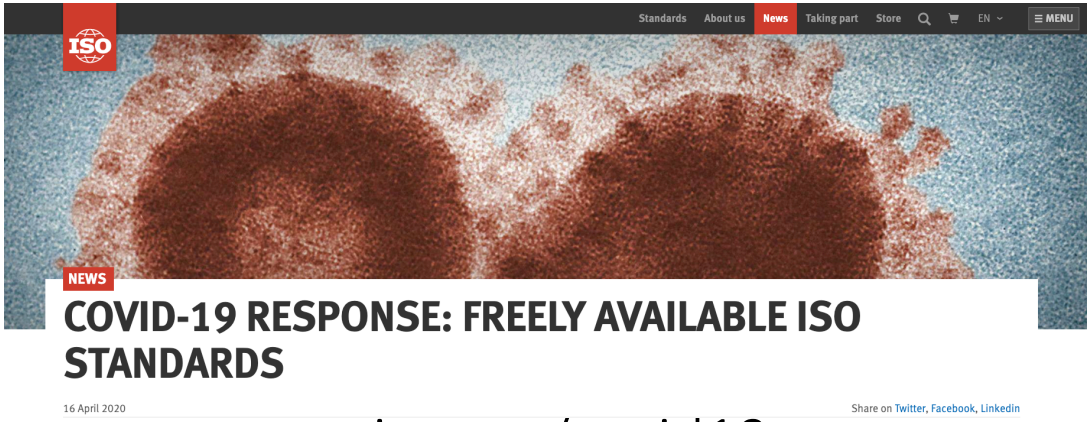
STAMP and New ISO Standard for Cybersecurity

Carlos Lahoz

STAMP Workshop (July-29-2020)

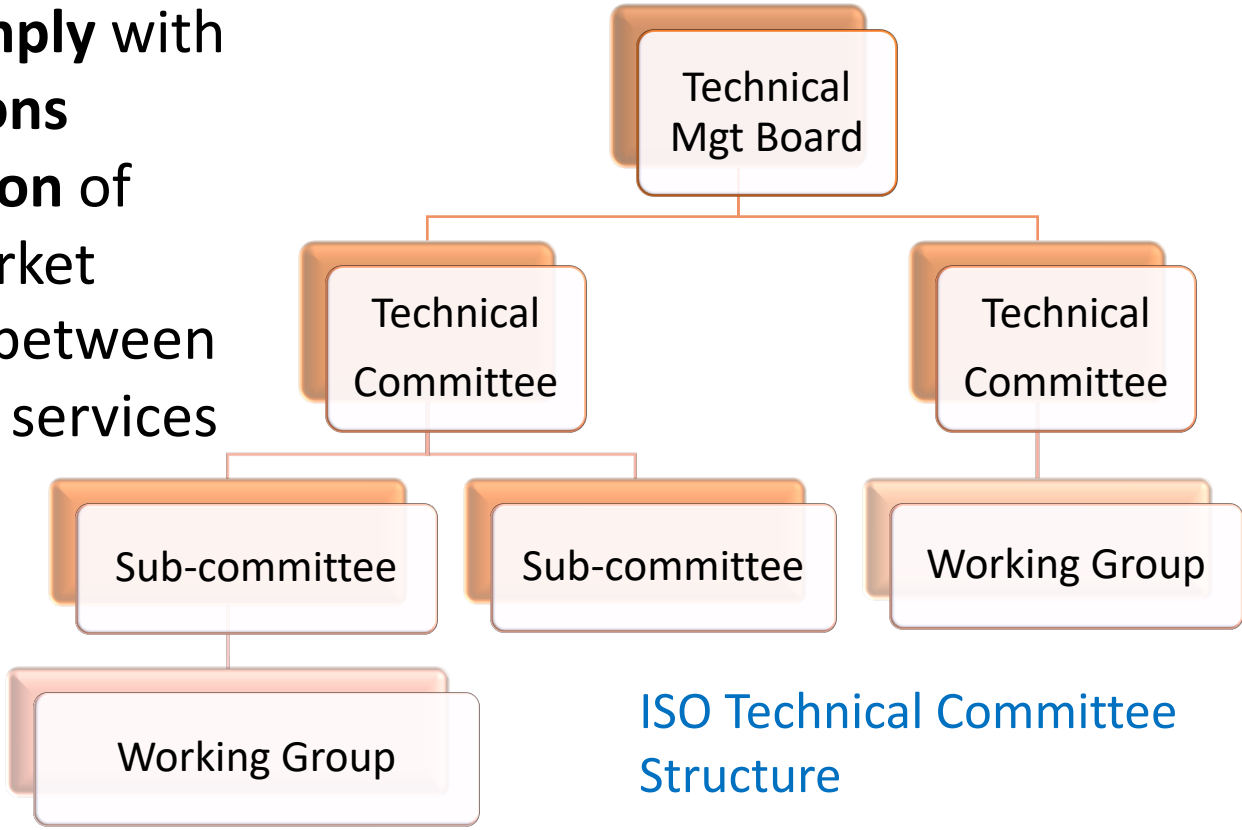


iso.org/covid19

iso.org

Standards provide people and organizations with a **basis for mutual understanding**, and are used as tools to facilitate communication, measurement, commerce and manufacturing.

- facilitating **business interaction**
- enabling companies to **comply** with relevant laws and **regulations**
- speeding up the **introduction** of **innovative products** to market
- providing **interoperability** between new and existing products, services and processes.



ISO Technical Committee Structure

ISO/TC 20 - Aircraft and space vehicles

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.

TC20 Structure:

- ISO TC 20/SC 1 Aerospace electrical requirements
- ISO TC 20/SC 4 Aerospace fastener systems
- ISO TC 20/SC 6 Standard atmosphere
- ISO TC 20/SC 8 Aerospace terminology
- ISO TC 20/SC 9 Air cargo and ground equipment
- ISO TC 20/SC 10 Aerospace fluid systems and components
- ISO TC 20/SC 13 Space data and information transfer systems
- **ISO TC 20/SC 14 Space systems and operations** → **WG5** Program Management and Quality
- ISO TC 20/SC 16 Unmanned Aircraft Systems
- ISO TC 20/SC 17 Airport Infrastructure
- ISO TC 20/SC 18 Materials

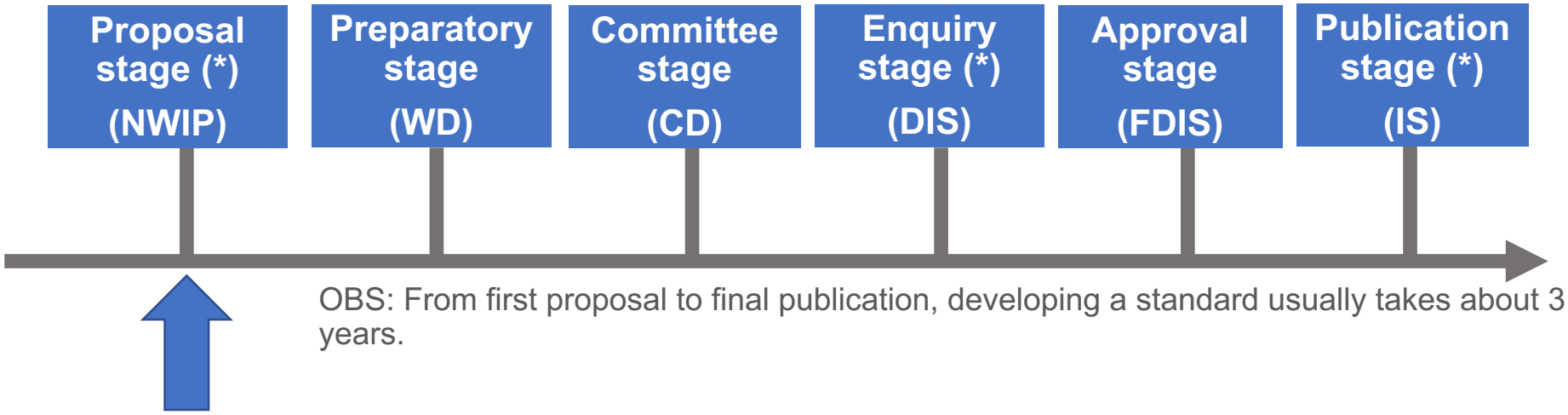
WG1 Design engineering and production
WG2 Interfaces, integration and test
WG3 Operations and ground support
WG4 Space environment

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



ISO Standard for Cybersecurity, new initiative from (TC20) Space systems and operations /(SC14) Space System and Operations /(WG5) Program Management and Quality

ISO std proposal stage- cybersecurity

- NWIP: first step is to confirm that a new International Standard in the subject area is really needed. (Global relevance policy.)
- New work item proposal (NWIP) is submitted to the committee for vote using Form 4.

Form 4 proposal presented in ISO TC20 - SC14 / WG5, 21st Meeting (5-7 Nov 2019 in Saint Petersburg, RU): Space System - Cybersecurity Management Guidelines NWI proposal - Carlos Lahoz, Brazil

Country members at the meeting: USA, Germany, Japan, Russia, China, France and Brazil.

cybersecurity for space: motivation

"Space systems (satellites and ground systems) are frequently the target of cyberattacks. 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. Gregory Falco. Aerospace Information Systems. Volume 16, Number 2. February 2019.* (*) MIT · Computer Science and AI Lab

cyberattacks in space systems

Deliberate **jamming** incidents on services over Satellites, **ARABSAT** Operations Center/AOC (recorded 290 Incidents in 2012).

عرب سات
ARABSAT
عالمنا... عالمكم.
Our world. Your world.

In 2013, researchers at the University of Texas at Austin illustrated the potential risks of relying on GPS for navigation when it used **GPS spoofing** to take control of a 65-meter, $80 million **super yacht** in the Ionian Sea.

Coordinated cyber attacks from North Korea near its border with South Korea produced electronic **jamming** signals that affected **GPS navigation** for passenger aircraft, ships, and in-car navigation for roughly a week in April –May 2012

cyberattacks in space systems

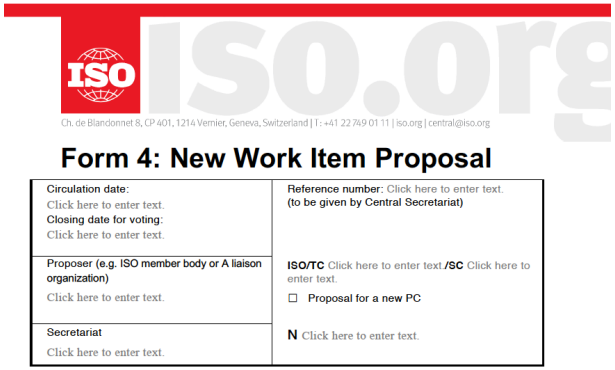
A NASA Operational Messaging and Directory Services (**NOMAD**) Summary Report (2012) revealed that during a 6-month period **NASA** received over **240,000 phishing** attempts.

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.

The Windows XP-based **laptops** on the **ISS** were **infected** with a **virus** called W32.Gammima.AG in 2008, after a cosmonaut brought a compromised laptop aboard which spread the malware to the networked computers.

Cybersecurity Mgt System Guidelines

NWIP (Form 4 and the outline of the STD) for Space System - Cybersecurity Management Guidelines: The idea is to recommend STAMP (STPA and CAST) as an approach to apply in this standard.


ISO iso.org

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

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

Introduction
1 Scope
2 Normative References
3 Terms and Definitions
4 Cybersecurity overview
5 Cybersecurity Management System
6 Requirements for cybersecurity
7 Process and activities for cybersecurity
8 Prevention and resolution for cybersec incidents
9. Cybersecurity culture
Bibliography

STAMP (STPA and CAST) can help to improve the security analysis and its use is adequate in all of this topics

status of the NWIP

52th Meeting – meeting held by Webex (May 26 to 27, 2020). Members participants: France, UK, Germany, Japan, China, US, Brazil and Russia

Extract from the Minutes-of Meeting document:

52nd Meeting

Carlos Lahoz has proposed form 4 and a first WD, see **Attachments 18-01 and 18-02**. Action 51-02 is closed.
Discussion happened during the meeting on the need and interest of making such standard.
This standard should be a high level standard. Some discussions are also at the agenda of WG3.

Conclusion: most of WG5 members are ready to support this NWIP. Before to send to SC14 secretariat, WG5 convenor will check with WG3 if they want to join the activity, before to launch the NWIP.

Next step: Fall meeting (53th WG5, planned from 3 -5/Nov/20 in Paris /BNAE) - WG5 convenor will check with WG3 if they want to join the activity, before to launch the NWIP (in 2020 yet).

final considerations

Guideline give an overview of how to perform a task, procedure or policy. It is recommended but not is a mandatory.

Also, ISO/IEC 27001(*), about security, is accepted in many countries as a framework for information security / cybersecurity implementation. This NWIP initiative address in specific issues from space systems, not superseding the ISO 27001.

Although STAPsec is a security approach to STPA, it must be well adjusted for space systems applications.

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

Thank you
Carlos LAHOZ

carloslahoz@gmail.com

TC20/SC14/WG5 Brazilian delegate and author of two Standards:

ISO/IS 18676:2017. Space systems - Guidelines for the management of systems engineering.

ISO/CD 22893. Space systems - Software Product Assurance (under development)