FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/FDIS
22893

ISO/TC **20**/SC **14**

Secretariat: **ANSI**

Voting begins on:
2021-12-13

Voting terminates on:
2022-02-07

Space systems — Software product assurance (SPA)

Reference number
ISO/FDIS 22893:2021(E)

© ISO 2021

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

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

3 Terms and definitions

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/FDIS 22893
https://standards.iteh.ai/catalog/standards/sist/d6ce8f32-c796-4cd3-8318-
c7fa10dfdc51/iso-fdis-22893

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 software-system 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.