INTERNATIONAL STANDARD

ISO 22893

First edition
2022-04

Space systems — Software product assurance (SPA)

Systèmes spatiaux — Assurance produit logiciel (SPA)

Reference number
ISO 22893:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The objectives of software product assurance are to provide adequate confidence to the customer and supplier that the software satisfies its requirements throughout the system lifetime.

This document describes a set of product assurance activities related to software engineering and software safety to be used for the development, maintenance and operation of software for space systems. These activities deal with management and engineering process, life cycle models, assessment and improvement processes, in summary, the quality and safety characteristics of software space products.

Space systems include manned and unmanned spacecraft, launchers, payloads, experiments and their associated ground equipment and facilities. Software includes ground and on-board applications.

Space software can be divided into two macro areas for its development, maintenance and operations: the space software segment and the ground software segment. The space software segment is the software embedded in the vehicle which flies into space (on-board computer, payload platform, etc.); and the ground software segment is the software of the equipment on ground during the launch or during the control the spacecraft (telemetry stations, control bench for launch, satellite control, etc.).

This document does not distinguish between software product assurance and software safety, dependability and quality assurance roles. Software product assurance is a management process that integrates software safety, software dependability and software quality assurance. The purpose is to organically integrate safety, dependability and quality assurance activities. As a result, the goal of providing safe and reliable products that meet customer requirements is that these three areas work closely in tandem.

The purpose of this document is to identify a set of management guidelines and requirements for dealing with space systems engineering activities and is intended to define the minimum existing processes on the subject seeking to reach an international agreement on the topic.

Space systems — Software product assurance (SPA)

1 Scope

This document defines a set of software product assurance requirements in terms of processes and products to be used for the development, maintenance and operation of software for space systems. It provides a uniform basis for defining the software product assurance activities to be applied and maintained throughout the whole software life cycle, from project conception until the software retirement.

This document mainly applies to the space software segment and critical software of ground software segment (e.g. the software which is directly interface to the space segment).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9000, *Quality management systems — Fundamentals and vocabulary*

ISO 10795, *Space systems — Programme management and quality — Vocabulary*

ISO 14300-2, *Space systems — Programme management — Part 2: Product assurance*

ISO 16404, *Space systems — Programme management — Requirements management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 9000, ISO 10795, ISO 14300-2 and ISO 16404 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Software product assurance overview

4.1 General

Software product assurance (SPA) is an activity that ensures the success of a software project; therefore this is the main objective of the software safety, dependability and quality. Success is based on the assurance of the development, maintenance and operation of software requirements in terms of meeting the interest of stakeholders, estimating costs, setting schedules and achieving results.

In this regard, SPA has a high level of administrative role; and software safety, dependability and quality assurance (SQA) are activities included in SPA. The software product assurance activities are conducted in line with the overall product assurance (PA) activities, meeting the requirements and the expectations of the customer, management, software engineering and system engineering, tailoring the software processes taking into account dependability safety and security aspects, software/system development constraints and project/product quality objectives.

Also, the software processes and its related products shall be managed to conform to standards, taking into account relevant regulations; to be consistent, complete, correct, safe, secure and as reliable as warranted for the system and operating environment; and to satisfy the needs of the stakeholders.

Software product assurance shall manage the software safety and security activities, identifying the criticality of the software, and applying hazard analysis and other related activities to ensure that the software is developed to perform properly, safely and securely in its operational environment, while meeting all quality requirements.

In this document, "contractor" is defined as an entity, which is executing software assurance. In addition, there is a supervising product assurance entity that can be performed by another organization body (e.g. space agency).

4.2 Product assurance activities related to software engineering

Software product assurance consists in activities to support and monitor the software engineering processes and methods. Software product assurance encompasses the entire software life cycle and the development processes, which include processes such as requirements definition, software design, reuse coding, automatic code generation, source code control, code reviews, software configuration management, verification, testing, release management, product integration, and software delivery and acceptance.

Also, software product assurance shall be provided by independent assurance people in which all the work products, activities and processes comply to the project specific plans, such as the software management plan.

4.3 Product assurance activities related to software safety and security

Software product assurance is involved in development through each software engineering stage and aims to ensure that all necessary safety and security analyses have been performed.

This will ensure:

- that the mission software does not fail due to an unexpected error either within the system itself or due to human operation;
- that data are always available for processing;
- that the software system is correctly performed.

Software product assurance assesses the software engineering activities and products to allow the software to be executed without any potential hazards that can affect the system.

The software product assurance takes the lead in or ensures the safety and security analysis process for the software systems and software components to determine and to deal with the criticality classification of software products based on the impact of its potential losses.

4.4 Product assurance activities related to software reliability

For projects that have software reliability requirements, a quantitative requirement for software reliability shall be stated as a forecast; and the operational or test results shall indicate the confidence level associated with the forecast that the software product will meet the requirements.

5 Software product assurance management

5.1 General

The software product assurance shall identify the responsibilities of the supplier/developer (hereinafter referred to as the contractor) responsible for software product assurance for the software project, as well as the expected outputs that should be presented in the software product assurance plan (SPAP). The expected outputs should include the quality requirements, software engineering models to be used in the development, reporting, reviews, audits, alerts and problems handling processes for quality assurance.

The software engineering joint to the software product assurance shall present the main features of the SPAP, the software baselines and reviews to be perform, audits, the handling of alerts and problems, risk management, critical item control, supplier management, procurement, assessment, and process improvement. Also, the software product assurance together with the software engineering shall describe the roles, responsibilities, authority, and interfaces and interrelation of personnel who manage the software product assurance. The software product assurance shall describe the configuration control, how to handle critical items, the independent verification and validation approaches, software metrics, software reuse, and any other activity that can be pertinent.

5.2 Software product assurance planning and control

The SPAP shall define the activities and tasks applied to ensure that software developed for a space product satisfies the project's established requirements and stakeholders' needs within project cost and schedule constraints and with an acceptable level of risk.

The SPAP shall specify the product assurance management safety, dependability and quality activities and tasks with their requirements, objectives and schedule to the related objectives in the software engineering management, software development and software maintenance plans. The plan identifies documents, standards, practices and regulations applied for the software and how these items are monitored and controlled to ensure adequacy and compliance. The plan also identifies tools, techniques, methodologies, procedures for problem reporting, corrective action, safety and security measure; training, reporting and documentation.

The software product assurance shall monitor and control the effectiveness of the SPAP used during the development of the software.

5.3 Risk management

The software engineering, together with the software product assurance, closely follows the risk management. This shall ensure that the risks emanating from software are removed or mitigated and have no impact on risks related to the functioning of the system. These activities are under supervision of the project manager.

The software product assurance shall provide the results of the safety and security analyses including the criticality classification of the software products to be developed and the information about the failures that can be caused at higher level by the software products to be developed.

5.4 Supplier selection and monitoring

The contractor shall establish mandatory attributes or selection criteria that the organization will evaluate in its arrangements with supplier selection, such as quality, safety, delivery, service, simplicity, risk, agility.

The contractor shall establish a monitoring process which shall include the review and approval of the suppliers' product assurance documents, the continuous verification of processes and products, and the monitoring of the final validation of the product.

5.5 Procurement process

The contractor defines a procurement life cycle requirement through phases, such as identification and procurement planning, market research, solicitation and award, and management and closeout. Each phase shall generate products such as the procurement plan, statement of work, request for information (RFI), invitation to bid (ITB), request for proposals (RFP) or invitation to negotiate (ITN).

The process of buying a software service (procurement) encompasses the entire life cycle from the initial identification of a need to the retirement and disposal of the item.

The software product assurance shall provide quality requirement inputs to the procurement process, defining a procurement life.

5.6 Tools and support environment

The software development environment shall be selected according to criteria defined together with the software engineering, taking into considerations criteria like availability, compatibility, performance, maintenance, the available support documentation, the acceptance and warranty conditions, the conditions of installation, training and maintenance and intellectual property rights constraints.

5.7 Assessment and improvement process

The software product assurance shall monitor and control the effectiveness of the processes used during the development of the software, including the services provided by third parties. The process assessment and improvement performed at organization level can be used to provide evidence of compliance for the project and with the organizational policies.

The process assessment model, the method, the scope, the results and the assessors shall comply with the project requirements described in the SPAP or in an appropriated document. The results of the assessment shall be used as feedback to improve as necessary the performed processes, to recommend changes in the project, and to determine technology advancement needs.

The process improvement shall be conducted according to a documented process improvement. Evidence of the improvement in performed processes or in project documentation shall be provided. The software engineering shall ensure that the results of previous assessments are used in its project activity.

6 Software process assurance

6.1 General

6.2 to 6.4 describe the main activities of the software product assurance related to the activities of software engineering processes.

6.2 Software product assurance related to software engineering processes

6.2.1 General

The software product assurance related to software engineering processes shall describe the main characteristics of the software development life cycle that shall be defined or referenced in the SPAP, such as phases, input and output of each phase, status of completion of phase output, milestones, dependencies, responsibilities and role of the stakeholders at each milestone review.

6.2.2 to 6.2.10 describe the main activities of software product assurance related to the activities of software engineering.

6.2.2 System requirements analysis process

The system requirements baseline shall be defined during the system requirements analysis process and subject to documentation control and configuration management as part of the development documentation. For the definition of the system requirements baseline, all results from the safety and security analyses in this level shall be used.

The contractor shall ensure that the system requirements are formal, correct and completely described in terms of their functions, capabilities, safety, security, human-factors, interface, operations, maintenance and quality requirements.

6.2.3 Software requirement analysis process

The software requirements shall be complete and unambiguously defined and subject to documentation control and configuration management as part of the development documentation.

The software product assurance shall support the software requirement definition process, assuring that the results from the safety and security analyses shall be used, including non-functional requirements necessary to satisfy the requirements baseline, such as performance, safety, security, quality, maintainability, configuration management and verification and validation.

The software product assurance shall conform to the traceability matrix of software requirements.

6.2.4 Software architectural design process

The software architecture design shall identify items of hardware, software, and manual operations. It shall be ensured that all the system requirements are allocated among the items. Hardware configuration items, software configuration items, and manual operations shall be subsequently identified from these items. The results of the evaluations shall be documented.

The software product assurance shall evaluate the items considering the criteria such as traceability and consistency to the system requirements, appropriateness of design standards and methods used, feasibility of the software items fulfilling their allocated requirements, its operation and maintenance.

Design and distribution of non-functional requirements, such as processing time requirements, memory and interface specifications, shall be detailed in accordance with the decomposition of the software functions and modules. Also, safety and security requirements should be detailed and allocated in the design.

6.2.5 Software detailed design process

The contractor shall ensure that each individual item of the architecture design is in accordance with the detailed design and its decomposition in terms of functions and modules. Interface specifications shall be detailed in accordance with the considerations of the boundaries and interrelations, and the design of the module.

6.2.6 Software construction process

The contractor shall ensure that during the development process the coding standards are followed, including naming conventions and commentary rules. These standards shall be reviewed with the interested parts to ensure that they reflect product quality requirements. The tools to be used in code developing and checking conformance with coding standards shall be identified in the SPAP before coding activities start.

The code shall be put under configuration control immediately after unit testing.

6.2.7 Software testing process

The contractor shall ensure that the testing process is performed in accordance with the testing procedures, including the verification if the tests cover all test units and test components. This activity also includes the verification if the test results are recorded in a format that allows determination of pass or not pass.

In case of test cases performed, they shall be checked to ensure they reflect the method and use of the software or computer system.

6.2.8 Delivery and acceptance process

The delivery and acceptance process requires the software to be acceptance-tested, verified and validated. The details of the acceptances testing, including specific tests suited to validate the software to the target environment, shall be documented in the acceptance test plan.

Before the software is ready for acceptance, the software product assurance shall ensure that the delivered software complies with the contractual requirements, including any specified content of the software acceptance data package.

After finalisation of acceptance testing, a report on the tests and test results shall be established. This test report shall be signed by the product assurance manager and project manager and/or engineering manager. These documents shall also be made available to the organization responsible for the maintenance of the software product.

6.2.9 Operations process

The contractor shall ensure that customer and user's expectations and the quality of the software mission related to the operation process are met. The contractor shall also verify parameters such as availability of data and permissible information degradation.

6.2.10 Maintenance process

The contractor shall define the maintenance activities specific to verification and validation activities applicable to maintenance interventions. The maintenance plan shall be verified against specified requirements for maintenance of the software product.

The maintenance plan and procedures shall include the minimum scope of maintenance, maintenance life cycle, maintenance activities, quality measures to be applied during the maintenance and maintenance records and reports.

These activities also apply to tasks such as verifying the partial changes to software called patches, and additions and enhancements to software features during their operational life. Verify if during a non-expected failure that causes a system failure during reprogramming, the software or computer system is restored to a working state.

6.3 Software product assurance related to support process

6.3.1 General

The software product assurance related to support process shall describe the main activities of the software product assurance, addressed to the quality processes, such as documentation management, software configuration management, quality assurance, verification, validation, safety and security analysis, software review, software audit, problem resolution, usability, reuse, automatic code generation processes.

This process shall include:

- the system-level analyses leading to the criticality classification of software products based on the severity of system failures consequences;
- the measures to avoid propagation of system failures between software components of different criticality and risk of software how classify components whose malfunction can cause system failures of higher criticality components;
- what documents shall be controlled by configuration, in-house verification and validation (V&V) activities or independent V&V activities;
- the evaluation analyses for the selection of existing software instead of new development and so on.

6.3.2 to 6.3.11 describe the main processes of support performed by software product assurance.

6.3.2 Documentation process

Software product assurance shall ensure that the applicable issues of all documents and data are available at all locations where activities required for the implementation of the software product assurance programme are performed.

Software product assurance shall identify the project documents requiring approval including those requiring approval and review by PA.

Where documented information is held electronically, consideration of the retention times and accessibility should take into account the rate of degradation of the electronic media and the availability of the devices and software needed for future access (e.g. back-up policy, protection methods).

6.3.3 Safety and security analysis process

The software product assurance, together with the software engineering, shall identify the methods and techniques for the software safety and security analysis to be performed at technical specification and design level.

The safety and security analysis process of the software products shall be performed, using the results of system-level analyses, in order to determine the criticality of the software components.

Methods and techniques that cover all aspects of software system interactions shall be used in safety and security analysis, such as systems-theoretic process analysis (STPA). Complementary, traditional approaches can be used such as software failure modes and effects analysis (SFMEA), software fault tree analysis (SFTA) or software common cause failure analysis (SCCFA).

6.3.4 Critical items handling process

The critical items handling process shall describe how to measure, justify and apply levels of safety and security assurance of critical software items. Measures can include features for failure isolation, failure handling, and defensive programming techniques.

6.3.5 Configuration management process

The configuration management process shall establish and maintain a configuration control to ensure the integrity of the software items and make them available to concerned parties. A software configuration management plan shall be developed describing the configuration management activities, such as configuration control activity and software problem resolution activity, including procedures, responsibilities and schedule for performing these activities.

The contractor shall conduct the identification and recording of change requests; analysis and evaluation of the changes; approval or disapproval of the request; and implementation, verification, and release of the modified software item. The software problem resolution management activity provide support for the configuration management process.

6.3.6 Metric process

The metric process shall establish metrics to use to manage the development and to assess the quality of the engineering, support and organization processes. Metric process shall be collected, stored and analysed by applying quality models and procedures.

Metric shall relate to the actual performance against planned tasks, the number of problems detected during software engineering process, mainly in the verification, validation and integration phases. Metrics reports shall be included in the software product assurance reports.

6.3.7 Verification process

The verification process shall perform the verification activities related to the quality requirements and shall be specified in the verification and validation plan. Verification activities include techniques such as review, inspection, walkthrough, model simulation, traceability analysis, formal proofs.

An independent software verification can be performed by a third party, with a combination of reviews, inspections, analyses, simulations and testing.

6.3.8 Validation process

The validation process shall be performed in accordance with the verification and validation plan, including unit, component and integration tests, validation against the technical specification, validation against the requirements baseline and acceptance tests.

The process shall ensure that tests are conducted in accordance with approved test procedures and data, the configuration under test is correct, the tests are properly documented, and the test reports are up to date and valid.

When testing under the operational environment is performed, the following shall be addressed: the features to be tested, the specific responsibilities for carrying out and evaluating the test and after completion, the restoration of the previous operational environment.

Independent software validation can be performed by a third party, when the criticality and the risks associated with the project or part of it were justified.

6.3.9 Review process

The review process shall perform periodic reviews activities to be held at predetermined milestones as specified in the SPAP. Stakeholders should determine the need for any ad hoc reviews in which agreeing parties may participate.

The parties that participate in a review should agree on the items at each review, such as meeting agenda, software products under review, problems to be reviewed, scope and procedures and entry/exit criteria for the review. Problems detected during the reviews shall be recorded.

6.3.10 Audit process

The contractor shall perform internal audits to ensure appropriate implementation of the requirements of the PA program using established and maintained procedures.

The contractor shall perform audits of suppliers to ensure that the required product assurance standards and contractual requirements are appropriately implemented.

In addition to the planned audits, extra audits shall be performed when necessary, to overcome failure, consistent poor quality, or other problems.

6.3.11 Problem resolution process

The problem report shall establish a problem resolution activity for handling all problems detected in the software products and activities. Each problem should be classified by the category and priority to facilitate trend analysis and problem resolution.

The software product assurance shall perform to verify the resolution of each problem since its detection, investigation, cause analysis and resolution of the problem.