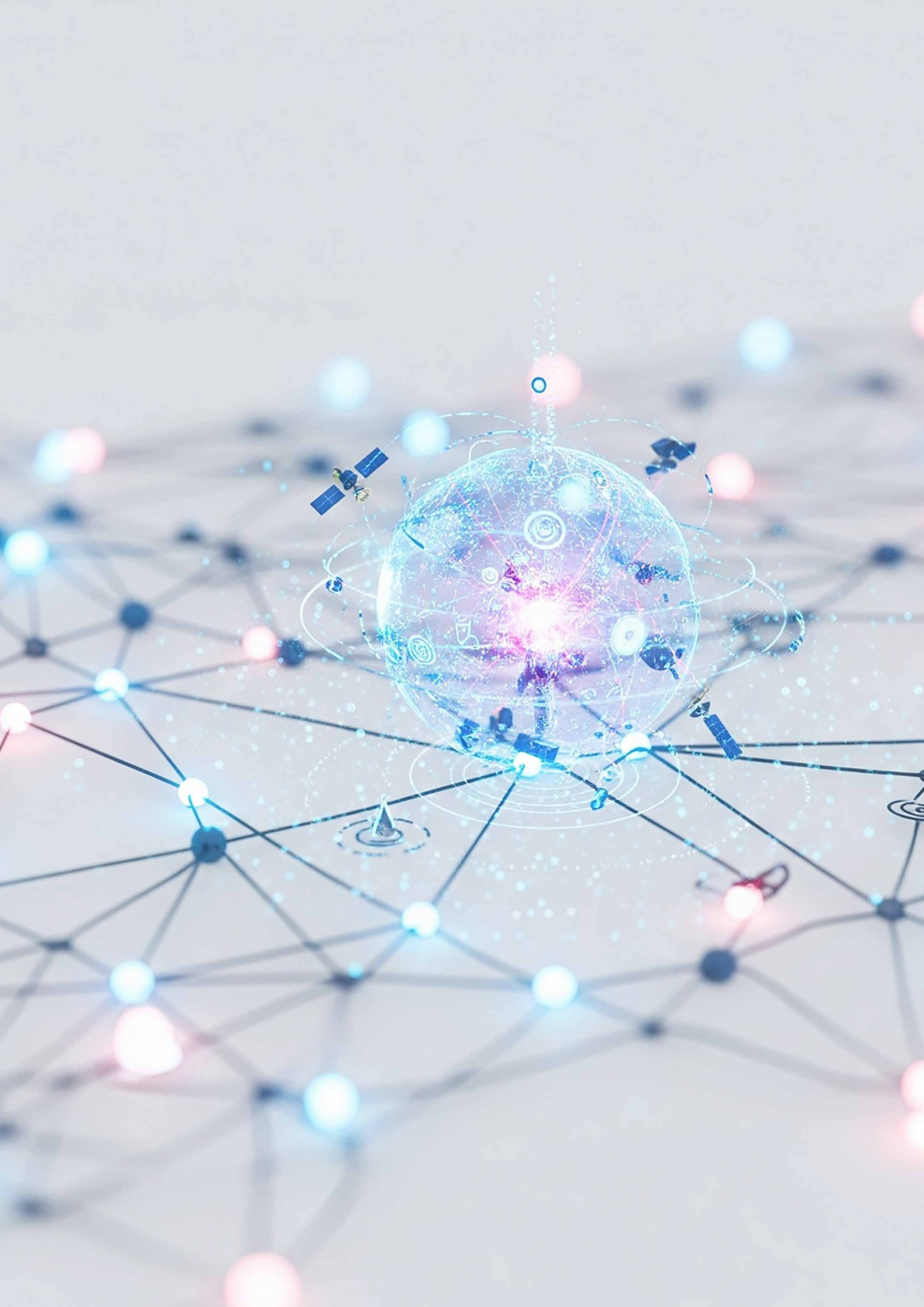
DEFENCE AND SPACE
Cyber Programmes Germany

Space Security, Let's Innovate!

Our White Paper about Space Security

AIRBUS



Content

Executive Summary

Airbus Defence and Space Cyber Programmes Germany is a fully integrated business of Airbus Defence and Space. Having protected Airbus Defence and Space's complex systems and networks for over 30 years, we, are leveraging our Airbus DNA to develop products and solutions for customers facing similar challenges, based on state-of-the-art trusted technologies.

Our teams are strongly involved in key space, military and defence projects, we are leading the End-to-End system security, starting from the Concept to the accreditation, we are driving innovation and building secure technologies to face the cyberthreat landscape and to be ready for the future challenges.

Since the Cybersecurity awareness month October draws to a close, Cyber Programmes Germany – leveraging its extensive background in cybersecurity for space and critical infrastructure – would like to share insights into key challenges for space security. We are sharing scenarios that highlight existing vulnerabilities and underscore the critical need to embed security from the earliest stages of system development. Our white paper is drawn upon our experience, vision, and findings, while also exploring the evolving need for space-based support for other critical infrastructures, such as the energy and the maritime sectors.[1]

[1] Inputs provided within this white paper are subject to discussion and different opinions and visions.

Ms. Amal Mosbah

Cybersecurity leader with +16 years of experience designing, delivering and managing critical infrastructure products and solution with a special focus on security architecture, compliance and certification, I am currently Head of System Engineering leading an exceptional and unique team of cybersecurity and aerospace experts and architects, playing a key role in shaping future space security.

Dr. Nils Maeurer

A seasoned Cybersecurity Expert, I spearhead the cybersecurity architecture initiatives for cutting-edge space communications systems, ensuring robust protection and resilience. Recognized as an expert in system architectures for end-to-end secure and resilient SATCOM, I have made significant contributions to the field. Additionally, I authored the RFC 9372 and is I am dedicated 7-year member of the IEEE.

M. Shehryar Ishtiaq

Driven by a passion for space exploration and digital defence, I am a Cybersecurity and Aerospace Architect dedicated to safeguarding the future of space industry through innovative cyber security solutions. I bring proven expertise and industry-recognized credibility to fortify the cybersecurity foundations of the space domain and build a resilient and secure space ecosystem that supports humanity's continued expansion beyond Earth.

M. Maximilian Roth

Cybersecurity and Aerospace Architect; I am dedicated to strengthening resilience and embraces todays and future challenges in space. With several years of experience in space field with the German Space Agency and member of BSI expert group "Cybersecurity in Space" I am contributing to security of future space system and I am a co-author of multiple BSI publications.

Introduction

Space Security Key Drivers

Satellite deployment and usage have grown significantly in recent decades. Initially serving scientific purposes, their applications now include communication, military, and aeronautical uses. Commercial satellites are now crucial for essential services and global connectivity, which, in turn, creates cybersecurity challenges and necessitates safeguarding national and European sovereignty.

Several initiatives have been launched to promote the need for security regulations in the space sector.

On June 25, 2025, the European Commission released the EU Space Act, a proposed regulation addressing the safety, resilience, and sustainability of space activities within the European Union.[2]

In the same year, the US introduced the "Secure Space Act"[3] to the House of Representatives, which has since been passed by the House.

At the German national level, the BSI has published TR-03184[4] Information Security for Space Systems.

[2] https://defence-industry-space.ec.europa.eu/eu-space-act_en
[3] https://www.congress.gov/bill/119th-congress/house-bill/2458
[4] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03184/tr-03184.html

Many **Cyberattacks on space systems are backed by nations seeking strategic advantages**.

These operations often involve espionage, sabotage, or attempts to disable critical infrastructure.[5]

Feb 2022

Viasat KA-SAT

Deployment of wiper malware called "AcidRain" that was designed to remotely erase vulnerable modems and routers causing the interruption of the Internet services impacting critical Infrastructure

Sep 2024

TIDRONE Campaign

Cyber espionage campaign targeting entities in Taiwan's military and satellite industries

Early 2025

Breach Attempts Starlink Infrastructure

Russian state-linked hackers (e.g., APT Turla/Secret Blizzard) were reported to be persistently targeting Starlink/SpaceX

ground/terminal infrastructure, exploiting hardware and software weaknesses

Aug 2025

GPS Spoofing Attack

GPS Spoofing is ongoing since months and has a very big impact on the Aviation industry specially in conflict areas

[5] The different listed cyber-attack as well as the attempts are extracted from different reading and different public sources.

Space System Security

Let's innovate!

The space industry can significantly benefit from the knowledge and progress made in various fields during the industrial revolution, including Edge Computing, IoT, and AI.

By considering satellites as IoT devices and constellations as the cloud, we can draw inspiration from the security measures and controls implemented in the Edge Industry to address the challenges of Space Security.

Satellites as IoT Devices

Data Collection
Satellites, or even small devices on them, can function like IoT sensors or trackers, collecting data from vast, hard-to-reach areas of the Earth.

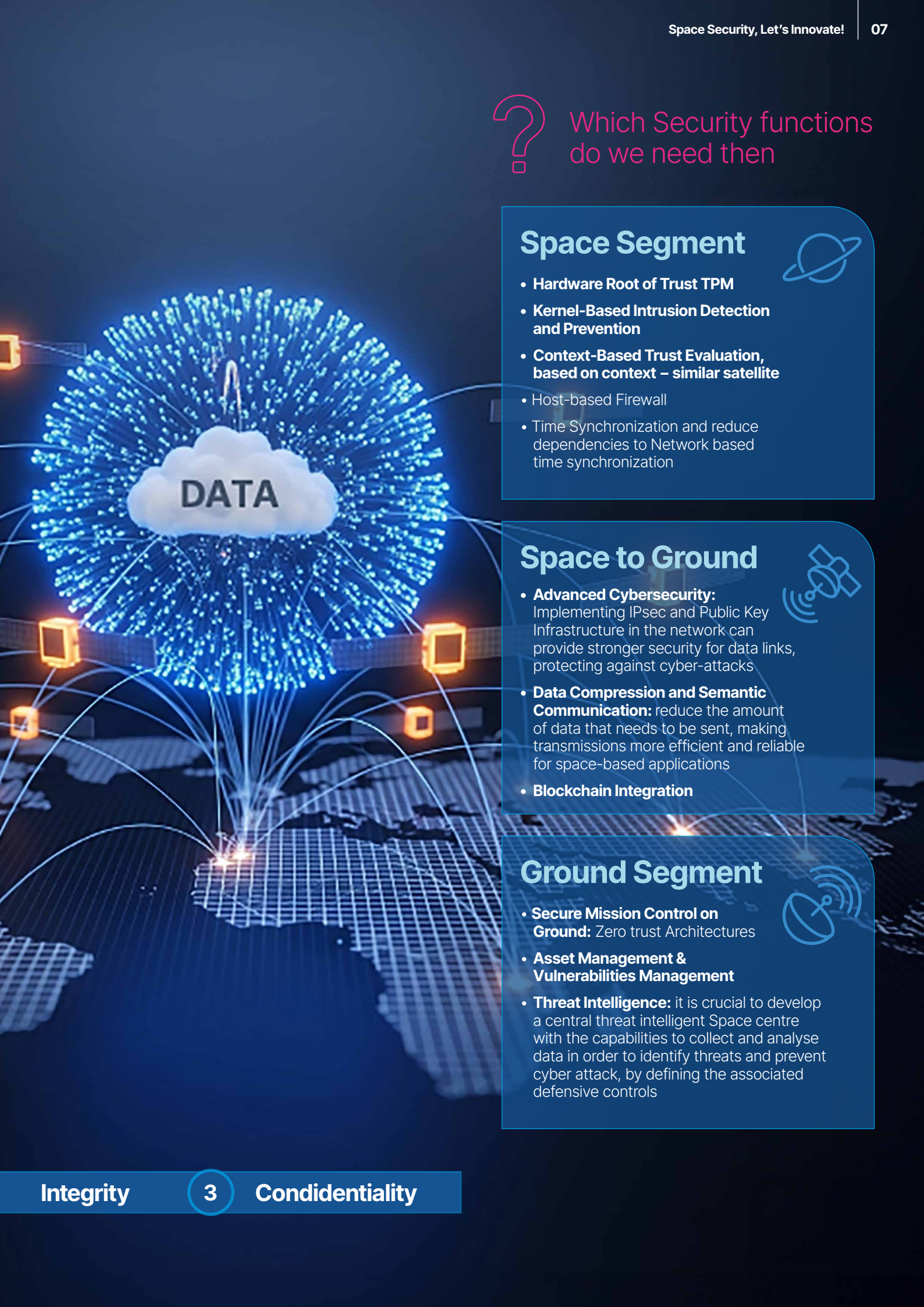
Data Transmission
These satellite "IoT" devices then transmit their collected data to a larger satellite constellation, similar to how a typical IoT device sends data to a gateway or the cloud.

Orbit (Constellation) as the Cloud

Distributed Computing
A constellation of satellites acts as a distributed cloud, receiving data from individual "satellite IoT" devices.

Data Routing and Processing
Data is routed through the constellation and potentially processed or aggregated at various points within the network before being relayed to the ground.

Bridging Connectivity Gaps
The entire system provides a robust, resilient, and global network that bridges gaps in terrestrial networks, offering connectivity where it was previously impossible or unreliable.



Which Security functions do we need then

Space Segment

- **Hardware Root of Trust TPM**
- **Kernel-Based Intrusion Detection and Prevention**
- **Context-Based Trust Evaluation, based on context – similar satellite**
- Host-based Firewall
- Time Synchronization and reduce dependencies to Network based time synchronization

Space to Ground

- **Advanced Cybersecurity:** Implementing IPsec and Public Key Infrastructure in the network can provide stronger security for data links, protecting against cyber-attacks
- **Data Compression and Semantic Communication:** reduce the amount of data that needs to be sent, making transmissions more efficient and reliable for space-based applications
- **Blockchain Integration**

Ground Segment

- **Secure Mission Control on Ground:** Zero trust Architectures
- **Asset Management & Vulnerabilities Management**
- **Threat Intelligence:** it is crucial to develop a central threat intelligent Space centre with the capabilities to collect and analyse data in order to identify threats and prevent cyber attack, by defining the associated defensive controls

Integrity 3 **Condidentiality**

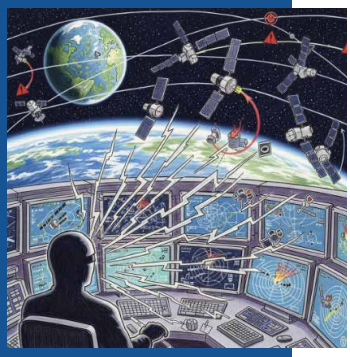
STORYTIME

How Secure do you think your Space System is?

SCENARIO 1

Interceptor satellites

Did you know, satellites, once presumed to be out of reach for attackers, were never really out of reach at all? The concept is perhaps as old as the space industry itself. Take for instance the KOSMOS interceptor satellites developed in the 1960s as part of the Soviet anti-satellite (ASAT) program, which flew close to U.S. spy satellites throughout the 1970s and 1980s and even as recent as 2020 – to monitor and observe them. This long lineage continued into 2025, when Kosmos-2558, a modern Russian inspector satellite, again maneuvered near the U.S. reconnaissance satellite USA 326, reportedly releasing a secondary object while in co-orbit- an event tracked and analyzed by TU Delft experts. Most recently, the Chinese Shiyan-24C (three satellites) and Shijian-6 05A/B (two satellites) in 2024 demonstrated similarly precise synchronous maneuvers, described as a "dogfighting exercise in space." Such interceptor satellites, active from the 1960s through 2025, illustrate a continuous evolution of proximity-operation capabilities and remain a crucial consideration in the design of robust space cybersecurity concepts to prevent observation and information leakage.



SCENARIO 2

Attack on SSA System

With the ever increasing space debris and new satellites are being inserted to orbits, the space is getting crowded – pun intended. Most modern satellites have a Space Situational Awareness system to help and assist with avoiding a collision or similar catastrophic event. These systems provide information to operations control to take a decision on evasive maneuvers to avoid the developing situation, sometimes even assisted by automated systems. These SSA systems can be attacked to trigger a response in order to steer particular space assets into desired positions for strategic advantage or even cause disruption or Denial of Service.

SCENARIO 3

Cyber and Space Situational Awareness

Did you know that with clever techniques it is possible to extrapolate active zones and predict things planned to happen before they even take place? In this scenario a situation is explored where based on traffic data, the layer of protection mechanisms, encryption level etc. It is possible to predict, for instance, where the Red assets are concentrated? How do they plan on moving? Which type of assets are they? In modern architectures this could even enable inter-domain analysis based on various parameters such as how much traffic flows through which zone or simply a change in a satellites position and orientation (pose).

SCENARIO 4

Anyone Listening? The Open Secrets of Space Communications

Even today, SatCom too often ships without the basics-end-to-end encryption, strong authentication, or hardened user terminals – so signals, control links and even telemetry can be intercepted or spoofed with commodity kit and open-source stacks; DEF CON Aerospace Village talks repeatedly demonstrate practical attack chains against cubesats, modems, radiosondes and operator networks. Real-world reporting and peer-reviewed research confirm the risk: investigative work has shown unencrypted GEO traffic leaking calls, texts and corporate/military metadata to inexpensive receivers.

Systemic vulnerabilities in SatCom user-segment modems and ground equipment that make exploitation straightforward are discovered on a daily basis. Fixing this requires immediate adoption of secure-by-default cryptography and key-management (following contemporary key-length guidance) and a designed migration path to post-quantum algorithms-NIST's transition guidance and key-length recommendations both emphasise hybrid and staged upgrades because satellites routinely remain in service for decades, so a today's crypto choice must survive tomorrow's quantum era.

LET'S GO

Have you thought about Deep Space Missions?

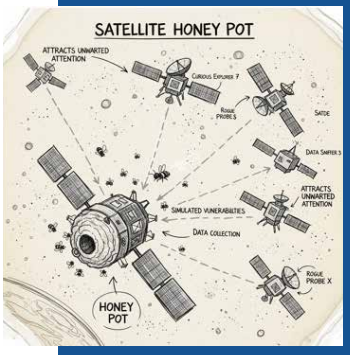
Within Airbus Defence and Space Cyber Programmes Germany we are performing the first Security concept for Deep Space Mission. We look at deep space missions from a unique perspective and propose a two tier solution tailored to the operational landscape of the spacecraft through its entire lifecycle.

Usually thinking about deep space most often cyber security is ignored due to the assumption how can one attack a deep space satellite without deep space antenna? But spacecrafts that have to go into deep space, have to fly through lower orbits and GTO! It is during this time that the spacecraft can be attacked even by amateur antennas if proper protection is not implemented causing significant damage whether monetary or critical mission delay.

For instance in a two tier lifecycle protection system: the spacecraft is evaluated first for the GTO phases against attacks, e.g. stronger encryption and authentication schemes, and then for the deep space phase, freeing resources such as computation power to be used for other data processing functions.

THINK ABOUT IT!

What About Space Honeypots?



The application of honeypots in the space domain, particularly through the development of satellite honeypots, offers a unique opportunity to proactively address the growing threat of cyberattacks against space assets. By intentionally creating decoy satellite systems designed to attract and observe malicious activities, we can gain invaluable insights into the methods, tools, and objectives of state-sponsored and other sophisticated actors targeting space infrastructure. This approach not only aids in identifying zero-day vulnerabilities in satellite systems but also allows for real-time analysis of attack vectors, ultimately strengthening the resilience and defensive capabilities of genuine operational satellites and ground segments. The intelligence gathered from such deployments can inform the development of advanced countermeasures, secure by design principles for future space missions, and enhance overall space situational awareness from a cybersecurity perspective.

Space Situational Awareness: Need for Security

Space Situational Awareness (SSA) which is often referred to as Space Domain Awareness (SDA) which is the combination of analysis of Space Weather Events (SWE), Space Surveillance, Tracking (SST) and Near-Earth Objects (NEO).

SST provides an overview of what happens in space around the clock.

Is a collision coming up? Then, a collision avoidance maneuver might be necessary.

Did space debris scatter into multiple smaller elements? A detailed fragmentation analysis can be performed to improve situational awareness.

Is an object coming closer to Earth to re-enter Earth's atmosphere? A comprehensive analysis of this re-entry is useful to understand its possible impact on the surface to warn the affected population.

Therefore, many governmental (e.g., ESA, DLR, EU) and commercial organizations are working on creating a complete overview of the space environment.

For SST, a combination of different sensors is necessary: radar to track LEO satellites and to create a survey over a certain area to detect new objects (or objects which are off their predicted orbits); Satellite Laser Ranging can be used to detect single objects with extremely high precision; Telescopes can be used to create a small surveillance area and to analyse single (or close by) objects. The combination of these three devices brings the strengths of each to the table and highly improves the object catalogues in which all detected objects are listed with their latest orbit parameters (and other important information).

SST reduces, in times of highly increasing number of objects, the probability of a collision of a high value target, such as an expensive research satellite, due to the high update rate of the orbit parameters of all (detectable) objects around the satellite which helps to determine when an evasive maneuver is needed. The SST organisation often provides a probability of collision between two objects. Some even provide maneuver recommendations – however, the task has always to be performed by the owner/operator.

This highlights the crucial need to secure all communications, connections, data processes, and exchanges with various partners.

Optimal Security is inherently integrated, not superficially applied, retrofitting security into an existing system is not only more costly but also typically less effective. Given the current cybersecurity threat landscape, we must depart from conventional practices and adapt our processes and workflows to embed cybersecurity from the beginning.

Secure By Design

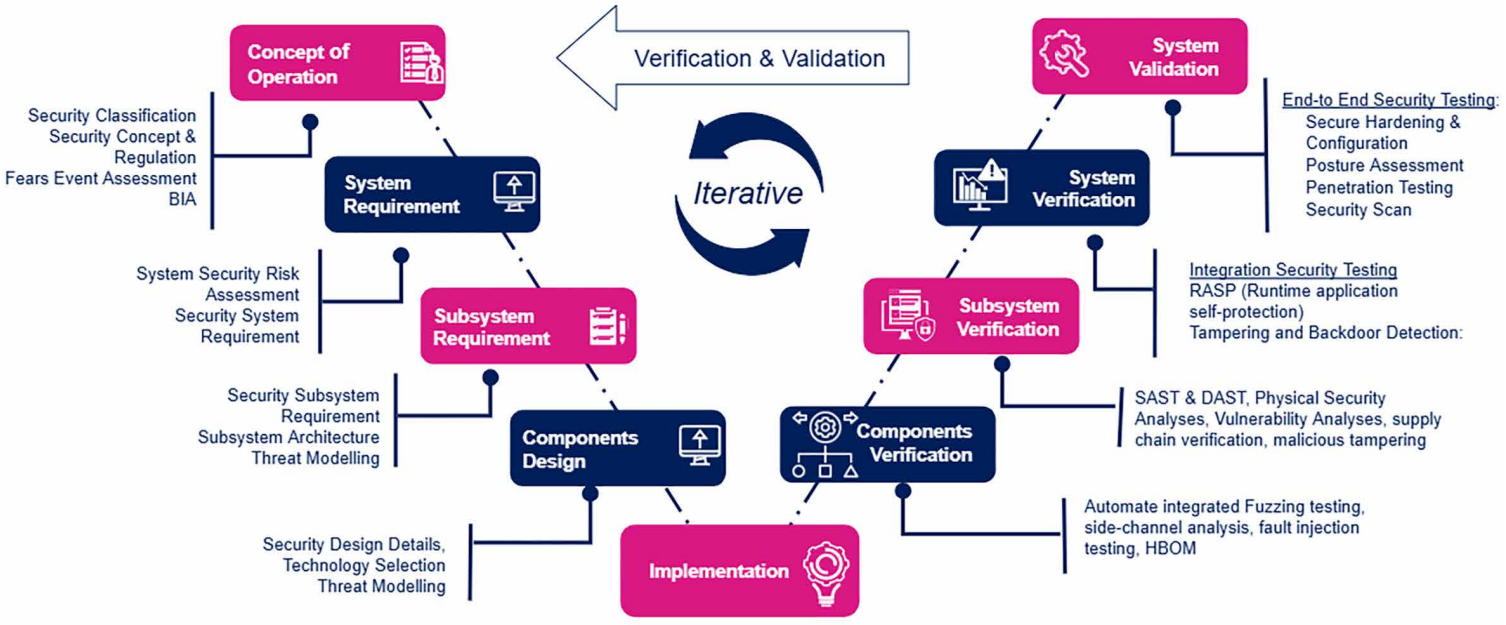
How to ensure the End-to-End System Security?

To achieve a Secure Space Mission, a comprehensive approach is required that integrates security considerations throughout the entire system lifecycle, from initial design and development to deployment and ongoing operations. This "Security by Design" philosophy emphasizes proactive measures over reactive responses, fostering a robust and resilient space infrastructure.

Security in the V-Model Development

The V-Model, a widely adopted system development methodology in the space industry, provides a structured framework for integrating security requirements throughout the system lifecycle. By embedding security requirements, measures and controls into each phase, from requirements definition to system acceptance, the V-Model facilitates the creation of inherently secure space systems. This includes defining security objectives, conducting threat modelling, designing security controls, implementing secure coding practices, and performing rigorous security testing at every stage.

Furthermore, the development of referential architectures tailored to specific space mission classifications (e.g., Critical Mission, Manned Mission, Scientific Mission ...) is crucial. These architectures will serve as blueprints, outlining standardized security measures, protocols, and best practices relevant to the operational environments and threat landscapes of each mission type. This approach ensures a consistent and comprehensive application of security, moving beyond generic solutions to provide targeted and effective protection for diverse space assets



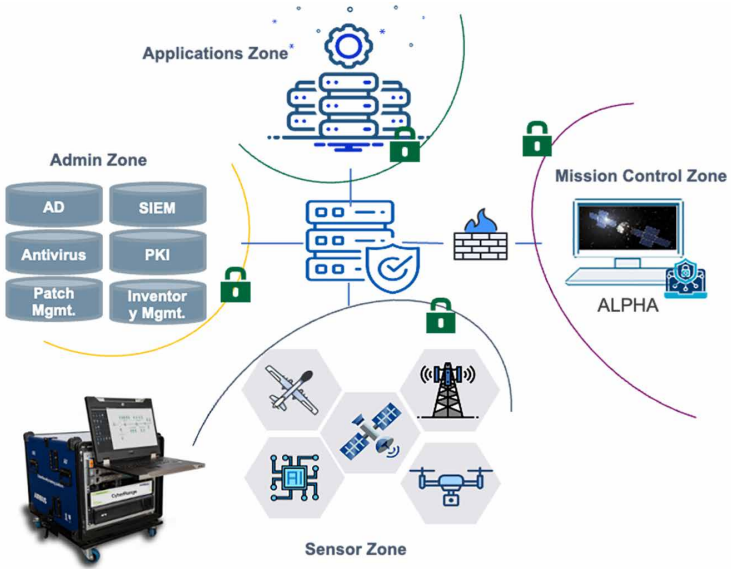
Secure Platform to Build Secure Missions – COTS

The integration of Commercial Off-The-Shelf (COTS) space products is becoming increasingly vital to address the evolving security requirements of diverse space missions. COTS products offer a compelling advantage by providing flexibility and adaptability, allowing for rapid deployment and customization to fit various mission classifications (e.g., Critical Missions, Manned Missions, Scientific Missions...).

This approach does not only streamline development cycles but also enables the seamless incorporation of future security enhancements and capabilities, ensuring that space systems remain resilient against emerging threats. By leveraging COTS solutions, the space industry can achieve a more agile and cost-effective approach to securing its assets, while maintaining high standards of reliability and performance.

However one of the challenges that we need to overcome is the definition of a Space Cybersecurity standard to be used as guideline for the mission development, today there are several cybersecurity standards in use, e.g. the **NIST 800-53**, also the IT Security standards like **ISO27000** familly. Nevertheless, space has its specifications that need to be taken under considerations.

The European Space Agency ESA has classified Space Missions according to the criticallity, this is an important step twoards defining reference architectectures and standarizing the secuirty requirements based on the mission classification.[6]

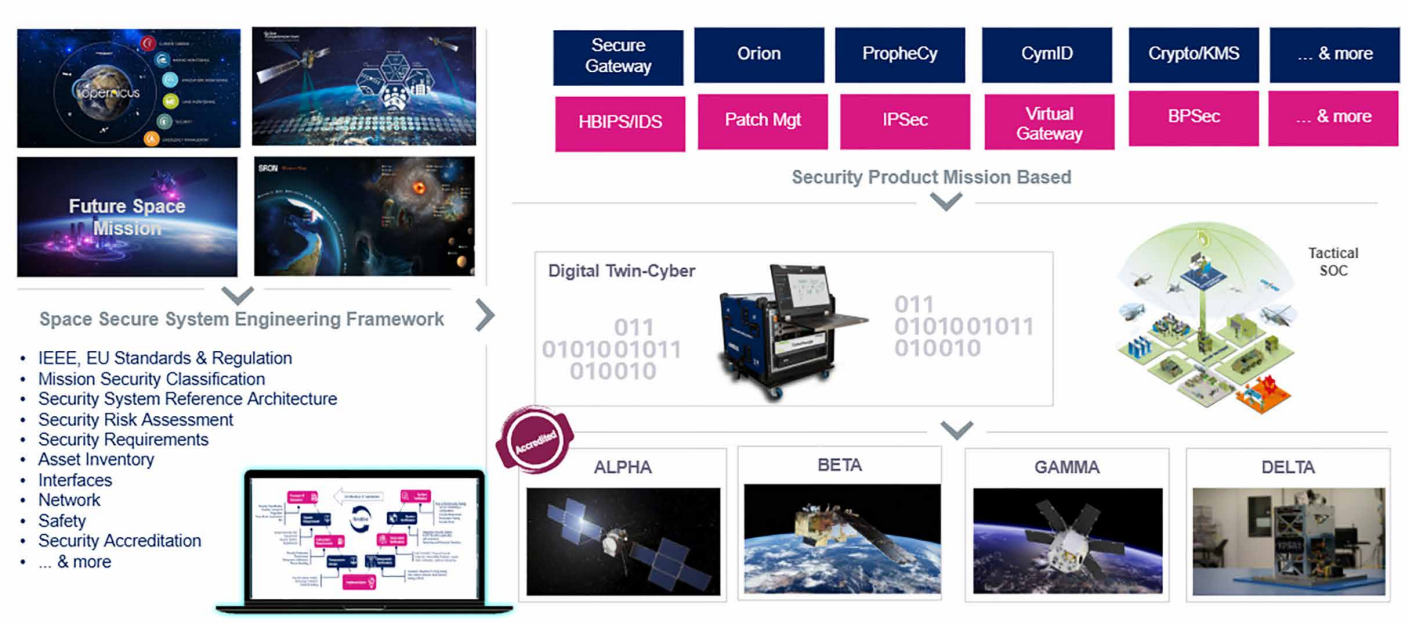


Cyber Simulation and Digital Twins for Space

Verification and validation are crucial phases in mission development. To ensure a successful delivery, it is essential to have a cyber environment that provides the capabilities for system integration and testing, security testing, and interfacing with various external systems for the end-to-end verification and Validation, a Cyber digital twins can be the solution for Space missions.

A Space Cyber Simulation Environment will provide the capability to implement the security concept from system and network design, modelling the different zones, define the communications protocols and interfaces and the different security controls, we will be then able to verify and validate the compliance and robustness of the security solution and perform the different security testing required before the go-live of the Mission.

[6] Mission Classification as well as the Mission example are from the European Space Agency (ESA), ref. CMIN 2025



One Platform Multiple Mission Designs & Simulation

End to End Testing and Simulation

Simulate the Ground Segment, IT Infrastructure and Network, with the capabilities to integrate supplier product and interface with external system e.g. the Satellite, User Segment, **UAVs** …

Support Accreditation Process

Capabilities to verify and validate security requirement (incl. secure hardening) and perform security testing including Penetration test to support the Auditing and Accreditation process, in addition to the continuous vulnerability management and security patch testing

Flexibility and Openness

Capabilities to Model real or representative system, and integration of new product / system e.g. threat intelligence to monitor the evolvement of the Cyber threat or New Security Modules e.g. IPSec, New System e.g. Spacecraft

The Emergence Use of Satellites to support other Critical Infrastructure

Power Grid: Opportunities and Challenges

The Power Grid and Power plants are one of the most critical infrastructures which are nowadays facing challenging security threats and strongly depend on the geopolitical situation.

The re-thinking of the communication and security of power grids is evolving and Space Communication could be the solution to face limitations of the current physical communication relied on by the energy sector.

The advancement of technology, transitioning from 5G to non-terrestrial networks, coupled with the enhanced capabilities of new satellites, offers substantial benefits for Power Grid operations and optimization.

Such technologies will be crucial for strengthening the energy sector through secure communication channels, expanding connectivity to rural areas, providing capabilities for monitoring and forecasting energy production with accurate functionalities like methodological information and geolocation information, in addition to providing redundancy capabilities and resilience against terrestrial disasters.

Enhance and Secure Maritime and Harbour Operations

The maritime and harbour industry, much like the energy sector, faces significant cybersecurity challenges. While Space geolocation and surveillance are already integral to maritime operations, there's a critical need to secure and enhance these capabilities, especially given the escalating threat of cyberattacks.

Non-terrestrial networks technologies offer substantial benefits for optimizing and improving the performance of container terminal operations. Additionally, advances in geolocation and imaging can greatly enhance safety within these environments. However, as critical and safety-sensitive infrastructures, harbour operations demand robust security controls and high resilience.

We will elaborate further about the capabilities that space System can bring to the security of the Energy, Harbour and Maritime operations in our next **White Paper**.

How can we support you?

Our teams provide comprehensive cybersecurity services across the space domain, encompassing ground, space, and user segment security. We possess extensive knowledge of cybersecurity standards and certifications and actively contribute to national and European standardization groups to advance space security guidelines.

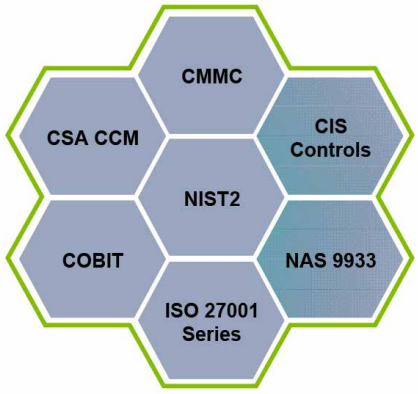
We provide Tailor Made Secure Aerospace & Defence Solution Space, Ground Station, and User Segment

Ground Segment Security

- System Security Architecture
- Network Security (Secure Gateway, NGFW...)
- Secure Communication
- Information Security Concept
- Secure Hardening
- Security Testing
- Secure Kubernetes and Virtualization
- Cloud Security & more

Space Segment Security

- System Security Architecture
- Onboard System Security
- Payload Security
- Secure Communication and Quantum Cryptography
- Secure 6G/5G TNT
- Smart Satellite (AI) & more



Security Assessment & Compliance

- Risk Assessment and Controls
- Compliance Assessment
- Maturity Assessment
- Accreditation Plan & Certification
- System Security Requirements Statement
- Audit & Pen Testing
- Secure Operations

To know more about our Services **here**

Contacts

For more information about our activities in Airbus Defence and Space Cyber Programmes Germany you can contact **cyberprogrammes-sales@airbus.com**

AIRBUS

Airbus Defence and Space
Willy-Messerschmitt-Str. 1,
82024 Taufkirchen, Germany

Reference 0287-1. December, 2025.
Concept design by grafik@mendel-design.com.