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

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.