04/2024

BDLI Whitepaper

Security for Space Systems

Connecting.The.Dots.

Content

Contact

Sentiana Schwerin
Manager Digitalization,
Cyber Security & UAS/AAM

schwerin@bdli.de
+49 173 769 7881

Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V.

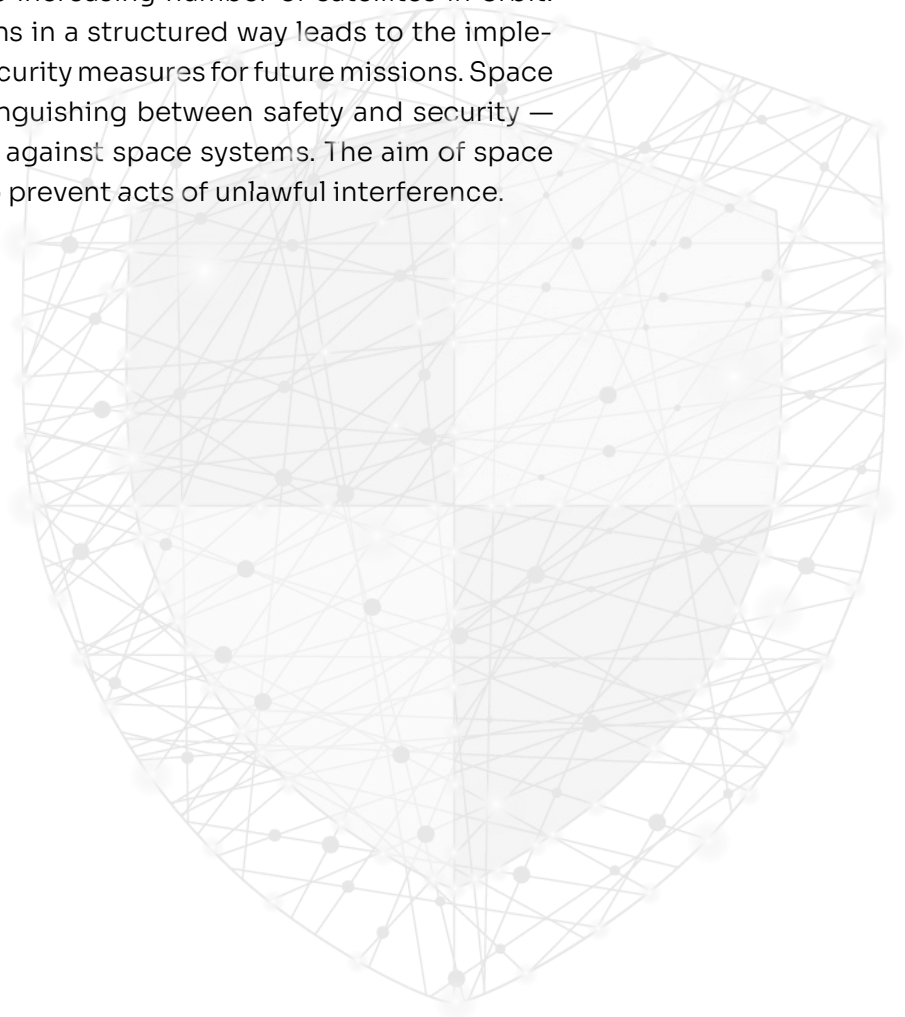
ATRIUM | Friedrichstraße 60 | 10117 Berlin
Tel. +49 30 2061 40-0 | kontakt@bdli.de

www.bdli.de

Introduction

Threats to space-based systems are becoming increasingly numerous and complex. It is therefore necessary to address these threats by implementing industry-wide standards. Significant efforts are being made to develop guidelines in this field. For example, the German Federal Office for Information Security ("BSI") defines the key objective of cyber security for space infrastructures as follows: **Strengthening cyber security for space infrastructure with relevance for government, the economy and civil society in order to safeguard the availability of services via secure and trusted communication.**[1] For this purpose, the BSI has published a profile and a technical guideline targeting security for space systems.

Documents such as the above help to understand and manage the risks to space missions and ensure secure and successful operations. This is especially important considering the increasing number of satellites in orbit. Managing risks to space missions in a structured way leads to the implementation of necessary cyber security measures for future missions. Space systems security — clearly distinguishing between safety and security — exists to prevent malicious acts against space systems. The aim of space systems security is, therefore, to prevent acts of unlawful interference.



1 https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfeehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt.html

1. Scope of This Document

This document gives an overview of the national and international efforts regarding the definition of guidelines for the aerospace industry. It explains why and in which way cyber security needs to be implemented for space systems.

For this purpose, space systems architecture is described, followed by an explanation of the security-by-design approach recommended for space systems. Next, a threat analysis shows the main threats that need to be controlled by cyber security measures. Furthermore, industry standards in the fields of cyber security or cyber security of space systems are mentioned. Then, the minimum requirements for space systems are explained, followed by a description of information security for space systems.

2. Space Systems Architecture

In this context, architecture refers to different parts working together or interacting to achieve a specific purpose. Space system architectures are based on the mission they perform, with each mission having a specific architecture. Nevertheless, space systems architectures generally have several components in common. The general architecture can be broken down into three physical parts: the space segment, the launch segment and the ground segment.

Relevant classes of space missions are communication, positioning and navigation, weather, remote sensing and launch. Satellite communications enable the exchange of data across the globe within the footprints of the antennas of the network of communication satellites. Such communication relies on ground telecommunication infrastructure, transmitters and receivers to facilitate critical communications under a wide range of circumstances and situations.[2]

Satellite positioning and navigation systems enable the location of a position all over the world, on land, the sea, or in the air at any time, allowing continuous information even when using a moving receiver. This is particularly relevant where maps or orientation points are unavailable or limited.[3] Meteorological missions consist of a series of satellites providing observations and measurements from orbit for numerical weather prediction and also contributing to climate monitoring.[4] Finally, remote sensing missions enable the monitoring of the physical characteristics of an area by measuring its reflected and emitted radiation at a distance.

Satellites contain payloads to accomplish their primary mission and the necessary infrastructure for operating the payload.

2 https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Space_for_Earth/Space_for_health/Satellite_communications
3 https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Space_for_Earth/Space_for_health/Satellite_positioning_navigation
4 https://www.esa.int/About_Us/Business_with_ESA/Business_Opportunities/Meteorological_Missions

3. Security by Design for Space Systems

The security-by-design approach ensures that security is incorporated into the system starting from the earliest design phase. Security by design (or secure by design) refers to a range of security practices aiming to create systems that are impenetrable to cyber-attacks. The principles of security by design involve incorporating security measures into the entire life cycle of space systems, including design, development and operation.

Lifecycle phases in focus:

- Conception and design
- Production
- Testing
- Transports
- Commissioning
- Operation
- Decommissioning

Security for space systems is addressed starting from the first lifecycle phase in focus, conception and design. As a result, secure design is integrated into the product from the very start of the project.

4. Threat Analysis

For cyber security measures to be implemented, it is important to get an overview of the relevant threats. Here below are listed some of the most urgent threats to space systems:

- Ground-based active interference (agent in the ground station)
- Ground-based adjacent active monitoring and interference (agents with special equipment in neighbouring buildings, etc., with access to the Internet infrastructure or via radio relay to the antenna systems)
- Reading and encrypting optical laser links
- Disruption of connection to the satellite at low elevation
- Space debris (including purposeful creation of space debris)
- Espionage satellites in close encounter/in LEO (e.g. attacking Galileo)

5. Cyber Security for Space Systems

There are several different cyber security standards available. The following standards are amongst the most commonly applied industry-wide standards:

- ISO 27k standards
- NIST standards
- BSI IT-Grundschutz (IT baseline protection) standards
- Further European standards, including EBIOS standards

When it comes to cyber security for space systems, some standards/guidelines have been published just recently or are still under development:

- NIST publications: NISTIR 8270 “Introduction to Cybersecurity for Commercial Satellite Operations”, NISTIR 8323 Rev. 1 “Foundational PNT Profile (Final)”, NISTIR 8401 “Satellite Ground Segment (Final)”
- Planned publication: ECSS-Q-ST-80-10C DIR1 “Space product assurance – Security in space systems lifecycles”

6. Minimum Requirements for Space Systems

The BSI IT-Grundschutz Profile[5] Space Infrastructures—Minimum Protection for Satellites Covering their Entire Life Cycle defines minimum requirements for space systems. It provides assistance in formulating requirements for minimum protection measures during the planning, manufacturing and operation of a satellite until the end of its mission. It covers at least the basic protection requirements for all types of satellite missions. The described security measures protecting the confidentiality, availability and integrity of information aim to minimise material loss and intangible damage across a satellite’s lifetime.

However, security measures must be adapted to each mission profile. The document also includes a list of relevant assets to be protected (applications, IT systems and premises), an assignment of corresponding BSI IT-Grundschutz modules and a checklist to support the implementation of those security requirements deemed necessary for the respective mission.

5 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=2

7. Information Security for Space Systems

Apart from the minimum requirements described in the profile, there are security measures that are recommended for space systems. The Technical Guideline[6] BSI TR-03184 maps relevant security measures to potential threats. Security measures include the following:

Technical security measures are concerned with implementing certain concepts, such as a backup concept, a configuration management concept and a patch management concept. Technical security measures also include the use of specific systems such as intrusion detection and prevention systems or security information and event management systems. In addition, certain methods, such as checksums, need to be applied to check the integrity of sent/received information. One last important aspect is carrying out vulnerability scans or penetration tests.

Additional IT-based security measures are concerned with the use of mobile devices under lock and key, the use of virus protection programs and remote access/remote deletion in case of loss of equipment.

On the other hand, organisational security measures are concerned with the training of staff on specific topics, such as handling certain equipment, as well as general security awareness. Emergency procedures also need to be put in place. For visitors coming to site, rules need to be implemented concerning the visibility of badges and the supervised presence in restricted zones. Another field of organisation security measures includes cyber threat intelligence and intelligence sharing amongst organisations.

Physical security measures consist of measures concerning the setup of secured/restricted areas (including monitored access), instalment of different types of environmental protection (e.g. fire alarm, fire extinguishing systems, air quality monitoring, protecting equipment against moisture, radiation monitoring, air conditioning), but also the use of clean rooms, fixing devices at their workplace or keeping documents and media under lock and key.

Security measures for software are integrity checks of the software supply chain, allowance of the installation of only tested and approved software and software supplier checks.

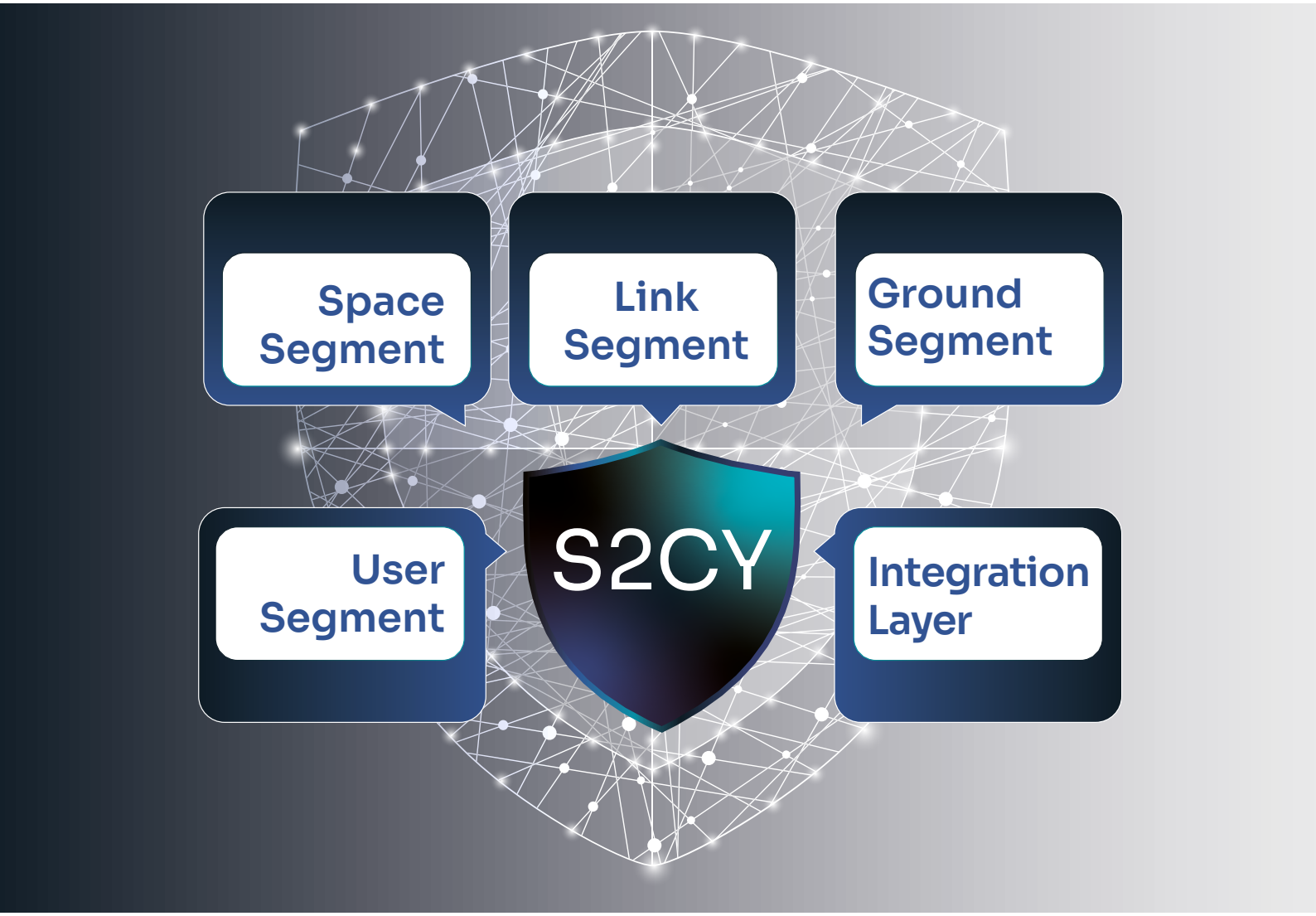
Network-specific security measures include setting up the network as a security zone or making use of separate task-specific networks.

Satellite-specific security measures are suitable frequency band management, communication with the satellite in several communication channels/media, encrypted communication, and detection of communication problems.

6 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile&v=2

8. Conclusion

The IEEE Standards Association P3349 - Space System Cybersecurity Working Group [7] is currently working on establishing international standardisation for space systems. For this purpose, the working group is divided into several subgroups, as shown in the following graph.



Further resources:

- The paper[8] summarises space security standardisation efforts
- SPARTA[9]
- ESA SPACE-SHIELD[10]

7 https://sagroups.ieee.org/3349/the-project/
8 https://australiancybersecuritymagazine.com.au/wp-content/uploads/2022/12/6.2022-4302-Int-space-standard.pdf
9 https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c
10 https://spaceshield.esa.int/

Both Sparta and ESA Space Shield are based on the MITRE ATT&CK® Matrix. Adversary tactics can be applied to several different fields, including space systems. Tactics are the adversary's goal. They are the reason for performing an action. Tactics represent the "why" of an ATT&CK technique[11]:

ID	Name	Description
TA0043	**Reconnaissance**	The adversary is trying to gather information they can use to plan future operations.
TA0042	**Resource Development**	The adversary is trying to establish resources they can use to support operations.
TA0001	**Initial Access**	The adversary is trying to get into your network.
TA0002	**Execution**	The adversary is trying to run malicious code.
TA0003	**Persistence**	The adversary is trying to maintain their foothold.
TA0004	**Privilege Escalation**	The adversary is trying to gain higher-level permissions.
TA0005	**Defense Evasion**	The adversary is trying to avoid being detected.
TA0006	**Credential Access**	The adversary is trying to steal account names and passwords.
TA0007	**Discovery**	The adversary is trying to figure out your environment.
TA0008	**Lateral Movement**	The adversary is trying to move through your environment.
TA0009	**Collection**	The adversary is trying to gather data of interest to their goal.
TA0011	**Command and Control**	The adversary is trying to communicate with compromised systems to control them.
TA0010	**Exfiltration**	The adversary is trying to steal data.
TA0040	**Impact**	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

The SPACE-SHIELD (Space Attacks and Countermeasures Engineering Shield) is an ATT&CK®-like knowledge-base framework for space systems. It is a collection of adversary tactics and techniques and a security tool applicable in the space environment to strengthen security. It is composed of threats that are relevant to space systems, leveraging the available and related literature. The matrix is tailored to the space segment and communication links, but it does not address specific types of mission, maintaining a broad and general point of view. The matrix contains information for the following platforms: generic, none, space segment, ground segment, and space-link communication.

11 https://attack.mitre.org/tactics/enterprise/

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
6 techniques	4 techniques	5 techniques	3 techniques	4 techniques	2 techniques	4 techniques
Active Scanning (RF/Optical) ↘ 4	Acquire or Build Infrastructure ↘ 4	Direct Attack to Space Communication Links ↘ 2	Modification of On Board Control Procedures modification	Backdoor Installation ↘ 5	Become Avionics Bus Master	Impair Defenses ↘ 1
Gather Victim Mission Information ↘ 3	Compromise Account ↘ 1	Ground Segment Compromise ↘ 2	Native API	Key Management Infrastructure Manipulation ↘ 2	Escape to Host ↘ 1	Indicator Removal on Host ↘ 1
Gather Victim Org Information ↘ 3	Compromise Infrastructure ↘ 2	Supply Chain Compromise ↘ 3	Payload Exploitation to Execute Commands	Pre-OS Boot ↘ 1		Masquerading
In orbit proximity intelligence ↘ 6	Develop/Obtain Capabilities ↘ 9	Trusted Relationship ↘ 3		Valid Credentials ↘ 3		Pre-Os Boot ↘ 1
Passive Interception (RF/Optical) ↘ 4		Valid Credentials ↘ 3				
Phishing for Information ↘ 2						

Full Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD) with sub-techniques:

↗ https://spaceshield.esa.int

TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0093 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
4 techniques	4 techniques	4 techniques	2 techniques	3 techniques	5 techniques	12 techniques
Adversary in the Middle ↘ 1	Key Management Policy Discovery	Compromise a Payload after compromising the main satellite platform	Adversary in the Middle ↘ 2	Protocol Tunnelling	Exfiltration Over Payload Channel	Data Manipulation ↘ 3
Brute Force ↘ 1	Spacecraft's Components Discovery	Compromise of another partition in Time and Space Partitioning OS or other types of satellite hypervisors	Data from link eavesdropping ↘ 3	Telecommand a Spacescraft ↘ 3	Exfiltration Over TM Channel	Ground Segment Jamming ↘ 1
Communication Link Sniffing ↘ 1	System Service Discovery	Compromise the satellite platform starting from a compromised payload		TT&C over ISL	Optical link modification	Loss of spacecraft telecommanding ↘ 1
Retrieve TT&C master/session keys ↘ 3	Trust Relationships Discovery	Lateral Movement via common Avionics Bus			RF modification	Permanent loss to telecommand satellite ↘ 1
					Side-channel exfiltration	Resource damage ↘ 7
						Resource Hijacking
						Saturation of Inter Satellite Links ↘ 1
						Saturation/ Exhaustion of Spacecraft Resources ↘ 5
						Service Stop ↘ 2
						Spacecraft Jamming ↘ 3
						Temporary loss to telecommand satellite ↘ 1
						Transmitted Data Manipulation

Full Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD) with sub-techniques:

↗ https://spaceshield.esa.int

Bundesverband der Deutschen
Luft- und Raumfahrtindustrie e. V.

www.bdli.de