IEEE INTERNATIONAL TECHNICAL STANDARD FOR SPACE SYSTEMS CYBERSECURITY

Why Space Systems Need Cybersecurity Frameworks and Standards?

- Widespread use of Commercial of the shelf (COTS) components
- Extremely complex supply-chains
- Complex operator ecosystems
- Lack of space industry-wide cybersecurity standards
- Every critical infrastructure is more or less reliant on space assets, hence space cybersecurity regulations are needed also for human and economic safety in other sectors
- International space cooperation needs harmonization of rules and practices to operate safely

Existing Space Cybersecurity Standardization Efforts

CCSDS (Consultative Committee for Space Data Systems): is an international organization that develops and promotes standards for space data systems.

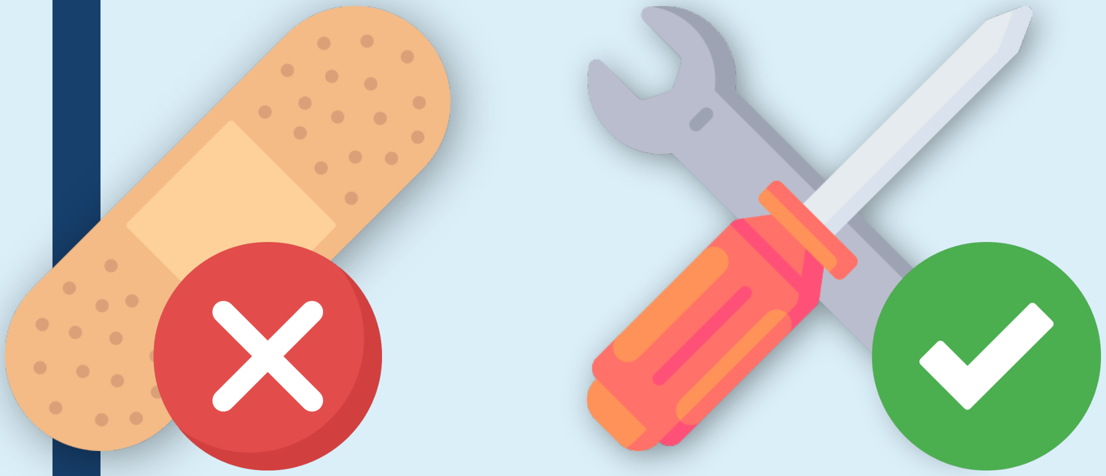
NASA Space Asset Protection Standard: the NASA Space Asset Protection Program (SAPP), established in 2019, has published a standard to establish protection requirements ensuring NASA missions are resilient to threats

German IT Baseline Protection Profile for Space Infrastructure : the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik or BSI) released in June 2022 its own guidance for the security of space assets.

Japanese Guidelines on Cybersecurity Measures for Commercial Space Systems: The Japanese Ministry of Economy, Trade and Industry (METI) has assembled a set of guidelines tailed specifically for security commercial space assets.

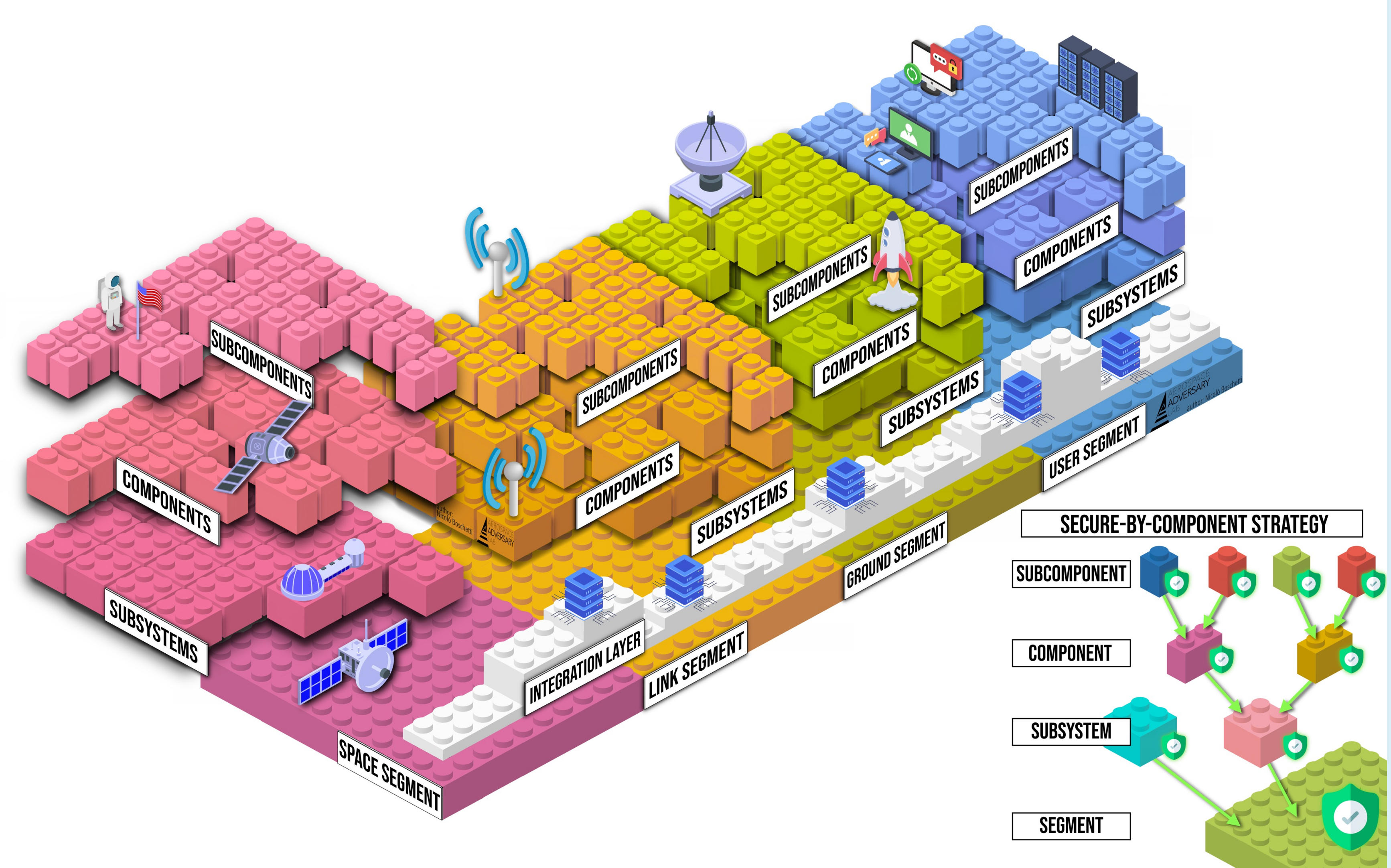
ECSS (European Cooperation for Space Standardization): is a cooperation between European space agencies that develops and publishes a set of standards for space systems, that could have repercussion on cybersecurity.

What is missing: Secure-by-Design

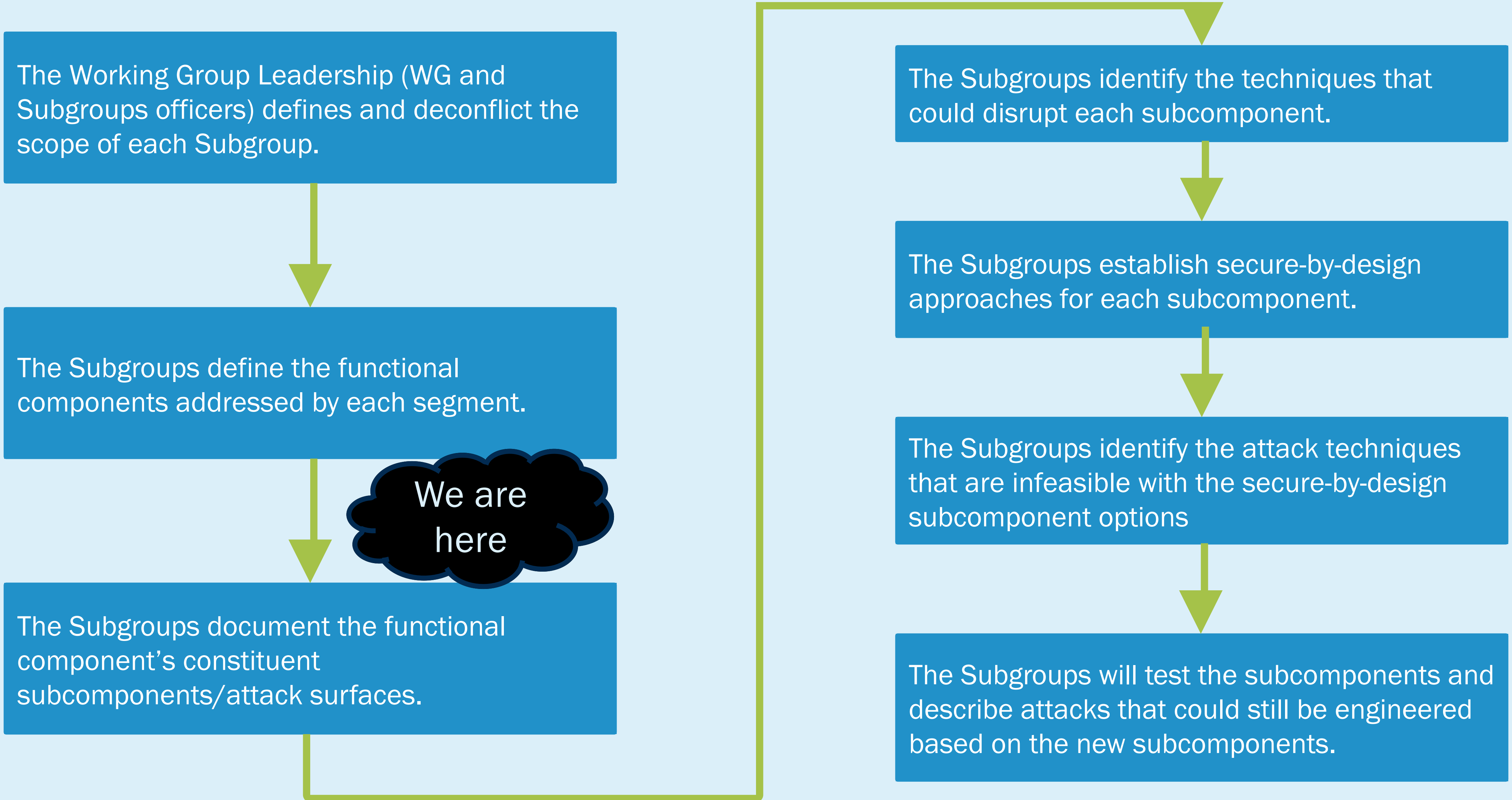


- Technical debt plagues most sectors, including the space ecosystem
- New Space has the unique opportunity to redefine systems that will be in use for the coming decades
- Adopting a secure-by-design approach to standards development moves away from the need for security controls to address poor design choices
- **Secure-by-design Standard enables future-proof requirements moving away from risk management guidelines**

Secure-by-Component



Our Process



The Working Group Leadership (WG and Subgroups officers) defines and deconflict the scope of each Subgroup.

The Subgroups define the functional components addressed by each segment.

We are here

The Subgroups document the functional component's constituent subcomponents/attack surfaces.

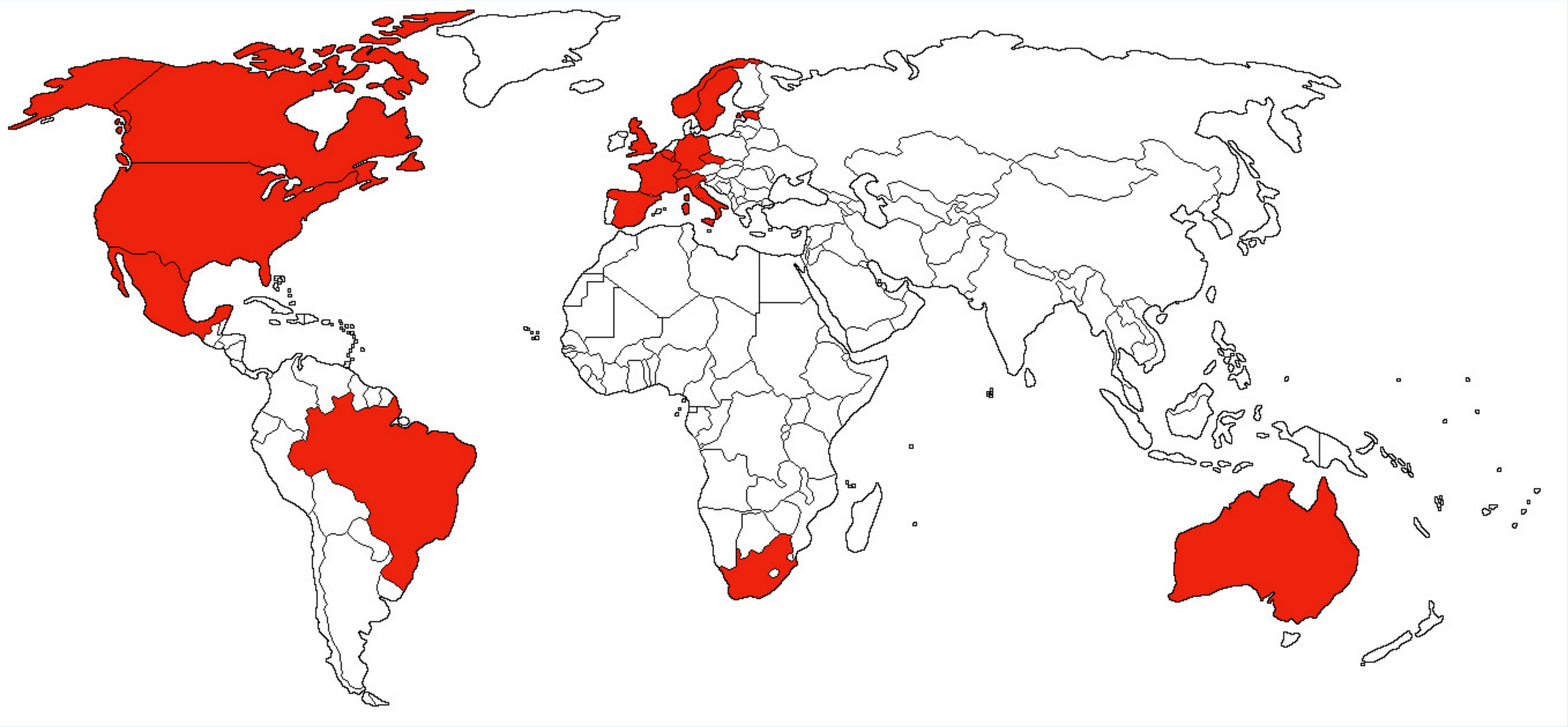
The Subgroups identify the techniques that could disrupt each subcomponent.

The Subgroups establish secure-by-design approaches for each subcomponent.

The Subgroups identify the attack techniques that are infeasible with the secure-by-design subcomponent options

The Subgroups will test the subcomponents and describe attacks that could still be engineered based on the new subcomponents.

WG International Participation to date



Subcommittees

Space Segment

- Satellite payloads (communication, imaging, etc.)
- Orbital positioning systems (GPS, Galileo, etc.)
- On-board computer systems

Link Segment

- Ground-to-space communication systems (antennas, transceivers, etc.)
- Space-to-ground communication systems (antennas, transceivers, etc.)
- Data encryption/decryption systems

Ground Segment

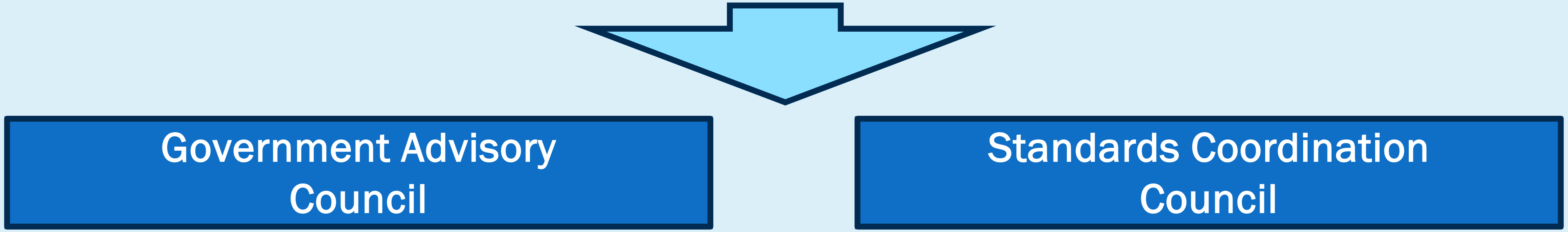
- Ground stations (command and control, data processing, etc.)
- Network infrastructure (fiber optic cables, routers, etc.)
- Cybersecurity systems (firewalls, intrusion detection, etc.)

User Segment

- End user devices (satellite phones, tablets, etc.)
- Ground-based communication systems (base stations, towers, etc.)
- Software applications (navigation, remote sensing, etc.)

Integration Layer

- Application Programming Interfaces (APIs)
- Data links (Ethernet, USB, etc.)
- Integration and testing systems (simulators, emulators, etc.)



Government Advisory Council

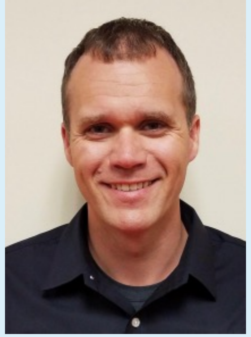
Standards Coordination Council

Leadership

Chair
Gregory Falco
gfalco@cornell.edu

Vice Chair
Jill Slay
Jill.Slay@unisa.edu.au

Secretary
Nicolo Boschetti
nb624@cornell.edu



SPACE SEGMENT
Brandon Bailey

brandon.bailey@aero.org

LINK SEGMENT
Gunes Karabulut-Kurt

gunes.kurt@polymtl.ca

GROUND SEGMENT
Kymie Tan
&
Arun A Viswanathan

kymie.tan@jpl.nasa.gov
arun.a.viswanathan@jpl.nasa.gov

USER SEGMENT
Carsten Maple

cm@warwick.ac.uk

INTEGRATION LAYER
Johannes Willbold

johannes.willbold@rub.de