historical information on the design or a similar design; and include acceptance decision points.
 - **Risk Statement:** A statement (e.g., Given that <SPF scenario>, has/have <likelihood of occurrence>, there is the possibility that <local/intermediate consequences – effect(s)>) will occur, resulting in <ultimate effect/severity or purpose related consequence statement>) that captures the condition and potential consequence. See Section 4.3.5
 - **Source:** Reference(s) for the data provided.
 - **Summarized System Effect:** A brief statement of SPF mode and consequence(s) regarding operation, function, or status of an item/system. See Section 4.3.2.1, Identify Effects/Impacts, for more detailed definition.
 - **Used On:** The next higher element or process or system the critical item supports.

Figure 8 - CIL and SPF Table Templates

Common Cause	Effectuated Items (Failure Mode Identifiers)	LXC (Likelihood and Severity Criticality Rating)	Mitigations/Action Plan Recommendations
Impact/Shock	ABC (ABC_###) NJL (NJL_###, NJL_###)	#x# #x#, #x#	Test ..., Plan... Plan ...
Vibration	ABC (ABC_###) NJL (NJL_###, NJL_###)	#x# #x#, #x#	
Temperature			
Contaminants (FOD)	ABC (ABC_### ...)	#x# ... or Lowest_#x# - Highest_#x#	Clean room level ...
Improper Workmanship/ Manufacturing			
Maintenance			
Electromagnetic Interference (Conducted /Radiated)			
Radiation (TID, DDD, SEE)	FPG (FPG_### - ###)	Lowest_#x# - Highest_#x#	Part control ... Test ... Shielding ...
Micrometeoroid and Orbital Debris (MMOD)			
Others (list all considered)	List each item and it FMs	Give LxC for each FM or Range or worst case for each item	Match Item to LxC(s) and Recommendation(s)

**Figure 9 – Example of Common Cause Susceptibility Table for Risk Generation
(Inclusion in FMECA report is optional)**

4.3.5 Risk Assessment

Each CI needs to be assessed for risk (as defined in GPR 7120.4D) and considered for mitigation/replacement/design changes. Each SPF needs to be assessed for risk (as defined in GPR 7120.4D) and considered for mitigation/design changes. In addition, performing risk assessments for any item susceptible to common causes or with failure mode that has a criticality rating of 3, 4, or 4T ought to be considered. For risk assessment, a risk statement (that includes the failure potential along with likelihood and consequence), Likelihood-Consequence label (LxC), and risk control/mitigation recommendations need to be provided in the general format shown below:

(LxC) Given that <CI-failure mode, SPF, grouping of CI/SPFs, or other significant mode, common cause, or item of concern >, has/have <likelihood of occurrence estimate-statement (including number or low/med/high)>, there is the possibility that <consequences – effect(s)> will occur, resulting in <ultimate effect/ severity or purpose related consequence statement>. It is recommended that (list as many as is applicable):

- Process recommendations such as procedure, operations, and parts controls changes.
- Design recommendations such as software exception handling, redundancy increase, sensor optimization, and FDIR/Safing additions.
- Planning recommendations such as contingency plans to be formulated to quickly respond to failure signatures.

All risks identified should be documented in the FMECA report and be proposed to / discussed with system/process stakeholders (e.g., CSO, cognizant engineer, and/or Risk Manager / Systems Engineer) so that they can accept the risk, and a failure risk control plan (See [Appendix B](#)) can be developed and implemented to avoid the potential for the realization of these risks or at least reduce the failure consequences to an acceptable level or as much as feasible.

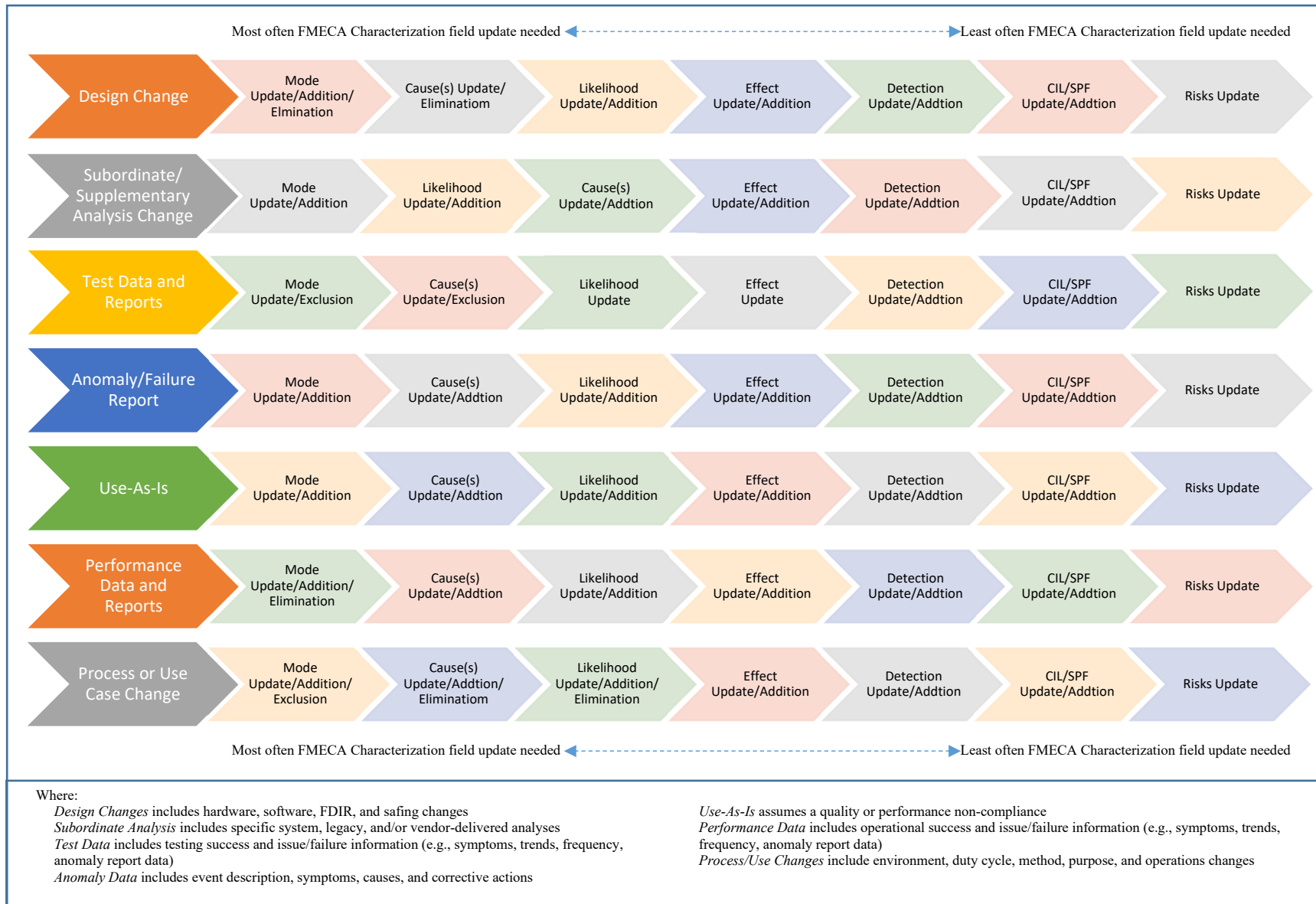
4.4 Data Incorporation

Since a FMECA is a living analysis, it must continually be updated (See [Figure 1](#) and [Table 2](#)) based on inputs from the stakeholders responsible for sharing data (See [Section 4.2](#)) and data provided by subordinate/legacy FMECAs, risk mitigations, changes in design and Safing/FDIR, supplementary analysis results (PSA/WCA, Single Event and Effects Analysis [SEEA], or other reliability analysis), specification-compliance or testing issues/results (e.g., revised detection signatures), and performance/operational changes to remain accurate and useful. For example, if an element of the system/process (or on a similar system) experiences an anomaly in use (blue row of [Table 2](#)), the FMECA analyst will need to review the anomaly report and characterize all values of a new or existing failure modes accordingly (especially common modes); if an element of the system/process passes a workmanship vibration test (amber row of [Table 2](#)), the FMECA analyst will need to review the test report and re-characterize all values of the existing failure mode accordingly, especially causes. This re-characterization will likely not change or eliminate the failure effect, likelihood, detection, risk, or associated CIL or SPF entries unless workmanship is the only cause for the mode.

Note: Any changes will need to be flowed to relevant subordinate FMECA (e.g., specific system or vendor delivered) analysts as well for the same purpose.

If a subordinate/legacy analysis is used as a source for a higher indenture-level analysis, its data should be incorporated as causes, D/P provisions, and other fields as necessary (See [Figure 4](#)). This means that subordinate legacy D/P provision specificity (e.g., FDIR-Proc, specific symptoms or compensations) should be incorporated in the higher indenture level analysis. Note: Any data being incorporated (and referenced) in any type of FMECA should be evaluated for accuracy and applicability prior to incorporation. This can be done using the expectations herein or a credibility evaluation as shown in [Appendix C](#).

Table 2 - Potential Data Incorporation Flows



4.4.1 Legacy Analysis

As discussed in previous sections, a legacy FMECA analysis can be used in a higher-indenture FMECA, however it can also be re-used. To re-use a legacy FMECA (or submit it as a deliverable) for the next instantiation of a design, the following process should be used, or a new analysis should be performed:

- Compare the current design/process and operations to that of the legacy analysis; if it is the same or similar then proceed, otherwise begin a fresh analysis (See [Section 4.3](#)).
- Determine the legacy analysis approach (strategy, assumptions, and indenture level); if the legacy analysis approach is consistent with the current assessment and/or risk assessment desired, then proceed, otherwise use the legacy analysis as reference data in performing a fresh analysis (See [Section 4.3](#)).
- If the design/process and use are the same, then perform a summary analysis:
 - Summarize each logical set of failure modes (See [Figure 10](#)) at the next higher indenture level (e.g., subsystem level if legacy was done at the LRU level) using the legacy failure modes as causes (See [Section 4.3.2.3 - Causes](#)) while ensuring that all effects and compensations are brought forward to enable verifications.
 - Ascertain a composite likelihood of occurrence, consequence, and detection/prevention (and total RPN) values using analysis-specific RPN definitions ([Table 1](#)).
 - Add legacy FMECA references, flags/labels, comments, and recommendations as necessary (See [Section 4.3.2.4](#) and [Figure 7](#)).
 - Record these in a new FMECA worksheet as shown in the [Figure 10](#), assess/reiterate risks/SPFs/CIs, and be prepared to attach the legacy FMECA and SPF-table/CIL to the report (See [Section 5.0](#)).
- If the design/process and use are not the same but are similar, then:
 - Identify the differences in the design/process and use, then perform an analysis update:
 - Review and update all postulated failure modes, ensuring differences are accounted for.
 - Review and update causes and effects/impacts of each failure mode.
 - Review, update, and verify the consistency of each failure mode's or cause's available prevention and mitigation strategies and detection capabilities.
 - Review and update likelihood of occurrence, consequence, and detection.
 - Review and update flags/labels, comments, and recommendations as necessary (See [Section 4.3.2.4](#) and [Figure 7](#)).
 - Postulate any new failure modes not captured based on the legacy design/process and use.
 - Assess/reiterate risks/SPFs/CIs (See [Sections 4.3.3](#) and [4.3.5](#)).
 - Document/Communicate results (See [Section 5.0](#)).

OR

- Identify the differences in the design/process and use and perform a new/updated analysis/analyses of the design/process-deltas at the same indenture level as the original legacy analysis. Then prepare a summary analysis (as shown above) using both the original legacy and new or updated FMECA as legacy analyses. Note: This is only advisable for discernible and separable design changes since system/process use variations are likely to impact multiple areas, and it may be more difficult and time-consuming than performing an analysis update.
- Ensure that the original legacy analysis is annotated to indicate sections that are no longer applicable.

Project _Name Failure Modes, Effects, and Criticality Analysis Summary Worksheet														
Project:										Analyst:		Organization:		
System/Subsystem: <i>System_Name (ABC)[Acronym]</i>										Date:		Version:		
FMECA-Mode Identifier (Unique Ref. No.)	Element Name	Element Function or Purpose	Potential Failure Mode	Potential Cause of Failure	Likelihood of Occurrence (Rating & Value)	Potential Effects of Failure			Failure Type	Severity Value	Mitigating Factors (Detection/ Prevention)	D/P Rating	RPN	Comments
						Local Effect	Next Level Effect	Ultimate Effect						
ABC_###	Upper Indenture level Name	Purpose_1 Purpose_2 Purpose_3 ... Purpose_n	Mode	Legacy Failure Mode_1 (mechanism 1) ² Legacy_FM_causes ... Legacy FM_n (mechanism n) Legacy_FM_cause.n.1 ... Legacy_FM Cause_n.n	# (0-5) ¹ ----- Composite #.## x10 ^{-#} or 0.## or ##.##% or Range from table 1	Legacy_Effect_1 Legacy_Effect_2 ... Legacy_Effect_n	Effect_1 Effect_2 ... Effect_n	Effect_1 Effect_2 ... Effect_n	1, 1SC, 2S, 2, 3, 4, 4T, Or 5	1-5	Prevention: Pre-Ops- Legacy list ² In-Ops – Legacy FDIR Proc list ² Detection: Pre-Ops- Legacy list ² In-Ops – sensor XYZ reading of ### and safing RSTZ_1 ² Mitigation: FDIR Proc_ABC triggered by sensor XYZ reading of ### ²	1-5	##	¹ Composite Likelihood based on TM_##### pred. report ² Legacy FMECA ##### Critical Failure Mode is noncredible due to successful workmanship test. Loss of Science Loss of inhibit for mechanical hazard ### Failure creates hazard of impact injury in I&T (See hazard ###) Update failure mode when workmanship vibe test is completed. Needs Verification of FDIR Proc ABC
ACS_1	Attitude and Control Subsystem	Provide 3-axis Stabilization Provide Precise Pointing Provide Maneuver Control Determine Attitude Manage Ops Disturbances	Loss of Pointing	Loss of Magnetic Torquers(MT-##) ² Wire failure ... Loss of Coarse Sun Sensor (CSS-##) ² Detector failure... Loss of Fine Guidance Sensor (FGS-##, FGS-##) ² Mirror Misaligned Servo Stuck... Loss of Star Trackers (ST-##, ST-##) ² Optical degradation Camera degradation Loss of RWAs (RWA-##) ² Wheel jammed ...	¹ ----- 2.01x10 ⁻³	Loss of magnetic field generation Sun Position Unknown Guide Star loss No Star Pattern to match RWA does not spin	RWA Speed Saturation Sun Intrusion and Damage to Optics Unknown Position in space No Momentum generated	Loss of Science More than 0.007 arcsecond of pointing deviation Uncontrolled or no movement of system	1	5	Prevention: Pre-Ops- Legacy list In-Ops – Legacy FDIR Proc list Detection: Pre-Ops- Legacy list In-Ops – sensor XYZ reading of ### and safing RSTZ_1 Mitigation: FDIR Proc_ABC triggered by sensor XYZ reading of ###	1	5	¹ Composite Likelihood based on TM_##### pred. report ² Legacy FMECA ##### Needs Verification of FDIR Proc_ABC ... Critical Failure Legacy List ...

Figure 10 - Summary Failure Modes, Effects and Criticality Analysis Worksheet Example

5. COMMUNICATION, MONITORING, AND REPORTING

5.1 Communication/Monitoring

Since FMECA development is a process of investigation of failures, consequences, and potential solutions (arguably the most valuable part of performing a FMECA), it is best completed with the involvement of not only reliability engineering, but also all PDLs (hardware and software), SMA personnel, systems engineering, and I&T project/system team members to ensure failure implications are understood and captured and mitigations are implemented appropriately. In involving this diverse group of stakeholders during the FMECA investigation process, it is essential that all possibilities are considered by all participants in an open dialog (meetings are usually best) facilitated by the FMECA analyst. During these dialog sessions, unspecified design considerations and exception-handling will be discovered and potentially resolved. Note: If the resolution is defined outside of the FMECA investigation process, it should be communicated to the FMECA analyst and the investigation team so compatibility and potential beneficial or detrimental effects and retention/elimination rationale can be identified and managed/investigated.

Once a FMECA iteration is developed (and peer reviewed or evaluated using [Appendix C](#) or other means), it will need to be shared effectively with project/system stakeholders and documented (See Section 5.2). Sharing should be done using various methods, beyond report dissemination only, to ensure all stakeholders are reached. These sharing methods should include at least the discussion/integration of FMECA results/implications during engineering peer reviews, milestone reviews, design/operations working groups, anomaly investigations, risk management, TRR/ORRs, I&T procedural development, and FDIR development/implementation. The best tools for sharing the huge amount of data within a FMECA are the CIL, the SPF Table, failure mode matrices, and a risk/result summary.

- (i) CIL – The CIL communicates in a list form (See [Figure 8](#) and [Section 4.3.3](#)) only items with critical-consequence failure modes and their retention rationale, usage, associated failure modes, and control plan (actual or recommended). This type of list enables the quick understanding of critical design-item issues and can be used for action (e.g., risk mitigation) planning/tracking (if kept as a living register within or outside of the FMECA or entries in other systems like risk management) as well as non-conformance decision-making consideration.
- (ii) SPF Table – The SPF table (See [Figure 8](#) and [Section 4.3.3](#)) communicates only the system's purpose/mission-ending failure susceptibilities (e.g., category 1 failure modes and identifiers) or potentially hazard causing failures (e.g., category 1SC failure modes and identifiers) with their impact summary and risk, retention rationales, origination, likelihood, control plan (actual or recommended), and causes. This information allows for an efficient understanding of SPF issues and can be used for action (e.g., risk mitigation, design changes, FDIR refinement) planning/tracking (if kept as a living register within or outside of the FMECA or entries in other systems like risk management).

- (iii) **Failure Mode Matrices** – Failure mode matrices provide a representation of the entire set of failure modes of the FMECA and allow the comparison of each failure mode or set of failure modes (e.g., those for each system element), since each identifier is listed in the appropriate cells of the matrices employed. These matrices facilitate design/trade/ risk discussions, result presentation at reviews, and resource allocation decision making. Utilization of a failure mode ‘Threat Criticality Matrix’ (Figure 11) will summarize all potential failure mode risks in LxC-terms. However, since it is possible that a high-LxC failure mode may have D/P compensating provisions that already mitigate the threat, it may be advantageous to also utilize the ‘RPN Criticality Matrix’ (Figure 12). This matrix will tend to spread the failure modes from one cell in the ‘Threat Criticality Matrix’ across multiple cells and potentially change their color to reflect the D/P compensation situation and further inform stakeholders where additional resources or focus is needed (or not needed). A ‘D/P Criticality Matrix’ (Figure 13) can also be used, but it is important to note that it only shows if D/P provisions exist for each failure mode; it does not factor in likelihood. Therefore, it can communicate D/P or FDIR coverage (or mitigation level) and may be able to provide FDIR decision-making information, whereas the ‘D/P Matrix’ (Figure 14), when utilized, will show the mitigation/prevention effectiveness of D/P incorporation and where others may be needed (e.g., sensor optimizations, FDIR, Safing). In addition, any of these matrices can be enhanced with ‘change-arrows’ (e.g., $\Rightarrow$, $\Downarrow$, $\Uparrow$, $\Leftarrow$) indicating failure mode identifier cell placement changes to show effects of actions taken, potential actions, or analysis updates.

Likelihood of Occurrence	5								
	4								
	3								
	2								
	1								
	<1								
Criticality Matrix	Sev. Cat.	5	4T	4	3	2	1S	1	1SC
	Sev. Val.	1	2	3	4	5			
	Relative Severity of Failure Mode								

Likelihood of Occurrence	5						
	4						
	3						
	2						
	1						
	<1						
Criticality Matrix	Sev. Cat.	5	4T/4	3	2/1S	1/1SC	
	Sev. Val.	1	2	3	4	5	
	Relative Severity of Failure Mode						

Figure 11 - Threat Criticality Matrices

GSFC-HDBK-8004

Risk Priority Number	>26								
	21-25								
	16-20								
	11-15								
	6-10								
	1-5								
	<1								
Criticality Matrix	Sev. Cat.	5	4T	4	3	2	1S	1	1SC
	Sev. Val.	1	2	3	4	5			
	Relative Severity of Failure Mode								

Risk Priority Number	>26								
	21-25								
	16-20								
	11-15								
	6-10								
	1-5								
	<1								
Criticality Matrix	Sev. Cat.	5	4T/4	3	2/1S	1/1SC			
	Sev. Val.	1	2	3	4	5			
	Relative Severity of Failure Mode								

Figure 12 - RPN Criticality Matrices

Detection/ Prevention	5								
	4								
	3								
	2								
	1								
Criticality Matrix	Sev. Cat.	5	4T	4	3	2	1S	1	1SC
	Sev. Val.	1	2	3	4	5			
	Relative Severity of Failure Mode								

Detection/ Prevention	5								
	4								
	3								
	2								
	1								
Criticality Matrix	Sev. Cat.	5	4T/4	3	2/1S	1/1SC			
	Sev. Val.	1	2	3	4	5			
	Relative Severity of Failure Mode								

Figure 13 - D/P Criticality Matrices

Likelihood of Occurrence	5					
	4					
	3					
	2					
	1					
	<1					
Detection/ Prevention Matrix	D/P Val.	1	2	3	4	5

Figure 14 - D/P Matrix

(Advantageous to use before and after accounting for D/P within a FMECA to show effects)

- (iv) Risk/result summary – This is essentially the executive summary of the FMECA report. It should be able to be understood and have enough detail to be useable as a stand-alone reference. As such it should include:

- A list/depiction of the quantity of failure modes identified for each failure type
- Failure mode criticality communication matrices (e.g., threat and RPN at a minimum, shown above)
- CI overview and list (See [Section 4.3.3](#))
- Single Point Failure table and overview (See [Section 4.3.3](#))
- Risk statement (See [Section 4.3.5](#)) summaries

Ultimately, upon FMECA completion, findings must be communicated during each phase of development and operations so appropriate actions and decisions can be made. This can be done by sharing specific (or interim) results during working group discussion (e.g., fault management/FDIR), trade studies, safety/risk management, peer reviews, design reviews, test readiness reviews, and anomaly investigations and by sharing the formal report (See section 5.2) or results presentation. Fully communicating results will allow:

- System safety to respond to safety/inhibit related failure risks for inclusion in appropriate safety analysis and procedural control development.
- Quality/software assurance and stakeholders to make informed Use-as-Is decisions and verify that design and failure mitigation provisions are implemented, and requirements are met.
- Design/Systems teams to formulate/refine designs, testing, or operational concepts and define maintenance/refurbishment plans.
- I&T/Operations teams to diagnose and respond to issues in operations and testing.

Further, since a FMECA is a living analysis, it must be continually informed by other reliability analyses (including subordinate FMECAs), risk mitigations, changes in design and Safing/FDIR, specification-compliance issues or testing issues/results (e.g., revised detection signatures), and performance/operational changes to remain useful (see Section 4.4). These changes need to be

flowed to subordinate FMECA (e.g., specific system and/or vendor delivered FMECAs) analysts as well for the same purpose. This requires communication of these by vendors; design/systems, system safety, quality, and software assurance engineers; and I&T/operations teams to the FMECA analyst so updates can be made in a timely and effective manner. However, the FMECA analyst can also monitor I&T/operations progress for likelihood-reduction trigger updates, problem/failure reports for additional failure modes/signatures, and risk/CI control plans for design changes or likelihood adjustment (as well as facilitating the RMA evaluation of mitigation plans for additional risks prior to implementation).

5.2 Reporting

The RE should prepare a FMECA report that documents all the information included in the analysis methodology described above.

Each FMECA report will include the following data in a machine-readable format:

- Scope, type, indenture level, and operational scenarios/phases considered
- Methodology, Ground Rules, and Assumptions
- System/Item/Process description and Success Criteria
- Risks/Results Summary including failure mode matrices (Threat/RPN criticality matrices at a minimum). See Section 5.1 (iv)
- Critical Items List
- SPF Table
- Findings/Conclusions, Recommendations, Supporting Data, and Requirement Verifications (as applicable)
- Risk Statements for any proposed risks
- FMECA Failure Modes in a FMECA Table(s)/worksheet(s), or for legacy analysis, summary worksheet(s)
- FMECA Failure Mode Exclusion Table (noncredible failure modes list) if these are removed from the FMECA
- Subordinate/legacy analysis appendices

Note: The report template, found in [RMA SharePoint](#) and/or [Appendix C](#) can be used to facilitate reporting and analysis completeness.

A FMECA should be a living reference and updated as additional information becomes available (e.g., design details, operations/usage plan updates, test reports, performance data, issue logs). At PDR, the FMECA and its report should include the level of detail that is available. It is possible that FDIR designs will not be finalized at this point, but the FMECA can inform these efforts. For CDR, the previous versions of the FMECA analysis/report should be updated based on the details of the more mature/ detailed designs, subordinate FMECAs, and tests/verifications completed. This may add failure modes, controls, or risks, or it may make some previous failure modes noncredible. At TRRs for individual test-configurations (test-article and testing systems), any GSE FMECA (e.g., an interface FMECA or DNH FMECA) and report should include enough detail to ensure tests setups, connections, and operations are safe for both test-article and

testing systems. This will allow procedural and safety controls to be in place prior to any risk of hazard or failure. For Pre-ship/Operations Readiness Review (or Launch Readiness Review and Safety and Mission Success Review) the FMECA should be updated again with final designs, operational concept changes, and tests/verifications completed so the final pre-operations failure modes, controls, and/or risks are known and managed. During operations and maintenance/extension, the FMECA analysis/report should continue to be updated as warranted by the additional information received (e.g., pre-servicing/maintenance, post-servicing/maintenance, changes resulting from an anomaly or operational evolutions, and operational extension plans) so that decision makers and operations teams have up to date data for their action plans.

APPENDIX A – RECOMMENDED RELIABILITY PROGRAM PLAN WORDING

[Mission/Spacecraft/instrument/...] Failure Mode and Effects Analysis will be used to assess [hardware and software, process] failure mode effects using this handbook, MIL-STD-1629A, or similar methodology for [fault tolerance, risk, specific requirement verification...]. Analyses will quantify the likelihood, severity, mitigation, and prevention in a manner that facilitates mission risk assessment and critical item identification. In addition, single point failure (SPF) analyses will be performed on critical items/issues to identify/document failure causes, mitigation actions, risk, and retention / risk acceptance rationale.

Repeat the following for as many FMECAs as is being planned to support above:

For [spacecraft/instrument/...], [developer / responsible engineer] will perform a [FMECA type] on [Indenture level / scope] during [Operational phase / scenario].

[FMECA developer] or [spacecraft/instrument/...] or [responsible engineer] will continuously review and update the identified failure modes with design/operations changes and performance data to ensure that systems and subsystems have been properly analyzed and to confirm that each elements' performance requirements are met, and specified system/scenario fault tolerance is attained. [GSFC Mission Reliability will also incorporate the items into the mission-level FMECA(s).]

The resulting SPF and CI lists will provide Retention Rationale, Control/Action Plan, and FMEA-Mode Identifiers. SPF listings will also include mode characterization data - likelihood, causes, effects, risk level, and mitigations (current/planned).

APPENDIX B – FAILURE RISK CONTROL PLANS

Any risk identified by a FMECA can be managed or controlled by using NASA's NPR 8000.4 continuous risk management process shown below, but it is essential this be used for CIs and SPFs:

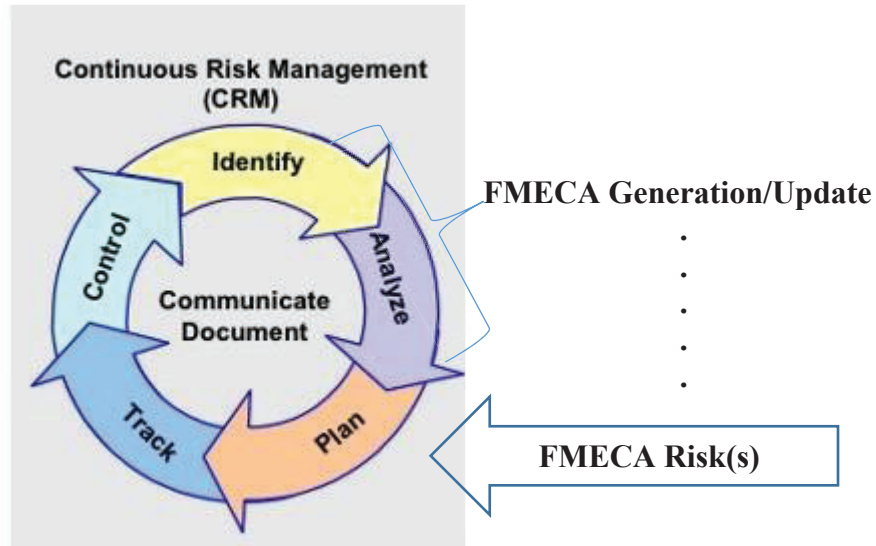


Figure B-1: Failure Risk Control via FMECAs and CRM Integration^{5,6}

The objective of the plan step is to decide what action (*Accept, Mitigate, Watch, Research, Elevate*), if any, should be taken to reduce the risks, i.e., to prevent the occurrence of consequence of a failure (See Figure B-2). Therefore, it is essential that any failure risk control plan have failure/risk description (including element/process, impacted systems/elements/processes, and causes), and mitigation/control/action objectives; delineate measures/actions/tasks to achieve mitigation/control/action objectives; be kept updated with actions taken/results, additional alternates, and risk/plan changes; and be communicated to all stakeholders. Many methods can be used to achieve this such as forms, spreadsheets, risk databases (highly recommended even if other methods are used to supplement), or monthly presentations. (See Examples in Figures B-3 – B-6).

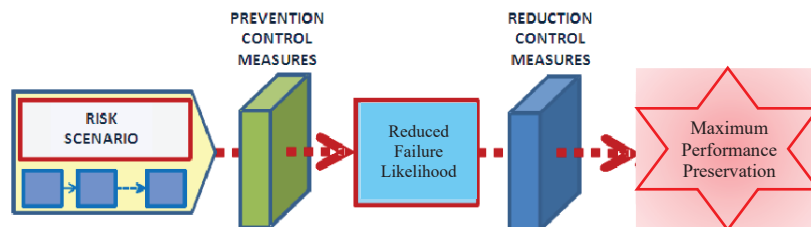


Figure B-2: Failure Risk Prevention and Consequence Reduction

⁵ <http://everyspec.com/ESA/download.php?spec=ECSS-Q-ST-10-04C.048172.pdf>

⁶ <https://www.nasa.gov/wp-content/uploads/2023/08/nasa-risk-mgmt-handbook.pdf>

GSFC-HDBK-8004

Critical Item Identification		CI no.	
System/Process/Mission –			
Subsystem/Procedure –			
Item/Step –			
Function –			
Title:			
Phase:			
Description of event (related critical situation(s)):			
Effects/Risks:			
Item Level –			
Next Level –			
Ultimate Level –			
Possible Cause(s):			
FMECA / Other Reference Source:			
Severity Rating:		Severity Category:	
Likelihood Rating:		Likelihood Value:	
Propagation (Y/N):		Propagation Time:	
Detection Rating:		Detection/Prevention Description:	
Single-Point Failure ☐ Yes ☐ No			
Applicable/Associated requirements:			
Item is confirmed as critical by	Discipline	Quality/SMA	Engineering
	Name Date Signature		
Critical Item Control Action Plan			
Action/Measure Proposed:	Actions Planned:		Action Status:
Resultant Risk Reduction Tracking (updated with each action or risk changed)	Risk_ID, Original LxC Risk_ID, Original LxC Risk_ID, Original LxC	New-1 LxC, date New-2 LxC, date New-2 LxC, date ... New-n LxC, date	☐ Open ☐ Open ☐ Open ☐ Open ☐ Watch ☐ Watch ☐ Watch ☐ Watch ☐ Accepted ☐ Accepted ☐ Accepted ☐ Accepted ☐ Closed ☐ Closed ☐ Closed ☐ Closed
Summary and Retention Rationale (including effectiveness of plan/actions, close-out plans/documents):			

Right Click to Open Document Above (save locally to use)

Project Plan for Mitigation Verification				
a. Item:		b. Status (month/day/year)		
c. Critical Item Control Plan (CICP) Number		d. Failure Mode Number(s)	e. Failure Mode(s)	
f.1 Have all mitigations been completed? ☐ Yes ☐ No		f.2 If Yes to f.1 are all mitigations' documentation provided? ☐ Yes ☐ No ☐ TBD Explanation (required for No/TBD):		
g. Mitigation				
#	Mitigation Identified on the CICP (Design, Review, Inspection, Test, Failure History, Operational Use, Handling)	Verifications	Documentation (Document, Section, Number, Step)	Status
1	<u>Design</u> -			
2	<u>Design</u> -			
3	<u>Handling</u> -			
4	<u>Inspection</u> -			
5	<u>Test</u> -			
6	<u>Review/Analyze</u> -			
n	<u>Etc.</u>			

Figure B-3: Examples of Forms for Control Plans

GSFC-HDBK-8004

Database Risk Report

RISK INFO

Last edited on 01/02/2024 by Nancy Lindsey

ID OCI-00302 Owner Nancy Lindsey Ranking Moderate Risk/Issue RISK Stage Open L C Related ID
 Date 01/02/2024 Author Nancy Lindsey Category Technical Risk Action Mitigate Timeframe Long-term Ranking 2 4
 Title FMECA Risk Risk Type Instrument-OCI Trigger FMECA Rev A Keywords WBS/System Level PAYLOAD, OCI Science (SCI)
 ELT Log #

Risk Statement

Given that <CI-failure mode, SPF, groupings of CI/SPFs, or other significant mode or item of concern >, has/have <likelihood of occurrence estimate-statement (including number or low/med/high)>,
 There is a possibility that < consequences – effect(s)> will occur,
 Resulting in <ultimate effect/ severity or purpose related consequence statement>

Context

The FMECA has identified the potential for a failure risk and It is recommends that (list as many as is applicable):

- o <Process recommendations such as procedure, operations, and parts controls changes.>
- o <Design recommendations such as software exception handling, redundancy increase, sensor optimization, and FDIR/Safing additions.>
- o <Planning recommendations such as contingency plans to be formulated to quickly respond to failure signatures. >

Cost

Min Impact Most Likely Impact Max Impact Schedule Min Schedule Most Likely Impact Max Impact
 Basis of Estimate Basis of Estimate

Mitigation Strategies

	Due Date	L	C	Plan	Completed	Cost	Min Cost	Max Cost	Actual Cost	Sched	Min Sched	Max Sched	Actual Sched
1. Research FDIR/redundancy solutions		0	0	Actions/Triggers: 1) Brainstorm failure mitigation solutions with SMA/RE and Science 2) Assess/Trade Cost/Schedule impacts 3) Select Solution									
2. Test solutions		0	0	Actions/Triggers: 1) Conduct mitigation testing on EDU during/after solution selected 2) Inform SMA/RE of results and system/ops changes 3) Conduct mitigation testing on Ops unit after solution implemented and assessed.									
3. Assess solutions for risks		0	0	Actions/Triggers: 1) Have SMA/RE re-assess failure risks and any solution resultant risks with Science and Systems collaboration.									
4. Implement solution in flight/operational system		0	0	Actions/Triggers: 1) Implement solution with Hardware/software assurance. 2) Update CONOPs and FMECA									
5. Monitor testing/operations for additional symptoms		0	0										

Status

Mitigation process begun.

MSR Status

Expected Closure Date

Currently Attached:

FMECA [CI/SPF].docx	2.01 MB	uploaded on 01/02/2024 11:32	EDIT	DELETE
---------------------	---------	------------------------------	------	--------

Figure B-4: Example of Control Plan & Tracking in a Risk Database

GSFC-HDBK-8004

Part/Process Number	Process Name / Work Description	Machine / Device / Jig / Tool	Characteristics			Special Characteristics	Method				Control Method	Reaction Plan
			No.	Product	Process		Production / Process Specification / Tolerance	Evaluation / Measurement Technique	Sampling			
									Qty.	Freq.		
10	Raw Material Incoming Inspection	Outsourcing	1	Spec		C	20Cr - 035	Quality certification	All		Quality Certification Required	Return to Supplier
			2	Chemical Composition		A	C: 0.18 – 0.24 S: 0.17 – 0.37 Mn: 0.50 – 0.80 Cr: 0.70 – 1.00	Spectroscopic analysis	1 pcs	Per lot		
			3	Surface		B	Without visible butt and stain	Visual inspection	2 pcs	Per lot		
20	Draw/Cut	Subcontract	11	Diameter		B	31.8 -0.05	Micrometer caliper	2 pcs	Per lot	Sampling	Return to Supplier
			12	Length		C	60 +1	Vernier caliper	2 pcs	Per lot		
30	Machine the two ends	C0625	21	Diameter		C	23±0.2	Micrometer caliper	10%	Per lot	Sampling	Rework / scrap
			22	Length		C	11.25 +0.4	Vernier caliper	10%	Per lot		
			23	Total Length		B	5.7 +0.03	Vernier caliper	20%	Per lot		

Figure B-5: Example of Control Plan & Tracking in a Spreadsheet

Project Failure Control Plan Item/System/Process:	
<u>Failure Risk:</u> <u>Objective:</u> <u>Significant Accomplishments :</u> <u>Budget Status/Tracking:</u>	<u>Schedule/Action Plan and Status:</u> <u>Points of Interest/Issues/Concerns</u>

Figure B-6: Example of Control Plan, Tracking, and Communication via Monthlies

APPENDIX C – FMECA CREDIBILITY DETERMINATION ASSISTANT

System/Process:						Authored By:	
FMECA Type:						Evaluation By:	
Indenture Level:		Scope: Ops/Use Phases:				Date/Milestone:	
ID		EVALUATION CRITERIA	RATING				COMMENTS
			Y	Y/N	N	N/A	
HIGH LEVEL DETAILS	1	Is the FMECA Strategy clear and complete? Type? Scope? Indenture-level? Usage/phase?					
	2	Are Methodology, Ground Rules (including RPN definitions), and Assumptions defined and explained?					
	3	Is Methodology, Ground Rules (including RPN definitions), and Assumptions consistent with GSFC-HDK-8004?					
	4	Is the System/Process definition and dependencies clear, complete (including block diagrams and drawing references), and up to date?					
	5	Are success (including duration) and failure definitions clear and documented?					
	6	Has a Critical Item List been supplied with failure modes identified for each item?					
	7	Has a SPF Table been supplied with retention rationale?					
	8	Are risks proposed and documented?					
ANALYSIS DETAILS	9	Have ALL failure modes been provided that are consistent with established strategy an include Local, Next Level, and Ultimate Effects? Do failure modes and their effects seem reasonable (do failure modes address the spectrum of likely failure modes and are the effects reasonable given the failure modes and applicable phase(s))? Are failure modes that were previously included that are now eliminated or determined noncredible noted?					
	10	Are all failure causes and mechanisms identified for each failure mode (fatigue, stress, environmental, interface, workmanship, software, etc.)? Are legacy/subordinate FMECA causal data included and cross referenced?					
	11	Has the likelihood been identified for each failure mode? Is duty cycle and other factors considered in likelihood?					
	12	Are mitigations/detections complete (capture each failure mode's signatures, symptoms, inhibits, controls, and impact-avoidance provisions (e.g., FDIR)), verifiable, and specific. Are related actions and update triggers noted?					
	13	Are RPN values/assessment consistent with RPN definitions and non-conflicting? Is the basis for the RPN value clear, cited, and reasonable? Are triggers for updates noted?					
	14	Are legacy/subordinate FMECAs or analyses attached/provided? Are failure mode data sources fully described/referenced?					
ANALYSIS RESULTS	15	Are results clearly summarized and actions/recommendations provided?					
	16	Are safety and mission success concerns/risks identifiable? Have safety concerns been coordinated with the program Safety Engineer?					
	17	Are risks identified and characterized?					
	18	Are failure mode impacts communicated (e.g., matrix provided) and comparable?					
	19	Are SPFs and CIs identified with retention rationale?					

Instructions on (Recommendations for) Use

In general, this Credibility Determination Assistant can be used in its entirety or to the extent needed by the FMECA analyst or the FMECA reviewer to make informed use determinations. Below is some general guidance on how to tailor the assistant depending on need:

Release Readiness and Peer Review: When evaluating an analysis for dissemination and use, the analysts themselves and peer reviewers can use the evaluation items as a checklist to ensure a quality product has been formulated. Thus, all evaluation items would be considered, but a credibility finding would not be generated.

Data Inclusion: When evaluating a legacy or subordinate analysis for inclusion in a larger system/process analysis, the validity of the failure modes and their characterizations may be all that needs to be assessed. Thus, only evaluation items 2, 9, 10, 11, and 12 may need to be performed to the extent needed to accurately incorporate that data. And an informal credibility opinion can be formulated and cited with the data's use.

Legacy Analysis Update: When evaluating a legacy analysis for updating, the analysts themselves can use the evaluation items to ensure the legacy product is worth updating and formulate a hitlist for improvement. Thus, all evaluation items would be considered, but a credibility finding would not be generated.

Risk Assessment: When using any FMECA to perform a risk assessment, it is essential that failure/faults are complete and characterized with at least likelihood and consequence. Thus, only evaluation items 9, 11, and 13 may need to be performed to the extent needed to accurately assess risk independently. But if a risk assessment has been included in the FMECA being evaluated, then evaluation items 8, 9, 11, 13, and 17 may be needed to ensure an accurate risk assessment is provided, and an informal credibility opinion can be cited with use of those risks.

CDRL Acceptance: When evaluating a delivered analysis for acceptance, the reviewer can use the evaluation items as a checklist to assess the quality of the product and formulate recommendations for improvement. Thus, all evaluation items would be considered (unless contractually excluded (e.g., MAR language, Data Item Description (DID), agreement) and a credibility finding formulated and shared.