Technical Specification

ISO/TS 20517

First edition
2024-07

Space systems — Cybersecurity management requirements and recommendations

Systèmes spatiaux — Exigences et recommandations en matière de gestion de la cybersécurité

Reference number
ISO/TS 20517:2024(en)

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

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 2
4 Cybersecurity overview **2**
4.1 General 2
4.2 Mission, programme and project 2
4.3 Project management 3
4.4 Systems engineering 3
5 Cybersecurity general principles **3**
6 Cybersecurity management plan **4**
7 Cybersecurity policies **5**
8 Requirements for cybersecurity **5**
9 Cybersecurity process **6**
10 Cybersecurity culture **7**
Bibliography **8**

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

Cybersecurity is a broad term used differently through the world. Cybersecurity concerns managing information security risks related to the organizations or products when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

Space is a critical sector that is no longer the domain of only national government authorities. Space is an inherently risky environment in which to operate, so cybersecurity risks involving space systems must be understood and managed alongside other types of risks to ensure safe and successful operations.

Over the past decade, space vulnerabilities have grown fast. Cyber intrusions into space organization start to happen, making the interested parts more aware of the cyber defence needs of space assets. A range of measures must be made available to prevent or anticipate an incident, or even a cyber war or conflict. Space systems already suffered from different kinds of attacks. Besides that, with the advent of space commercialization (NewSpace), there are increasingly cybersecurity concerns.

This document intends to make available to system engineers, project managers, software engineers, and space professionals requirements and recommendations about how to deal with cybersecurity in space systems.

System engineers, project managers and software engineers are the primary focus. The audience also includes safety engineers, quality managers and all the stakeholders in charge of making available, protecting, maintaining and disposing of any information related to space systems.

This document:

— provides a security approach under system life cycle perspective for the minimum required product assurance activities that contribute to cybersecurity;

— presents basic concepts, on pertinent cybersecurity management requirements and recommendations.

— provides requirements and recommendations for the management of the systems engineering applied to space systems and intends to define the minimum set of existing processes on the subject, seeking to reach an international agreement on the topic.

This document emphasizes the following aspects of the cybersecurity for space systems:

— Cybersecurity overview;

— Cybersecurity general principles;

— Policies, practices and responsibilities;

— Requirements for cybersecurity;

— Cybersecurity process;

— Cybersecurity culture.

Space systems — Cybersecurity management requirements and recommendations

1 Scope

This document defines requirements and recommendations to be used for the management of cybersecurity in space systems. Space systems include manned and unmanned spacecraft, launcher, payload, experiment, ground equipment and any other space facilities.

This document describes the processes, techniques, and responsibilities for managing the cybersecurity, ways to prevent and mitigate accidents and incidents.

This document addresses systems engineering activities and provides requirements and recommendations for security engineering. This document establishes a common reference for the space sector to work to manage the systems engineering issues related to cybersecurity for all space products, services and projects.

This document doesn't describe in detail the systems engineering processes or related project management processes, or detailed requirements or processes for cybersecurity.

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

ISO 14300-1, *Space systems — Programme management — Part 1: Structuring of a project*

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

ISO 17666, *Space systems — Risk management*

ISO 18676, *Space systems — Guidelines for the management of systems engineering*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 10795, ISO/IEC 27000 and the following 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/

3.1.1
cybersecurity
state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to violation of confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle

[SOURCE: IEC 81001-5-1:2021, 3.30]

3.1.2
systems engineering
transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems using systems principles and concepts and scientific, technological and management methods

[SOURCE: ISO/IEC/IEEE 15288:2023, 3.50]

3.2 Abbreviated terms

COTS	commercial off-the-shelf
GOTS	government off-the-shelf
MOTS	modified off-the-shelf
PA	product assurance
SE	systems engineering
STAMP	system-theoretic accident model and processes
STPA	system theoretic process analysis

4 Cybersecurity overview

4.1 General

This clause contextualizes the importance of space systems cybersecurity related to mission/programme or project, and in relation to project management and to systems engineering activities.

4.2 Mission, programme and project

The space systems cybersecurity shall be considered within the frame of the mission of the related space system and within the frame of the management of the related programme or project with the overall objective of optimizing performance, costs and schedules and of minimizing the risks.

This is an integral element of any programme or project; and it is particularly important due to the following:

— specific environmental conditions in space;

— need for a high level of performance;

— limited number of models;

— limited access to the product during operations;

— quasi-impossibility of making repairs in the case of failure during flight;

— associated high costs involved.

4.3 Project management

a) Within the frame of the space project management and in response to the project management specification as defined in ISO 14300-1, each supplier concerned shall:

— prepare a project management plan as required in ISO 14300-1, which contains descriptions of main activities, implementation methods and general procedures with respect to its organization;

— meet the cybersecurity requirements and recommendations as defined this document.

b) The prime objective of product assurance (PA) is to ensure that the space products accomplish their defined mission objectives and, more specifically, that they are safe, secure, available and reliable. In addition, PA shall:

— achieve effective cybersecurity space programmes by coordinating the development and implementation of appropriate PA methods and standards, as required in ISO 14300-2;

— meet the cybersecurity requirements and recommendations as defined this document.

c) In support of programme risk management, PA shall:

— ensure an adequate identification, appraisal, prevention, and control of technical and programmatic risks within programme constraints, as required in ISO 17666;

— meet the cybersecurity requirements and recommendations as defined this document.

4.4 Systems engineering

a) Cybersecurity generally refers to the confidentiality, integrity, and availability of information assets. Security management includes controls (e.g. policies, practices, procedures, organization structures, and software). Trustworthiness is a concept that includes privacy, reliability, resilience, safety and security, therefore worthy of being trusted to fulfil any critical requirements for a particular system element, system, network, application, mission, business function, enterprise or other entity.

b) As the world becomes increasingly digital, the issue of cybersecurity is a factor that the systems engineering practitioner shall consider. Both hardware and software systems are increasingly at risk for disruption or damage caused by threats taking advantage of digital technologies.

c) The systems engineering activities of the space system:

— shall be defined in the systems engineering management plan as required in ISO 18676 (mission analysis, requirements analysis, architectural design, detailed design, assembly, integration and verification, validation);

— meet the cybersecurity requirements and recommendations as defined this document.

5 Cybersecurity general principles

The cybersecurity general principles for space systems are to identify the assets, to document the point of entry to the assets, and to determine their environment.

As illustrated in Figure 1, the cybersecurity comprises three aspects:

a) assets;

b) security perimeter;

c) security environment.

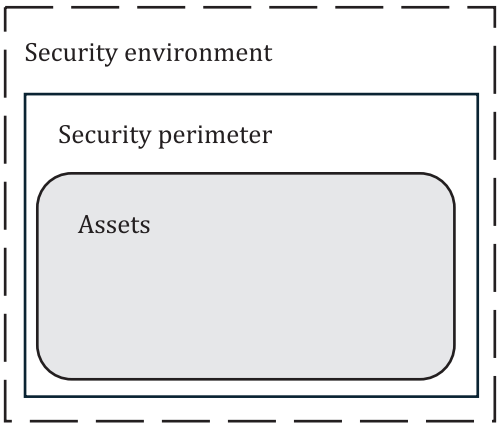

Figure 1 — Security scope (based on RTCA DO 326A)

Assets are the logical and physical resources of the space systems which contribute to mission accomplishment, such as spacecraft, launch facilities, communication link.

Security perimeter is the boundary between an internal security context and the external security environment of the space system under consideration. The purpose is to identify and trace points of entry to the assets such as the hardware interfaces, software interfaces and information exchange.

Security environment are persons, organizations and external systems that interact with the asset under consideration, so that the potential threat sources can be identified as such considering (not limited to): roles and entities, responsibilities and risk related, external dependencies (regulations, laws, contracts), classification of threats sources and vulnerabilities, etc.

6 Cybersecurity management plan

Space organizations should develop and implement a cybersecurity management plan for their space assets.

This plan shall ensure the ability to assess cyber risk (security analysis of systemic factors) and choose defence and mitigation techniques.

Space systems managers and operators should consider, based on risk assessment and tolerance, incorporating in their plans: safeguarding command, control, physical protection measures, protection against communications jamming and spoofing, protection of ground systems, operational technology, information processing systems and management of supply chain risks, and software vulnerability management.

The project manager shall ensure the following.

a) The cybersecurity risks in space systems shall be identified; mitigations shall be planned and implemented for these systems.

b) All systems including space flight software shall be evaluated for cybersecurity risks, including risks posed using commercial off-the-shelf (COTS) software, government off-the-shelf (GOTS) software, modified off-the-shelf (MOTS) software, reused software, auto-generated code, embedded software, the software executed on processors embedded in programmable logic devices.

c) The software systems with space communications capabilities are protected against unauthorized access.

d) The space flight and ground software systems are assessed for possible cybersecurity vulnerabilities and weaknesses.

e) The required cybersecurity verification and validation measures are implemented.

The project manager shall:

— implement the identified software security risk mitigations addressed in the project plan;

— verify and validate the required software security risk mitigations to ensure that security objectives identified in the project plan for space flight software are satisfied in their implementation.

Assessments for security vulnerabilities shall be included during peer reviews or inspections of software requirements and design. Automated security static analyses, as well as coding standard static analyses of software code, shall be carried out to find potential security vulnerabilities.

7 Cybersecurity policies

This clause defines requirements related to cybersecurity policies to enhance efforts to protect the space assets and supporting infrastructure from cyber threats, and to define responsibilities for space systems owners and operators to manage appropriate risks and mitigate the effects of an attack, in accordance with the specific mission requirements.

Cybersecurity policies shall be applied to terrestrial and space systems and integrated in all phases of development assuring the integrity of critical space assets.

A set of cybersecurity measures, including the ability to perform updates and respond to incidents remotely, shall be integrated in the space vehicle design, as most space vehicles in orbit cannot currently be physically accessed.

The policies for cybersecurity in space shall be through prevention, active defence, risk management, and sharing best practices.

The space organization shall include in its structure a cybersecurity manager, a security auditor, and a cybersecurity engineer.

A cybersecurity policy shall include:

a) definitions of the technology and information assets to be protected.

b) the definition of the kind of threats to those assets, and the rules and controls for protecting them.

c) the ways to train the employees regarding their roles in protecting the technology and sensitive information, how it can be shared and where and what devices and materials may be used in ground and space systems.

d) measures to promote staff awareness and training on insider threat mitigation precautions.

e) The establishment of ways to handle and store sensitive material.

8 Requirements for cybersecurity

This clause defines the mission and the stakeholder requirements related to cybersecurity to achieve the outputs expected and to ensure the security and resilience of a space system.

This clause covers technical, quality assurance, procedural, personnel, physical requirements, and others that have an impact on cybersecurity.

The requirements for cybersecurity are as follows.

a) Space systems and their supporting infrastructure, including software, shall be developed and operated using a risk-based cybersecurity approach.

b) Space systems shall be developed to continuously monitor, anticipate and mitigate evolving malicious cyber activities that can manipulate, deny, degrade, disrupt, destroy, survey or eavesdrop on space systems operations.

c) Space systems configurations shall be resourced and actively managed to achieve and maintain an effective and resilient cyber survivability strategy throughout the space systems life cycle.

The space systems managers and operators shall incorporate in their plans:

— mechanisms of safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats during the entire mission lifetime;

— physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems.

— protection against communications jamming and spoofing, such as signal strength monitoring programmes, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures designed to provide security against existing and anticipated threats during the entire mission lifetime; protection against jamming can be optional depending on the risk analysis results;

— ways to protect ground systems, operational technology, and information processing systems, to reduce the risk of malware infection and malicious access, the insider threats, logical or physical segregation; the regular patching; physical security; restrictions on the utilization of portable media; and the use of antivirus software;

— adoption of appropriate cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements such as information systems, antennas, terminals, receivers, routers, associated local and wide area networks, and power supplies.

— management of supply chain risks that affect the cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.

The organizational structure shall include as a minimum a cybersecurity manager, a cybersecurity internal auditor and a cybersecurity engineer.

9 Cybersecurity process

The cybersecurity process related to space systems shall be defined and shall be integrated in the SE (systems engineering) processes, such as in the V model development in accordance with ISO 18676.

The processes to analyse, detect, identify and mitigate potential cybersecurity incidents, to handle incidents (i.e. to contain and eradicate them and to recover the system), and to apply system safety and security analysis through a systemic and holistic approach, shall be defined.

The cybersecurity activities shall be based on systems theory, such as the system-theoretic accident model and processes (STAMP) approach. This systems theory method aims, through a top-down view, to propose cybersecurity mitigations for systems that are susceptible to cyber-attacks and are intensive in hardware, software, human and processes.

This method involves the following activities.

a) Activity 1: Use system theory and control theory foundations: define the assets, the security parameter, identify the types of threat, identify potential losses and accidents; identify hazards and constraints; create a hierarchical control structure model.

b) Activity 2: Identify types of unsecure control: identify unsafe and unsecure control actions finding in the hierarchical control structure.

c) Activity 3: Identify causes of unsecure control and eliminate or control them: identify scenarios leading to unsecure control actions; develop new requirements, controls, and design features to eliminate or mitigate unsecure scenarios.