ANSI/AIAA S-102.2.4-2015

Standard

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

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

ANSI/AIAA S-102.2.4-2015

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

Printed in the United States of America

ISBN 978-1-62410-377-3

Table of Contents

Figures

Tables

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 dictate 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.

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;