

Standard

Capability-Based Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements

AIAA standards are copyrighted by the American Institute of Aeronautics and Astronautics (AIAA), 1801 Alexander Bell Drive, Reston, VA 20191-4344 USA. All rights reserved.

AIAA grants you a license as follows: The right to download an electronic file of this AIAA standard for storage on one computer for purposes of viewing, and/or printing one copy of the AIAA standard for individual use. Neither the electronic file nor the hard copy print may be reproduced in any way. In addition, the electronic file may not be distributed elsewhere over computer networks or otherwise. The hard copy print may only be distributed to other employees for their internal use within your organization.

American Institute of Aeronautics and Astronautics

**1801 Alexander Bell Drive, Suite 500
Reston, VA 20191-4344**

www.aiaa.org

ISBN 978-1-62410-377-3



Documents
Document Sharing Hub

American National Standard

Capability-Based Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements

Sponsored by

American Institute of Aeronautics and Astronautics

Approved 24 July 2015

American National Standards Institute

Approved 14 August 2015

Abstract

This Standard provides the basis for developing the analysis of failure modes, their effects, and criticality in the context of individual products along with the known performance of their elements. The requirements for contractors, the planning and reporting needs, along with the analytical methodology are established. The linkage of this Standard to the other standards in the new family of capability-based safety, reliability, and quality assurance standards is described, and keywords for use in automating the Product FMECA process are provided.

American National Standard

Publication	Date	Major Changes
S-102.2.4-2009	January 2009	• First publication
S-102.2.4-2015	August 2015	• Figure 1: Elements of Failure Mode Identification • Figure 2: Elements of Failure Probability Estimation • Definition for “failure mode, effects and criticality analysis (FMECA) capability level” • Definition for “safety-impact” • Annex E: Product Unit-Value/Safety-Impact Category Definitions • Annex F: Product FMECA Process Capability Levels versus Product Life Cycle

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA ON FILE

American National Standard

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to affirm, revise, or withdraw this standard no later than five years from the date of approval. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

American Institute of Aeronautics and Astronautics
1801 Alexander Bell Drive, Reston, VA 20191

Copyright © 2015 American Institute of Aeronautics and
 Astronautics

All rights reserved

No part of this publication may be reproduced in any form, in an electronic retrieval system
 or otherwise, without prior written permission of the publisher.

Printed in the United States of America

Table of Contents

Foreword	vi
1 Scope	1
1.1 Purpose	1
1.2 Application	2
2 Applicable Documents	5
2.1 Normative AIAA References	5
2.2 Other References	5
3 Vocabulary	6
3.1 Acronyms and Abbreviated Terms	6
3.2 Terms and Definitions	6
4 General Requirements	11
4.1 Contractor Responsibility	11
4.2 Procedure	11
4.3 Product FMECA Report	12
5 Detailed Requirements	13
5.1 Define Product FMECA Ground Rules	13
5.2 System Design Data Collection	13
5.3 Failure Mode and Effects Analysis	13
5.4 Criticality Analysis	15
5.5 Detectability Analysis	16
5.6 Failure Isolation Analysis	16
5.7 Safety, Mission, and Maintainability Critical Items Analyses	16
5.8 Failure Compensation Method Analysis	16
5.9 Integrated Product FMECA/Hazards Analysis Database	16
5.10 Data Exchange Between Product FMECA Process And Other Project Functions	18
5.11 Product FMECA Input Data Maturity Evaluations	18
5.11.1 Failure Mode Analysis Input Data Maturity Categories	18
5.11.2 Failure Compensation Method Input Data Maturity Categories	18
5.12 Structured Review	19
5.13 Lessons Learned	19
ANNEX A - Safety, Reliability & Quality Assurance Processes	A-1

ANNEX B - AIAA S-102 Product FMECA Capability Level Requirements	B-1
ANNEX C - AIAA S-102 Product FMECA Keyword Data Element Descriptions	C-1
ANNEX D - AIAA S-102 Criticality Analysis Requirements	D-1
ANNEX E - Product Unit-value/Safety-impact Category Definitions (Example)	E-1
ANNEX F - Product FMECA Process Capability Levels Versus Product Life Cycle	F-1
ANNEX G - Bibliography	G-1

Figures

FIGURE 1: ELEMENTS OF FAILURE MODE IDENTIFICATION	3
FIGURE 2: ELEMENTS OF FAILURE PROBABILITY ESTIMATION	4
FIGURE 3: FAILURE PROCESS FLOW	14
FIGURE D-1: EXAMPLE CRITICALITY/RISK MATRIX WHICH IS CONSISTENT WITH MIL-STD-882E RISK MATRIX	D-6

Tables

TABLE 1: AIAA S-102 FAILURE MODE/HAZARD SEVERITY CATEGORIES	15
TABLE 2: PRODUCT FMECA FAILURE MODE ANALYSIS INPUT DATA MATURITY CATEGORIES...	18
TABLE 3: FAILURE COMPENSATION METHOD INPUT DATE MATURITY CATEGORIES.....	19
TABLE D-1: FAILURE PROBABILITY LEVEL DEFINITIONS.....	D-2
TABLE D-2: EXAMPLE CRITICALITY ANALYSIS WORKSHEET	D-3
TABLE D-3: FAILURE EFFECT PROBABILITY (β)	D-4
TABLE F-1: EXAMPLE PRODUCT FMECA PROCESS CAPABILITY LEVELS VERSUS PRODUCT LIFE CYCLE	F-1

Foreword

Mission Assurance is the project-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to system safety or mission success, throughout the product's useful life and post-mission disposal. Quality, system safety, and reliability are the major components of mission assurance. Although these three terms are often used interchangeably they have different meanings. Quality as used in this Standard is the ability of a product to meet the workmanship criteria established by an organization. A different, but often used, definition of quality: Quality is the set of all desired attributes that can be put in a product. In this sense, quality cannot be achieved without achieving the desired safety. Safety is the freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. Reliability is the ability of a product or system to perform its intended function(s) for a specified time or operating cycles. A high-quality product may not be a high-safety or high-reliability product even though it conforms to stringent workmanship specifications. The ISO 9000 series standards that establish the ability of an organization to consistently produce high-quality products do not necessarily establish that same organization's ability to consistently deliver high-safety and high-reliability products. Consequently, the ISO 9000 series certification process, which serves as the main international reference for Quality Program requirements in business-to-business dealings, is not the appropriate reference for international or domestic safety, reliability, and quality assurance program (SR&QA) requirements. More suitable references are the AIAA S-102 Mission Assurance standards, which provide a uniform framework for performing Safety, RAM, and QA (SR&QA) risk management in a manner which is commensurate with the product unit-value/safety-impact and systems engineering phase. See Annex E for an example categorization of various products by their respective unit-values and safety-impacts. See Annex F for an example matrix showing the Product FMECA process capability levels versus the product life cycle.

This Standard establishes uniform requirements for a capability-based Product FMECA. The principles of the Product FMECA as promoted in a capability-based approach can be learned from this Standard, but its proper use requires comprehensive planning, which includes understanding the requirement FMECA input and output data in the Systems Engineering Process. What distinguishes this Standard from all past and present Product FMECA standards is the following:

- it provides consistent criteria for rating the “capability” of an organization's Product FMECA process to identify, analyze, and manage failure mode risks in a manner which is commensurate with the product's unit-value/safety-impact and systems engineering life cycle phase.
- for a Capability Level 3 or above FMECA process, it calls for the collection and review of existing lessons learned, and the generation and formal approval of new lessons learned.
- for a Capability Level 4 or above Product FMECA process, it provides consistent criteria for rating the “maturity” of the Product FMECA input data.
- for a Capability Level 4 or above Product FMECA process, it calls for the use of predefined mission assurance data parameters to facilitate the exchange of Product FMECA data among computer-aided analysis tools and other project databases.

At the time of approval of this Standard the members of the S-102 Mission Assurance Standards Working Group were:

S-102 MASWG PARTICIPANT	INTEREST CATEGORY
Tyrone Jackson	General Interest
James E. French	General Interest
Diana DeMott	Practitioner
Alazel Jackson	Practitioner
Jan Swider	Producer
Pat Branch	Producer
Gregory E. Tarver (Observer)	User
Nathan Holt	User

The definitions for the S-102 MASWG participant interest categories are as follows:

- Producer - Authorized to represent a company that is engaged in the manufacture of products covered by the committee. A company that contracts out operations but still retains control over the process.
- User - Authorized representative of a company or organization whose primary activity causes it to use or employ the products, goods, or services that are affected by the standards developed by the particular committee. A consultant whose primary business involves representing Users is considered to be in this category).
- Practitioner – Subject matter expert of one or more mission assurance processes.
- General Interest

The above consensus body approved this document on 28 April 2015.

The AIAA Standards Executive Council (VP-Standards Laura McGill, Chairman) accepted this document for publication on 24 July 2015.

The AIAA Standards Procedures dictates that all approved Standards, Recommended Practices, and Guides are advisory only. Their use by anyone engaged in industry or trade is entirely voluntary. There is no agreement to adhere to any AIAA standards publication and no commitment to conform to or be guided by standards reports. In formulating, revising, and approving standards publications, the committees on standards will not consider patents that may apply to the subject matter. Prospective users of the publications are responsible for protecting themselves against liability for infringement of patents or copyright or both.

Downloaded from [AVIA](#) on 04/11/2015

1 Scope

This Standard establishes uniform requirements and criteria for a capability-based Product Failure Mode, Effects and Criticality Analysis (FMECA). The capability-based aspect of this Standard requires that the organization's FMECA capability be rated according to defined criteria for process capability and data maturity. The structured process that this Standard defines integrates the FMECA process with other mission assurance processes within systems engineering to identify, analyze, and manage failure mode risks in a manner which is commensurate with the product's unit-value/safety-impact and systems engineering life cycle phase. Also, it facilitates integrating FMECA data across different enterprises.

1.1 Purpose

The primary purpose of the Product FMECA is to collect and evaluate the necessary product design information to identify and eliminate or control, but not be limited to, all failure modes that pose unacceptable risk to system safety or mission success. Depending on how it is performed, the FMECA can be used for several different purposes, but its most important use in systems engineering is to aid the improvement of design safety or design reliability before the product design is solidified or product is manufactured. The capability-based FMECA is a set of activities that address product failure or mishap risk at one or more defined capability levels.

A failure mode is the consequence of the mechanism through which the failure occurs, i.e., the manner by which the failure is observed. Accordingly, a failure mode that poses unacceptable risk is a failure mode whose effect, either singularly or in combination with other failure mode effects, violates a product design requirement or goal. The FMECA is a systematic methodology that is widely used to evaluate the effects on systems and interfaces caused by the failure modes of functional, physical, or logical components. It supports estimating the criticality or risk of each failure mode in terms of its end-effects, and evaluates the appropriate failure compensation methods for safety-critical, mission-critical, and maintenance-critical failure modes. The Product FMECA shall comprise the following three components:

- Failure Mode and Effects Analysis (FMEA)
- Criticality Analysis (CA), and Detectability Analysis for repairable products
- Critical Item (CI) Analysis and Failure Compensation (FC) Analysis

The FMEA answers system failure questions regarding the *what's, how's, where's, when's, and why's*. The CA and the detectability analysis answer system failure questions regarding *relative significance*. The CI analysis and the FC analysis answer system failure questions regarding *failure mitigation*. The minimum activities that constitute the baseline practice for the Product FMECA are the following:

- establishment of the requirements and analytical ground-rules for the Product FMECA;
- establishment of Product FMECA Technical Performance Metrics (TPMs);
- collection and evaluation of the necessary product design information to identify and evaluate, but not be limited to, all failure modes that pose unacceptable risk across the product life cycle;
- selection and approval of a single FMECA worksheet format for the entire project, including the subcontractors and suppliers (this activity facilitates integrating the FMECA data across different enterprises);
- identification and documentation of the product's failure modes, failure effects, and failure mechanisms, root causes, or hazards, as required, based on failure mode models obtained or developed for each functional or physical element in the product;
- identification of product design features and operational activities that reduce the likelihood or manage the effects of failure modes;

- calculation of a quantified Criticality Number (Cm) for each failure mode;
- development of a qualified or a quantified detection success probability for each failure mode of a repairable system;
- application of Critical Item (CI) selection criteria and evaluation of failure mode mitigation approaches for each CI;
- development, documentation, and distribution of the Product FMECA Report.

The elements of failure mode identification are shown in Figure 1 and the elements of failure probability estimation are shown in Figure 2. These elements shall be included in the FMECA process as required.

1.2 Application

This Standard applies to acquisitions for the design, development, fabrication, test, and operation of commercial, civil, and military systems, equipment, and associated computer programs. This Standard provides a consistent approach for rating an organization's Product FMECA process capability by applying a five-level set of criteria. These criteria are based on performing a logical sequence of activities that improves the accuracy and comprehensiveness of the Product FMECA as the product advances through its life cycle in phases. Organizations may evaluate their existing Product FMECA processes against the criteria in Annex B to identify the additional features needed to achieve a target process capability level.

This Standard also applies to the integration of the Product FMECA/Hazards Analysis database with a Project Mission Assurance Database System. However, specification of this Standard shall not be construed as a requirement for the contractor to use a particular computer-aided design (CAD) system. Rather, contractors shall use the computerized tools of their choosing, given that those tools are validated to process input data and generate output data in formats that are compatible with the data definitions in this Standard.

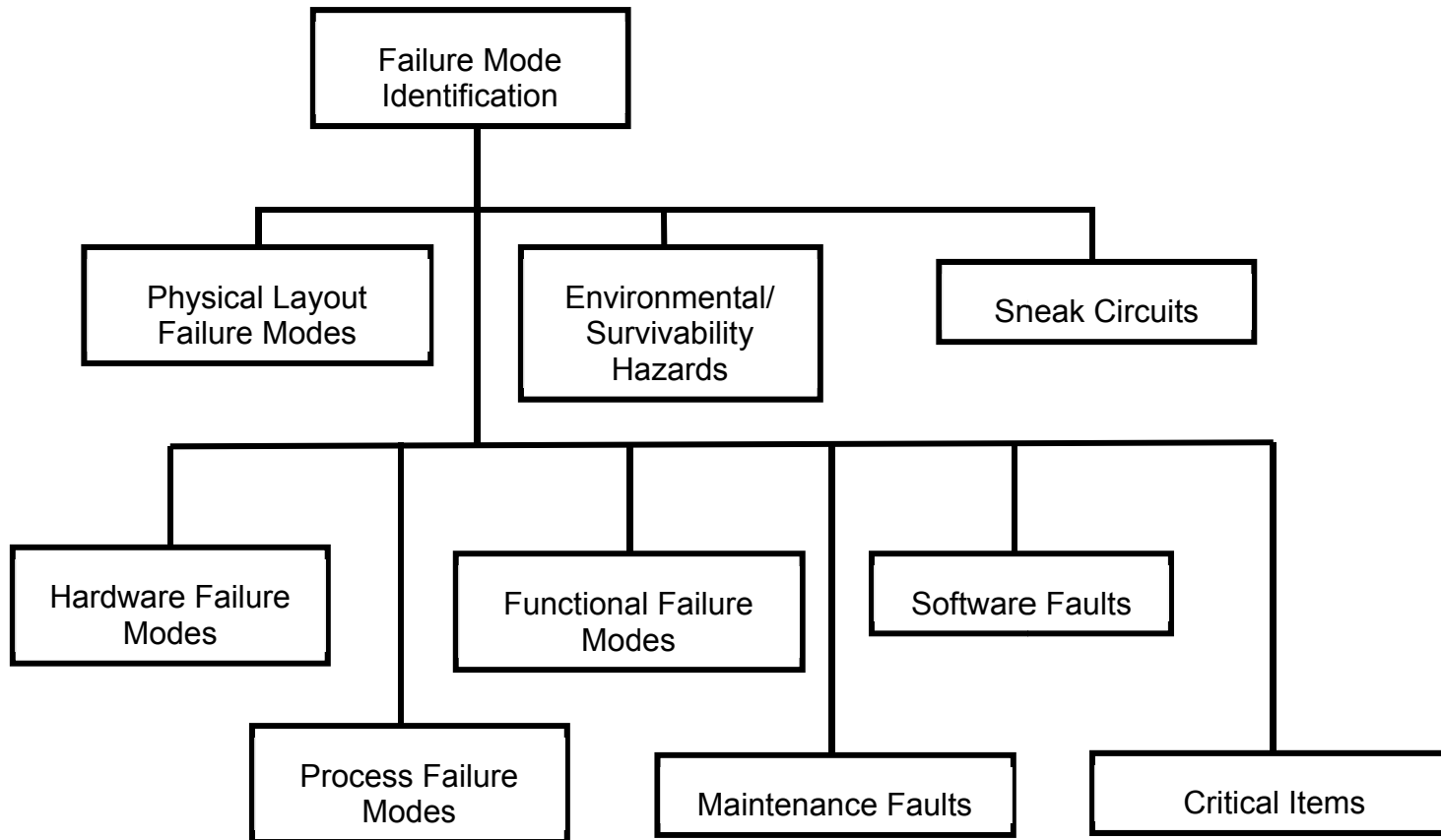


FIGURE 1: ELEMENTS OF FAILURE MODE IDENTIFICATION.

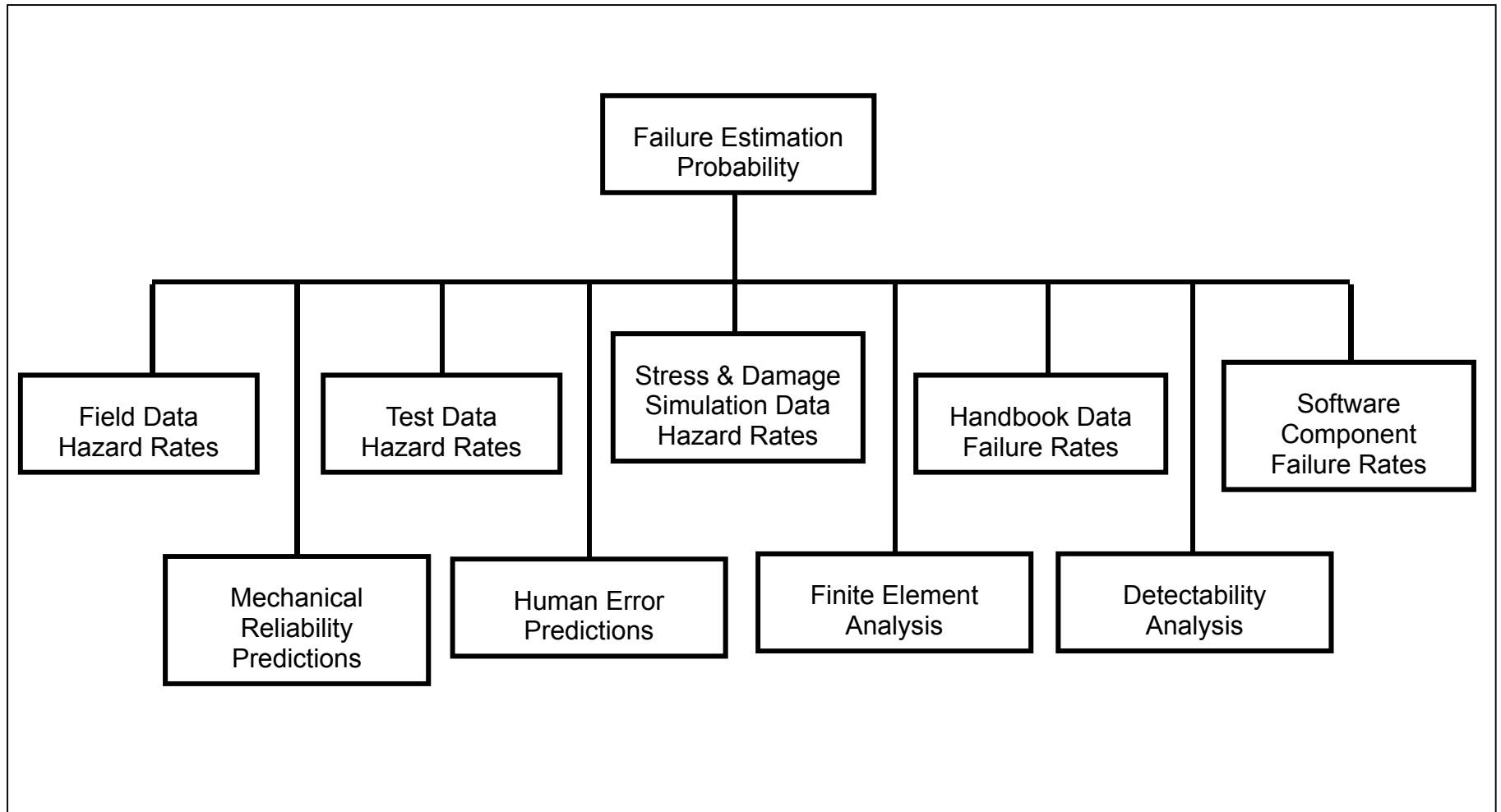


FIGURE 2: ELEMENTS OF FAILURE PROBABILITY ESTIMATION.

2 Applicable Documents

2.1 Normative AIAA References

The following reference documents of the issue in effect on the date on invitation for bid or request for proposal form a part of this Standard to the extent specified:

- 1) AIAA Standard S-102.1.4-2009 Failure Reporting, Analysis and Corrective Action System (FRACAS) Requirements
- 2) AIAA Standard S-102.1.5-2009 Failure Review Board Requirements
- 3) AIAA Standard S-102.2.2-2009 System Reliability Modeling Requirements
- 4) AIAA Standard S-102.2.5-2009 Sneak Circuit Analysis Requirements
- 5) AIAA Standard S-102.2.11-2009 Anomaly Detection and Response Analysis Requirements
- 6) AIAA Standard S-102.2.18-2009 Fault Tree Analysis Requirements
- 7) SEA-GEIA-STD-0007 Logistics Product Data
- 8) SEA-GEIA-HB-0007 Logistics Product Data Handbook
- 9) SEA-TA-HB-0007-1 Logistics Product Data Reports
- 10) SAE TA-STD-0017 Product Support Analysis

2.2 Other References

This Standard defines requirements for a capability-based FMECA, which is one of 38 SR&QA processes identified in Annex A. There are domestic and international standards that address most of these SR&QA processes. The SR&QA standards define the activities and data products that aid the identification, assessment¹, and management of failure mode risk for items from the lowest to the highest system indenture level.

¹ Assessment as used here includes qualification and quantification, and numerical evaluation and ranking of failure mode risks.

3 Vocabulary

3.1 Acronyms and Abbreviated Terms

CA	Criticality Analysis
CI	Critical Item
Cm	Criticality Number
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
H/W	Hardware
ILS	Integrated Logistics Support
PMP	Parts, Materials and Processes
QA	Quality Assurance
R&M	Reliability and Maintainability
SPFM	Single Point Failure Mode
SE	Systems Engineering
SR&QA	Safety, Reliability & Quality Assurance
S/W	Software

3.2 Terms and Definitions

acquisition activity

activity (Government, contractor, or subcontractor) that levies Product FMECA requirements on another activity through a contract or other document

ambiguity group

set of components that, if considered potentially faulty, does not give a unique solution in fault location

baseline practice

minimum set of activities that constitute an AIAA S-102 Capability Level 1 RAM practice

capability level growth

improvement in the ability of a task to support the systems engineering objectives due to an increase in resources, engineering data processed, or number of other tasks supported

capability-based Mission Assurance Program

concept of a coordinated effort among the project domains of safety, R&M, and quality assurance to assess and control product deficiency risk at one of five predefined capability levels

NOTE: Same as a capability-based SR&QA Program

capability-based SR&QA Program

concept of an coordinated effort among the project domains of safety, R&M, and quality assurance to assess and control product deficiency risk at one of five predefined capability levels

NOTE: Same as a capability-based Mission Assurance Program

credible failure mode

failure mode with a probability of occurrence greater than 1.0E-6, 0.000001, or one in a million

criticality analysis

grouping of probability of occurrences for failure modes according the Severity Category

NOTE: Each failure mode probability of occurrence represents a Criticality Number (Cm).

criticality analysis record

the full description a single criticality number.

data maturity level

a measure of correlation, in terms of one of three predefined data maturity levels (see Table 2), between specific types of input data and the degree of accuracy to be expected

detectability analysis

assessment of the means or methods by which a failure is detected, isolated by operator and/or maintainer and the time it may take

failure

termination of the ability of a unit to perform its required function

NOTE: A fault may cause a failure.

failure mode

consequence of the mechanism through which a failure occurs, or the manner by which a failure is observed

failure mode, effects and criticality analysis (FMECA)

the determination and documentation of a product's failure modes, and their effects and criticality (i.e. the relative measure of the consequences of the failure modes and their frequency of occurrences) through a systematic analysis of the design

failure mode, effects and criticality analysis (FMECA) capability level

measure of the ability of an FMECA process, as specified by a set of activities, to address the pertinent failure mode identification needs of a product that has a specific unit-value criticality and systems engineering phase (see Annex B for FMECA capability level definitions)

fault²

[1] [Software reliability] a manifestation of an error in software; [2] [Hardware reliability] any undesired state of a component or system; [3] [Components] a defect or flaw in a hardware or software component; [4] [Human reliability] procedure (operational or maintenance) or process (manufacture or design) that is improperly followed;

NOTES: [1] An accident may cause a fault; [2] a fault may cause a failure; [3] a fault does not necessarily require failure.

² Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

hazard

A hazard consists of a source of the problem, a mechanism that triggers the event, and an outcome which is the result. It is a condition that is prerequisite to a mishap and a contributor to the effects of the mishap

NOTE: A single point failure mode (SPFM) item is a hazard with respect to its potential to lead directly to loss of a safety-critical or mission-critical system function.

FMEA record

the full description a single failure mode.

FMECA worksheet

A documented that describes the failure modes and their effects, root causes, detection methods, severity categories, likelihood categories, criticality numbers, detection risk priority numbers, and compensation methods of an item

independent verification

provision of sufficient information for an organization or individual to obtain the same results as the analysts when redoing the analysis

inherent failure mode

result of characteristic weaknesses related to specified design and materials of an item

method

a formal, well-documented approach for accomplishing a task, activity, or process step governed by decision rules to provide a description of the form or representation of the outputs, i.e. a procedure

mishap

an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

mission

the purpose and functions of the space system (sensors, transponders, boosters, experiments, etc.) throughout its expected operational lifetime, and controlled reentry or disposal orbit time period. A space system may have several missions (e.g., primary mission, ancillary mission, and safety mission)

mission assurance

that part of Systems Engineering (SE) that focuses on identifying, evaluating, and mitigating or controlling existing and potential deficiencies that pose a threat to system safety or mission success, throughout the system's useful life and post-life disposal

NOTE: Deficiencies include damaging-threatening hazards, mission-impacting failures, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

non-credible failure mode or hazard

a failure mode or hazard with a probability of occurrence equal to or less than $1.0E-6$, 0.000001 , or one in a million

NOTE: Same as an improbable failure mode or hazard

opportunity

a chance to eliminate, avoid, or reduce a negative consequence

plan

an approach or method to achieve an objective

planning

the act of developing a problem description, one or more objectives to solve the problem, and an approach or method to achieve each objective

practice

one or more activities that use specified inputs to develop specified work products for achieving specified objectives (Ref. IEEE Standard 1624-2008)

procedure

an ordered set of specific activities that define a particular approach, i.e. a method

process-based lesson learned

important information created, documented, and retrieved according to a process or procedure descriptor

product-based lesson learned

important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor

prognostics

identifying conditions or clues that indicate imminent failure prior to its occurrence

propagating failure mode

irreversible physical and/or functional damage that is propagated across the interface as a result of failures in one of the interfacing units.

risk

risk (hardware) the combination of the severity of the event and the probability that it will occur; (2) (software) the combination of the severity of the event and the level of control the software exercises over the physical process. It is a future event that has some uncertainty of occurrence and negative consequence if it were to occur

NOTE: Risk can be associated with all aspects of a project (e.g., threat, technology maturity, supplier capability, design maturation, and performance against the plan), as these aspects relate across the Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS).

safety

freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

safety-critical

a term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component

safety-Impact

The level of safety risk to the environment, the occupational health of personnel, and other operational systems, caused by a system or end item when employed in an operational environment.

Note: This definition is similar to the definition for "Operational Safety" found in FI63-101/20-101. The difference being, the assessment of risk that a system may harm itself is addressed as part of mission success assurance, not by system safety engineering.