

# STAMP and ISO 20517 Cybersecurity for Space Standard

**CARLOS LAHOZ**

Institute Technological of Aeronautics ITA  
University of Vale do Paraiba UNIVAP  
ISO member - TC20/SC14/WG5

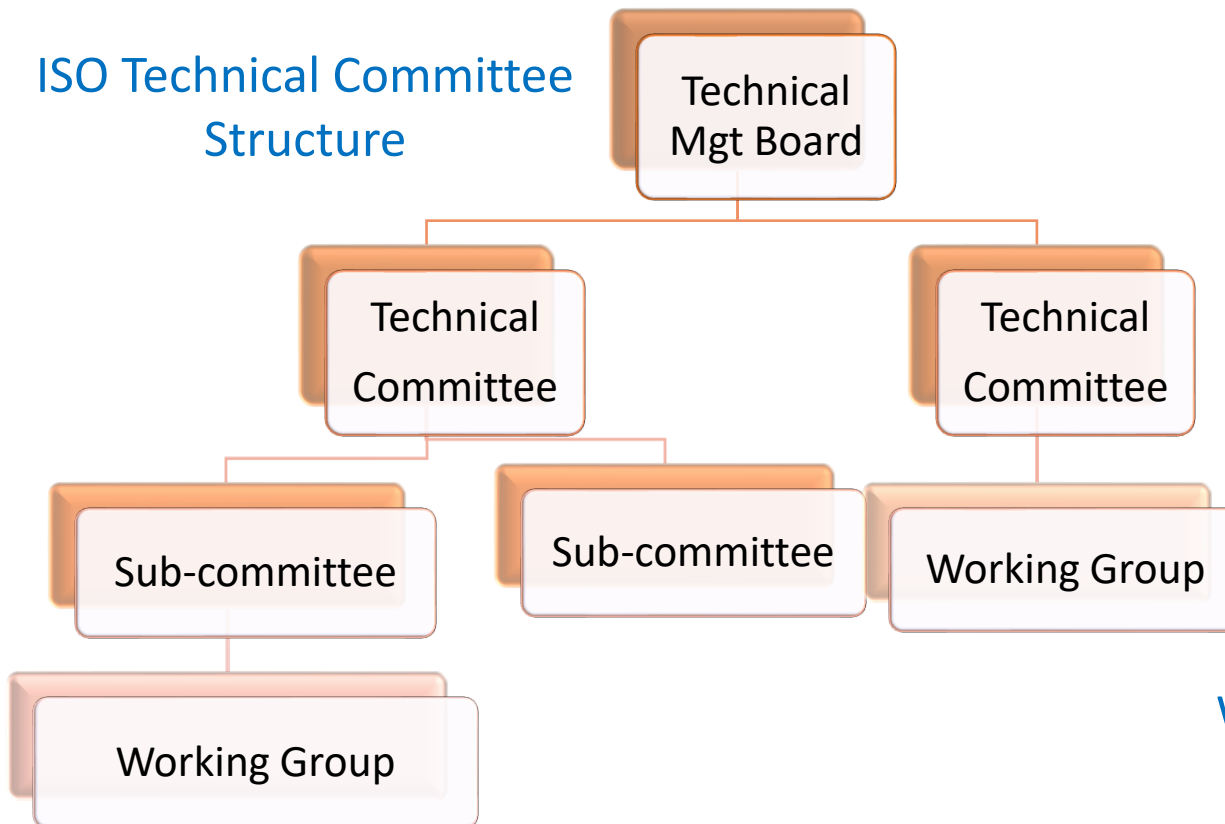


**STAMP Workshop (03-06 June-2024)**

# iso.org

This initiative came from ISO/TC20/SC14/WG5. The TC20 is in charge of standardization of materials, components and equipment for construction and operation of **aircraft and space vehicles**. 36 countries participating, over 600 published standards and 200 in development.

## ISO Technical Committee Structure



ISO TC 20



SC 14 Space systems and operations



WG5 Program Management and Quality

# ISO stages for std development

## Stages and Resources for STD development

(\*) = obligatory stage

**NWIP**=New Working Item Proposal

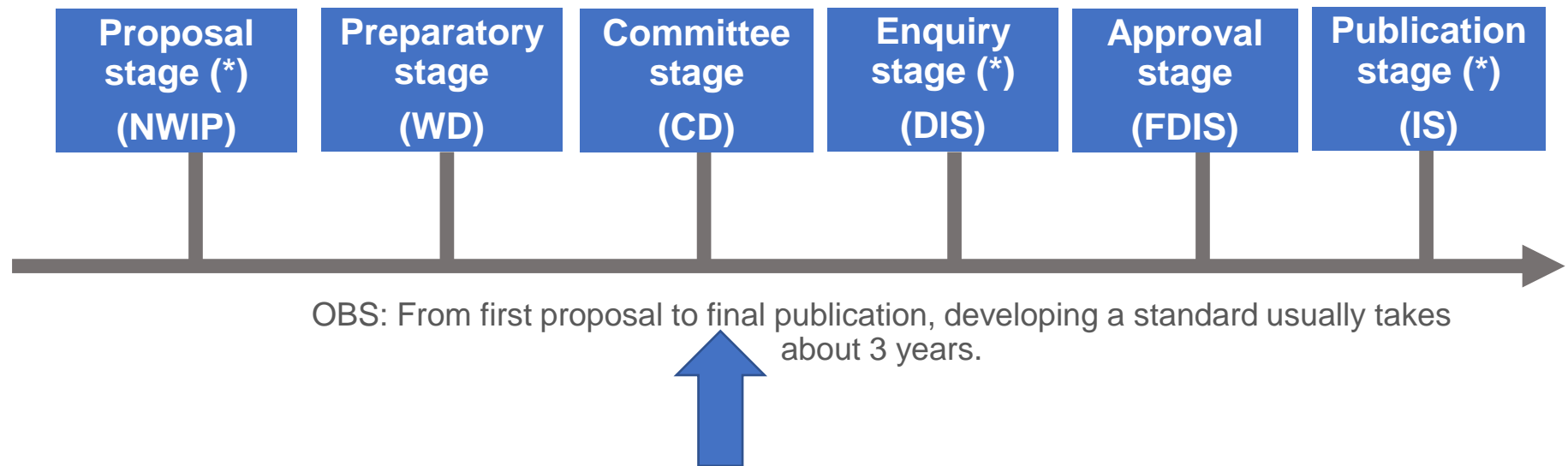
**WD**=Working Draft

**CD**=Committee Draft

**DIS**=Draft International Standard

**FDIS**=Final Draft International Std

**IS**=International Standard



Cybersecurity Management Guidelines (January - 2024)

# cybersecurity for space: motivation

“Space systems (satellites and ground systems) are frequently the target of cyber-attacks. Despite the space industry’s technical sophistication, their cybersecurity efforts have lagged behind that of other high-technology sectors.” (\*)

## Challenges:

- Critical infrastructure for global economy and military presence.
- Lack of standards/regulations for space cybersecurity.
- Complex supply chain and life cycle.
- Widespread use of COTS (Cubesats with open-source OS, for instance).
- Highly specialized workforce.
- Resource constraints (technical and financial).

(\*) *Cybersecurity Principles for Space Systems. Aerospace Information Systems. Volume 16, Number 2. February 2019. Gregory Falco. (MIT/CSAIL· Computer Science and AI Lab).*

# cyberattacks in space systems

In April 2018 an **unauthorized** Raspberry Pi **computer** , was **connected** in the NASA's **JPL server** by hackers. The attack in the NASA network, apparently got as far as the Deep Space Network (DSN) array of radio telescopes and numerous other JPL systems.


On February 24th 2022, only one hour before invading Ukraine, Russia launched a **cyberattack** on **ViaSat's KA-SAT** satellite network, which was used by the Ukrainian army (\*\*).

(\*\*) *“ESPI Report 84 - The war in Ukraine from a space cybersecurity perspective” October 2022. European Space Policy Institute (ESPI). Austria*



# outline – ISO 20517 cybersec guidelines

**March, 2023:** New Working Item Proposal NWIP (covers Form 4 and the outline of the Standard) for Space System - Cybersecurity Management Guidelines was accepted



Ch. de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland | T: +41 22 749 01 11 | iso.org | central@iso.org

### Form 4: New Work Item Proposal

<b>Circulation date:</b> Click here to enter text. <b>Closing date for voting:</b> Click here to enter text.	<b>Reference number:</b> Click here to enter text. (to be given by Central Secretariat)
<b>Proposer (e.g. ISO member body or A liaison organization)</b> Click here to enter text.	<b>ISO/TC</b> Click here to enter text./ <b>SC</b> Click here to enter text. <input type="checkbox"/> Proposal for a new PC
<b>Secretariat</b> Click here to enter text.	<b>N</b> Click here to enter text.

**January 2024:** became a Committee Draft CD TS and the name was changed to “**Space systems - Cybersecurity management requirements and recommendations**”

# outline – ISO 20517 cybersec guidelines

Introduction

1 Scope

2 Normative References

3 Terms and Definitions

4 Cybersecurity overview

5 Cybersecurity general principles

6 Cybersecurity management plan

7 Cybersecurity policies

8 Requirements for cybersecurity

9 **Cybersecurity process**



10 Cybersecurity culture

Bibliography

*“The cybersecurity activities shall be based on systems theory, such as the System-Theoretic Accident Model and Processes **STAMP** approach. This systems theory gives a method that 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” (extract from ISO 20517).*

# outline – ISO 20517 cybersec guidelines

The ISO 20517 standard intends to make available to system engineers, project managers, software engineers, and space professionals a guide on how to deal with cybersecurity in space systems.

Describes the **processes**, **techniques**, and **responsibilities** for managing cybersecurity, and ways to prevent and mitigate accidents and incidents.

In process and techniques, it is recommended STAMP (STPA) as a better approach to applying to cybersecurity.



# outline – ISO 20517 cybersec guidelines

STPA activities described in ISO 20517:

**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 cybersecurity constraints; create a hierarchical control structure model.

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

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

# final considerations

**ISO 20517** give an overview of cybersecurity including policies, management activities and process in terms of requirements and recommendations.

Also, ISO has already a standard for security **ISO 27001** (\*), which is accepted in many countries as a framework for information security/cybersecurity implementation. The ISO 20571 addresses in specific issues from space systems, **not superseding** the ISO 27001.

In this CD version, it is recommended that **STPA** as a better approach to cybersecurity analysis be applied in space systems.

*(\*)ISO/IEC 27001: 2013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements)*

Thank you  
Carlos LAHOZ  
carloslahoz@gmail.com

Waiting for your participation at  
LATIN AMERICAN STAMP WORKSHOP in September  
<https://www1.univap.br/la-stamp-workshop/>

