ANSI/AIAA S-102.0.1-2019

Standard

Capability-based mission assurance program – General requirements

AIAA

American National Standard

Capability-based mission assurance program – General requirements

Sponsored by

American Institute of Aeronautics and Astronautics

Approved 8 July 2019

American National Standards Institute

Approved 16 September 2019

Abstract

This Standard provides requirements and guidance for implementing a capability-based Mission Assurance Program (MAP), that achieves system safety and mission success requirements through the integrated execution of Safety, RMAT (Reliability, Maintainability, Availability, and Testability), and Quality Assurance best practices, which are prescriptively tailored to eliminate or control unacceptable technical risks throughout the system life cycle. The linkage of this Standard to other standards in the family of S-102 capability-based mission assurance standards is described, and an example set of data element descriptions (DEDs) that can be used to manage MAP data transfer and storage between and within organizations, is provided in Annex E.

LIBRARY OF CONGRESS CATALOGING DATA WILL BE ADDED HERE BY AIAA STAFF

Published by

American Institute of Aeronautics and Astronautics

12700 Sunrise Valley Drive, Reston, VA 20191

Printed in the United States of America

ISBN: 978-1-62410-594-4

Contents

Table...

Figures

Foreword

Mission Assurance is an outcome of a combination of properly applied best practices for System Safety, RMAT (i.e. Reliability, Maintainability, Availability, and Testability), and Quality Assurance, as opposed to being a separate discipline, process, or design consideration. In addition to Mission Assurance, best practices for Design, Manufacturing, Test, and Operations are also necessary to prompt confidence in the contractor's ability to deliver a system that is operationally safe, reliable, suitable, and effective during mission operations and post-mission disposal operations.

Capability-based Mission Assurance is achieved through prescriptive tailoring of best practices in System Safety, RMAT, and Quality Assurance (SR&QA). The primary objective of the Mission Assurance Program (MAP) is to plan and implement a set of SR&QA processes to identify, assess, and eliminate or control unacceptable system safety and mission success risks. These unacceptable risks may be realized at any point in time during the system life cycle, i.e. system definition, preliminary design, critical design, manufacturing, testing, storage, transportation, checkout, mission operations, and post-mission disposal. Note there is no universal list of unacceptable system safety and mission success risks that are applicable to all types of systems. However, similar systems will generally have the same types of unacceptable risks. Note the term *Mission Assurance* and the acronym SR&QA are used interchangeably throughout this Standard.

There are five non-normative annexes in this Standard. Annex A lists the forty-one basic Mission Assurance processes. Annex B describes the groups of activities that constitute the five capability levels of each SR&QA process described a MAP. Annex C describes the scope and purpose of each SR&QA process described in the forty-one process-level Mission Assurance standards. The SR&QA processes are grouped technically according to system safety, RMAT, and quality assurance programs, and programmatically according to Program Managerial, engineering, and testing functions. The standard system life cycle phases for all systems is shown in Table 3. Annex D provides an example of a systems safety-critical and mission-critical unacceptable conditions checklist. Annex E provides an example library of MAP data element descriptions (DEDs).

Note this Standard defines the *"what to do's"* at the depth necessary to facilitate consistency in planning and implementing a cost-effective SR&QA program. Generally, this Standard is intended to aid users to identify, assess, and mitigate or control SR&QA risks that are commensurate with the product's unit-value/mission-criticality and system life cycle data content/maturity. Specifically, this Standard is intended to be used for the following purposes:

1. To specify a minimum level of capability-based Mission Assurance in a Statement of Work (SOW), Memorandum of Agreement (MOA), or equivalent contractual document;
2. To plan the SR&QA activities needed to achieve a specific level of Capability-based Mission Assurance;
3. To consistently appraise the collective effectiveness of SR&QA activities performed on a system; and
4. To aid any type or size of engineering organization, ranging from one-person micro-companies to multi-division mega-corporations, in verifying that standard technical best practices are applied to the products and services delivered.

For a Capability Level 4 or above MAP, this Standard calls for the use of predefined mission assurance data parameters to facilitate the exchange of MAP data products 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	Chair/General Interest
Alazel Jackson	Industry
Diana Lynn DeMott	User
Pat Branch	Industry

Dana Tripp	Government
Eric Dela Cruz	Industry
Dr. Jan Swider	Producer
Willie Bell	Academia
Tim Riley	Academia
Janice Shanks	User
Allura Jackson	Academia
Valerie Robinson	Government
Bill Kude	User
Goncalo Esteves	Industry

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

- Academia — An individual from an educational institution (university and/or college) whose area of instruction and/or research is within the scope of the committee.
- General Interest — A General Interest organization or company is one that does not fit into the other categories listed. An individual from a company or organization (including a consultant) that regularly represents two or more interest categories may be classified as General Interest.
- Government — An individual from a governmental (State and Federal) organization that produces, uses, or regulates materials, products, systems, or services within the scope of the committee. Any branch of the U.S. military or any Federal or State agency (that is not classified as having jurisdiction over the implementation of a standard) will be classified as Government. A consultant whose primary business involves representing Government is considered to be in the Government interest category.
- Industry — An individual from a private organization that produces, purchases, sells, or uses materials, products, systems, or services within the scope of the committee.
- Producer — An individual who is authorized to represent a company that is engaged in the manufacture of products covered by the committee. A company that contracts out operations such as fabrication and/or assembly, but still retains some control of the overall production process, including for example, performance of such major functions as research and development, design, ownership of tools and dies, production scheduling, quality control, and wholesale distribution, is also considered to be a producer. A consultant or agent who is authorized to represent a manufacturer is considered a producer.
- User — An 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 User may also be an organization that represents the health and safety interests of the general public or of specific groups, including workers. A consultant whose primary business involves representing Users is considered to be in the User interest category.

The above consensus body approved this document on 8 Jul 2019.

The AIAA Standards Steering Committee (SSC) accepted this document for publication on 7 Sep 2018.

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.

THIS PAGE INTENTIONALLY LEFT BLANK

Introduction

The terms *System Safety, RMAT* and *Quality Assurance* are often used interchangeably, but they have very different meanings. *System Safety* is the acceptable level of risk for conditions, items, or systems that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. *RMAT is Reliability, Maintainability, Availability, and Testability. Reliability* is the probability that an item or system will perform a required function without failure under stated conditions for a stated period of time or number of cycles. *Maintainability* is the measure of the ability of an item or system to be retained in or restored to a specified condition. *Availability* is the probability that an item or system will perform as required and when required. *Testability* is the degree to which an item or system supports testing in a given test context. *Quality Assurance* is the part of quality management focused on providing confidence that quality requirements are fulfilled.

The scope and purpose of forty System Safety, RMAT and Quality Assurance (SR&QA) processes are described in Annex C. The SR&QA processes are grouped programmatically according to separate safety, RMAT, and quality assurance domains, and functionally according to documented management, engineering, and testing approaches. Annex B defines the tiered criteria used for rating the SR&QA risk management capability of an existing SR&QA program or for planning the desired SR&QA risk management capability of a new SR&QA program. The unique provisions of this Standard include the following:

- Consistent criteria (see Annex B) for rating the capability of SR&QA program to identify, analyze, and mitigate or control, potential and existing, product and process deficiencies in a manner that is commensurate with the product's unit-value/mission-criticality (see Table 2) and system life cycle data content/maturity (see Table 3);
- Structured planning to achieve a predefined level of SR&QA risk management capability for the overall SR&QA program or any individual SR&QA process through a statement of work (SOW), memorandum of agreement (MOA), or similar quid pro quo artifact;
- Collecting, reviewing, and applying existing lessons learned for rating the maturity of input data used for performing SR&QA analyses;
- Creating and disseminating new lessons learned to sustain continuous improvement of the SR&QA program throughout the enterprise;

1 Scope

This Standard applies to the design, development, fabrication, test, and operation of commercial, civil, and military systems, sites, facilities, services, devices, and software that are used in ground, nautical, aeronautical, and space missions. Criteria is provided for rating the capability of the entire Safety, RMAT, and Quality Assurance (SR&QA) program or an individual SR&QA process, with regard to the identification, assessment, and elimination or control of unacceptable risks that threaten system safety or mission success. The capability rating criteria defined in this Standard identifies the activities needed to achieve a measurable improvement in the effectiveness of SR&QA risk management in stages. Organizations may evaluate their existing SR&QA program against the criteria in this Standard to identify the activities that need to be added, deleted, or modified to achieve the project's acceptable level of technical risk management effort. The phrase "acceptable level of technical risk" means that the activities and resources used to identify, assess, and eliminate or mitigate technical risks are commensurate with the product's unit-value/mission-criticality and system life cycle data content/maturity.

This Standard provides prescribed-tailoring of SR&QA programs that are capable of achieving the following objectives concurrently: (1) successful completion of project milestones; (2) effective mitigation of technical risks (i.e. optimally eliminating, reducing, controlling, transferring, avoiding, accepting, and monitoring risks); and (3) efficient improvement of the technical risk assessment process. See Figure C-1 for a notional view of this concept.