# Designing Secure Space Systems

Zain A. H. Hammadeh*, Mohammad Hamad†, Andrzej Olchawa‡, Milenko Starcik‡,
Ricardo Fradique‡, Stefan Langhammer§, Manuel Hoffmann¶**,
Florian Göhler¶, Daniel Lüdtke*, Michael Felderer*‖, Sebastian Steinhorst†
*Institute of Software Technology, German Aerospace Center, Germany
†Department of Computer Engineering, Technical University of Munich, Germany
‡VisionSpace Technologies GmbH, Germany
§OHB Digital Connect GmbH, Germany
¶German Federal Office for Information Security, Germany
**Information Security Consulting Hoffmann, Germany
‖University of Cologne, Germany

***Abstract*—As space exploration advances and the commercialization and militarization of space technologies expand, ensuring the security of space assets has become a paramount concern. A key factor contributing to this challenge is the growing reliance on off-the-shelf hardware and software. While such components accelerate the adoption and commercial use of space technologies, they also introduce new vulnerabilities and broaden the attack surface. This paper highlights the critical importance of integrating cybersecurity concepts throughout the entire design lifecycle of space systems. It examines key dimensions of secure space system development, including secure engineering practices, comprehensive testing methodologies, strategies for cyber resiliency, and the role of standardization in fostering a consistent and robust security posture across the industry. By addressing these essential aspects, the paper underscores the need for a holistic, lifecycle-driven approach to safeguarding space systems against evolving cyber threats.**

***Index Terms*—cybersecurity, security, space.**

## I. Introduction

Much of the modern world's critical infrastructure depends on satellites and space systems, with the private sector's presence in the space market rapidly increasing [1]. These systems are prime targets for nation-state-level Advanced Persistent Threat (APT) actors, who are often backed by significant resources [2], [3]. However, despite advances in technology making space operations more accessible than ever, the focus tends to be on functionality and reliability, while cybersecurity efforts are often neglected and remain a secondary concern, typically treated as a byproduct of safety testing [4], [5]. Additionally, the long lifecycle of satellites makes it challenging and costly to implement cybersecurity upgrades, which, over time, significantly increases the potential attack surface [5], [6]. The lack of security awareness in space operations is being increasingly exposed through high-profile attacks [1]. In 2022, a widespread attack disabled modems communicating with Viasat Inc.'s KA-SAT satellite network, disrupting broadband satellite internet access over a large area [7]. Amid ongoing geopolitical tensions, satellite-based navigation systems have also been targeted in certain regions [8]. The extensive resources at the disposal of attackers are further highlighted by reports of them collecting signal intelligence directly from spacecraft [9] and infiltrating national satellite networks [10]. Many of these attacks exploit legacy hardware, software, and outdated protocols.

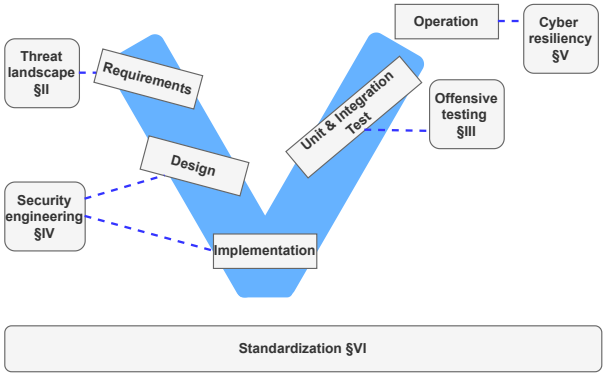


Fig. 1. V-model for space systems mapped to security concepts to emphasize the integration of cybersecurity in the space systems lifcycle

While efforts are being made to improve the security posture of space operations, research into the security of currently used space protocols, mission control software, and spacecraft on-board software frameworks reveals that security measures are still not consistently applied throughout the space mission lifecycle. Designing space systems follow the V-model. Figure 1 maps the V-model stages to the security aspects in a way inspired by ISO21434 [11]. This paper addresses the threat landscape of space systems and the efforts required to design more secure space systems. It highlights the need to integrate security into the software development lifecycle, emphasizing that security engineering and security testing should be incorporated alongside safety testing. Additionally, the paper underscores the importance of cyber resiliency, ensuring that space systems can continue to deliver their intended outcomes despite cyberattacks.

978-3-9826741-0-0/DATE25/© 2025 EDAA

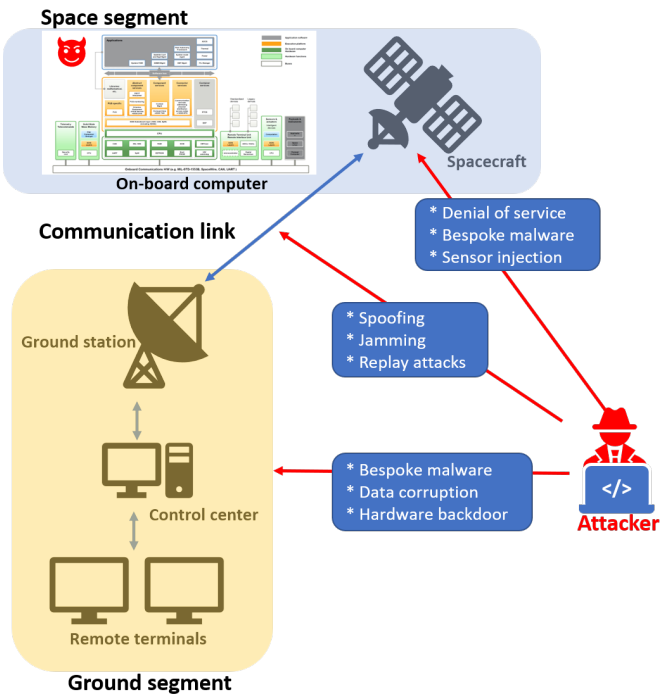


Fig. 2. Different space infrastructure segments may be subject to different security attacks

## II. Threat Landscape

One of the essential processes for ensuring a secure system is performing threat modeling. By leveraging threat modeling practices from other similar domains, such as automotive systems [12], [13] or cyber-physical systems [14], various effective approaches can be adopted for this process.

Threat modeling can be approached from different perspectives, such as analyzing assets, identifying potential attackers, and understanding attack vectors. In this section, we introduce the variety of threats that can target space systems. However, understanding the space threat landscape begins with identifying the three main segments of a typical space system, as illustrated in Fig. 2:

- **Ground segment:** The ground segment includes various critical components, such as ground stations, mission control centers, user terminals, data processing stations, and supporting physical infrastructure [1], [6]. Serving as the backbone for effectively controlling and monitoring satellites, it is one of the most impactful targets for potential attacks [1], [15].
- **Communication link:** The communication link refers to the Radio Frequency (RF) channels used to send and receive information between a spacecraft and the ground segment, encompassing all the protocols used [1], [6], [15].
- **Space segment:** This includes the spacecraft itself, all launch vehicles, payloads, on-board systems, communication systems, and all software required to operate the spacecraft [6], [15].

A wide range of adversarial threats exist to satellite operations, and multiple reports have previously attempted to categorize them based on target and type of attack [1], [6], [16], [17]. In short, an attack can target the ground segment, communication link, space segment, or a combination of these components [1], [6], [15]. Furthermore, attacks can be categorized based on their mode of operation into physical (kinetic and non-kinetic), electronic, and cyber threats [15], [16], [17].

### A. Physical attacks

Physical attacks can target both the ground and space segments and can be categorized based on their method:

*a) Kinetic attacks:* They aim to cause structural damage through direct high-energy impacts or close-distance detonations. These attacks can target both spacecraft and ground stations [15], [16]. They are further divided into the following categories [16]:

- *Direct-ascent Anti-Satellite (ASAT) weapons:* These are launched from Earth to strike a spacecraft in orbit.
- *Co-orbital ASAT weapons:* These are placed into orbit and then positioned closer to the target. They can be used to manipulate the target, including de-orbiting it.
- *Ground station attacks:* Direct attacks on a ground station can affect multiple space targets simultaneously.

Kinetic attacks cause significant damage, and if carried out in space, can also release debris that might affect other spacecraft in similar orbits [15], [16]. However, they are easily trackable and attributable. To date, no country has used this type of attack against another nation [16], although various countries have publicly demonstrated their capabilities against their own targets [15], [16].

*b) Non-Kinetic attacks:* They can affect a target without direct impact. These attacks can be grouped into the following types:

- *Physical compromise:* This includes compromising physical security measures, gaining unauthorized access to any part of the space mission infrastructure, and carrying out supply chain attacks [1].
- *High-powered lasers:* High-energy beams can be used to overheat or damage a spacecraft. These are difficult to pinpoint and can be launched from either ground or space locations, but they require a high degree of sophistication and resources [15], [16], [17].
- *Laser blinding:* This operates on the same principle as high-powered lasers, but with the intent to damage sensors and blind the spacecraft [16], [17].
- *High-altitude nuclear detonation:* A nuclear detonation at high altitudes can generate both an electromagnetic pulse (EMP) and a high-radiation environment, which can have indiscriminate effects in orbit [16].
- *High-powered microwave weapons:* These can be launched from both ground and space locations and can temporarily disrupt or permanently damage a spacecraft's electronic circuits [16].

### B. Electronic attacks

This class of attacks targets the electromagnetic spectrum used by space missions for communication [1], [15], [16]. More subtle than physical attacks, these can be difficult to distinguish from accidental interference. They can be grouped into the following types:

- *Spoofing:* This involves the capture, alteration, and/or retransmission of a signal in a way that misleads the receiver [15], [16]. It can include the injection of false information or commands to both the spacecraft and the ground station [15], [17].
- *Jamming:* This attack denies communication between the spacecraft and the ground station by injecting noise into the communication channel [16], [17]. While all satellites are susceptible to this type of attack, its effectiveness is limited by the line-of-sight requirement. This makes it easier to target the ground station receiver [15], and therefore more feasible to attribute.

### C. Cyber attacks

Cyber attacks target both the data and the systems used to transmit and process it [16] using malware infections, exploiting vulnerabilities in legacy communication protocols, and inserting false or corrupted data or commands in a system. While the objective of the attack may sometimes be clear, e.g., inserting ransomware [18], attribution is generally difficult. Although these attacks may not require significant resources, they demand extensive knowledge of the targeted systems. The potential impact can be severe, ranging from service disruptions to the complete loss of control over a satellite constellation [16], [17].

## III. Offensive Security Testing

While there is no universally accepted threat assessment method, common key elements can be identified, particularly in system characterization and threat identification [2], [5], [17], [19]. A widely used method for proactively identifying previously unknown threats is Offensive Security. This approach replicates the tactics used by malicious actors in real-world attacks to strengthen an organization's defense. Strategies under Offensive Security include:

- *Penetration testing (Pentesting):* Simulates a real-world cyberattack under specific constraints [20]. This may involve a combination of white-box, grey-box, and black-box approaches.
- *Red teaming:* A threat-focused penetration test emulating specific adversary tactics and capabilities [20].
- *Vulnerability assessment:* A systematic evaluation of an information system aimed at identifying, prioritizing, and remediating security vulnerabilities [20].

Regardless of the approach, these activities should not be treated as one-off exercises. They must be conducted periodically and following every major system release to ensure ongoing security.

As outlined in Section II, a space system comprises multiple components, most of which are driven by software. This applies to the space, ground, and user segments. Recently, security testing has conducted on several major space-related software applications. These efforts has led to publish more than twenty CVEs (see Table I[1]) and security advisories in [21]. Additionally, many more vulnerabilities are currently undergoing responsible disclosure, in collaboration with vendors to address or mitigate them. These findings highlight significant gaps in the cybersecurity culture during the development cycle of these applications, which could be addressed by integrating proper offensive security testing methods.

TABLE I
List of selected CVEs in Space Systems.

| CVE | Product | Score |
|---|---|---|
| CVE-2024-44912 | NASA Cryptolib | 7.5 HIGH |
| CVE-2024-44911 | NASA Cryptolib | 7.5 HIGH |
| CVE-2024-44910 | NASA Cryptolib | 7.5 HIGH |
| CVE-2024-35061 | NASA AIT-Core | 7.3 HIGH |
| CVE-2024-35060 | NASA | 7.5 HIGH |
| CVE-2024-35059 | NASA | 7.5 HIGH |
| CVE-2024-35058 | NASA | 7.5 HIGH |
| CVE-2024-35057 | NASA | 7.5 HIGH |
| CVE-2024-35056 | NASA | 9.8 CRITICAL |
| CVE-2023-47311 | YaMCS | 6.1 MEDIUM |
| CVE-2023-46471 | YaMCS | 5.4 MEDIUM |
| CVE-2023-46470 | YaMCS | 5.4 MEDIUM |
| CVE-2023-45885 | NASA Open MCT | 5.4 MEDIUM |
| CVE-2023-45884 | NASA Open MCT | 6.5 MEDIUM |
| CVE-2023-45282 | NASA Open MCT | 7.5 HIGH |
| CVE-2023-45281 | YaMCS | 6.1 MEDIUM |
| CVE-2023-45280 | YaMCS | 5.4 MEDIUM |
| CVE-2023-45279 | YaMCS | 5.4 MEDIUM |
| CVE-2023-45278 | NASA Open MCT | 9.1 CRITICAL |
| CVE-2023-45277 | YaMCS | 7.5 HIGH |

Typical security assessments are often limited to vulnerability scans, which are then transformed into the output of a formal security audit. While this is a useful starting point, it only identifies known vulnerabilities and is insufficient when defending against well-resourced, motivated attackers. Even existing vulnerabilities are often overlooked, with their priority downgraded due to operational assumptions.

This is where Offensive Security Testing outperforms traditional vulnerability scans. First, as noted, it identifies previously unknown vulnerabilities (commonly referred to as Zero-Days) [20]. Second, it contextualizes all vulnerabilities—both Zero-Day and N-Day—by attempting to exploit them in a representative environment. This often reveals that seemingly minor vulnerabilities, such as Cross-Site Scripting (XSS), can, when combined with other issues, create exploitation chains leading to far more significant and impactful outcomes.

The results of these tests go beyond raw statistics. They serve as valuable inputs for teams responsible for risk management within an organization.

### A. Importance of White-box Security Testing

Security testing can be black-box, grey-box, or white-box based testing. Experience shows that the white-box approach

[1]You find them on https://nvd.nist.gov/vuln/detail/"CVE number", e.g., https://nvd.nist.gov/vuln/detail/CVE-2024-44912

consistently yields the most significant and impactful results. Every vulnerability that have publicly disclosed in [21] was discovered in open-source software through white-box testing, where security experts had access to both the documentation and the source code.

In the space sector, most technologies are closed-source. However, given the sophistication of adversaries—often Advanced Persistent Threats (APTs)—obtaining closed-source software is among the least of their challenges. This reality highlights the critical importance of white-box testing.

White-box testing is not only the most efficient but also the most cost-effective method for defending against such advanced threats. It empowers ethical assessment teams working on behalf of space organizations to maintain an edge in the ongoing race against adversaries who often have far greater resources at their disposal.

## IV. Security Engineering

Experience shows that simply adding "security" to a system does not automatically improve its actual security. A recent example of this was the global IT outage caused by CrowdStrike's security software [22]. Hence, the integration of cybersecurity into the engineering lifecycle is imperative. This integration must enhance the security posture of space systems without introducing unnecessary complexity. To define how this can be accomplished, we identify four primary domains [2] essential for achieving security in the context of space system development:

- Security management: A management-driven process for identifying, implementing, and maintaining policies, procedures, and technologies to protect an organization's or system's assets from security risks.
- Security engineering: The discipline of designing and implementing secure systems and solutions to prevent or mitigate cyber attacks.
- Threat modelling:A systematic approach to identifying, assessing, and prioritizing potential threats and vulnerabilities to proactively mitigate risks.
- Security by testing: A strategy for ensuring system security through penetration testing, aimed at identifying and addressing vulnerabilities and weaknesses before they can be exploited by attackers.

To ensure resilience against cyber attacks, all of these domains are essential and are typically organized within the Security Management Process.

While the programmatic foundation is grounded in Information Security Management, the technical foundation relies on Security Engineering. Although existing organizational frameworks can often be adapted for space systems with appropriate modifications (refer to Section VI for an example), adapting technical foundations is not always straightforward—or even advisable. Without robust technical security measures, efforts in other domains become significantly more challenging.

[2]Others, for example security operations, cybersecurity education (of engineers, developers), governance have been skipped for brevity.

This is clearly illustrated by the frequent discovery of critical vulnerabilities in even the most security-focused systems, such as Fortinet [23], Palo Alto [24], and Cisco [25]. Such a situation would be unsustainable for space systems, where the typical security update cycles used in terrestrial environments (e.g., "patch days") are simply not feasible.

### A. Security Approach

A practical path toward achieving security begins with establishing a conceptual baseline through Security Management, based on frameworks such as ISO 27001 or BSI 200-2. This baseline should then be applied to existing systems or new system designs in a process we define as Security Engineering.

Threat modeling can play multiple roles: it can assess whether the resulting secure system design is adequate, help narrow down the scope of the problem early on, or analyze the attack chain to identify the optimal points where an attack can be stopped.

While the details of this process may vary, the core principles have been well established for a long time. However, we frequently observe breakdowns in the engineering phase. There are several reasons for this, and the key ones are:

- Existing legacy systems: Retrofitting security objectives onto legacy systems is often extremely difficult, if not impossible. A prime example is the Microsoft Windows operating system, which has evolved over decades with many legacy components that complicate modern security integration.
- Cost: Developing secure systems requires significant investments that implementers and customers may be reluctant to make. This can lead to shortcuts that compromise long-term security.
- Knowledge gaps: Security introduces additional layers of complexity in an already challenging field. Bridging these gaps at scale is far from trivial, especially when specialized expertise is required across various domains.

As outlined, these issues have a cascading effect on other security domains. Without solid technical foundations, security management and threat modeling become increasingly complex and burdensome, resulting in a downward spiral of unresolved security challenges. The outcome is what we commonly observe in today's enterprises: security efforts are driven by Security Management in combination with Security Testing. To simplify, vulnerabilities are identified and then patched as quickly as possible, often supplemented by the deployment of security appliances, regulations, and other temporary measures.

This approach is not inherently wrong. It prioritizes keeping large-scale legacy systems and enterprises operational under practical constraints. In an ideal world, legacy enterprise software would be replaced by systems designed with security in mind and firewalls would formally prove their security properties. In reality, this is unlikely to happen.

The goal is to avoid falling into this reactive cycle when developing space systems. Unlike traditional IT environments,

the legacy burden in space systems is smaller making it comparatively easier to establish solid security foundations from the start. When considering *New Space*, the legacy burden may even be considerably smaller. Moreover, adopting quick-fix solutions such as monthly security patches, antivirus software, and other stopgap measures is fundamentally unsuitable for space systems — not just for security reasons, but also due to the significant financial implications.

By focusing on proactive and integrated security from the outset, space system development can avoid the pitfalls of patch-driven security strategies and deliver more secure, cost-effective solutions over the system's lifecycle.

### *B. Security Approach for the Space Domain*

To understand how security can be achieved in a space project, we can draw insights from safety engineering. In safety-critical domains, such as aviation, every systems engineer is familiar with the principles of designing systems to ensure they are safe. Safety-critical components in software and hardware development receive special attention and are subjected to rigorous scrutiny.

Security presents an even greater challenge due to the adversarial nature of cyber threats, which introduces an additional layer of complexity. Nevertheless, the same core principle applies: engineers, developers, and other implementers must understand and incorporate security considerations relevant to their fields. Conversely, security experts must develop a solid understanding of the systems they aim to protect, including the underlying development principles and design constraints.

Once the knowledge gap is sufficiently reduced, a standardized approach to security system design must be selected. This approach should leverage established frameworks and best practices, such as:

- ISO 27001: A high-level security management framework that naturally incorporates ISO 27005 for risk analysis.
- The BSI security guidelines for space series (explained in Section VI), which provide domain-specific guidance for space systems.
- The French EBIOS method: A security management framework with a strong emphasis on risk assessment through threat modeling.

Other security frameworks, e.g., Microsoft SDL [26], OWASP SAMM [27], NIST Cybersecurity Framework [28], etc., and they can generally be distilled into three key steps:

- Definition of foundational aspects and principles: This involves identifying the key assets and potential threats to the system.
- Risk identification: Risks should be determined based on system attributes, potential attack vectors, or threat models.
- Definition and implementation of mitigations: Once risks are identified, appropriate mitigations must be defined and their implementation verified.

The definition of foundational security aspects can typically be handled by security experts in collaboration with project managers. This step is well understood and generally yields reliable outcomes.

Identifying attack vectors can be accomplished using established standards and guidelines, such as the aforementioned BSI series, or by employing threat modeling techniques like STRIDE [29]. While this process often succeeds at a high level, challenges arise when it comes to lower-level components in the product hierarchy. At this point, the analysis may either:

- Remain too high-level, failing to provide actionable technical input, or
- Become overly detailed and unmanageable, resulting in analysis paralysis.

This is where deeper security engineering becomes necessary. The solution lies in integrating security into the broader engineering process rather than treating it as a standalone activity. By doing so, meaningful and manageable security measures can be identified and implemented across all levels of the system.

### *C. Secure Engineering for Space*

At this stage of the security process, Security Systems Engineering, as we call it, should deliver a detailed analysis of where the true security challenges of the system lie and how they can be addressed within the system's design constraints. A high-level assessment such as, "*An attacker could hack the satellite through the TC (telecommand) link,*" offers little actionable value. Instead, the assessment needs to be more specific, such as: "*An attacker with control of system X in the Mission Operations Center (MOC) could send harmful telecommand messages to component Y, potentially exploiting a software vulnerability.*" This should be followed by an in-depth investigation into how the attacker might gain control of system X, how the harmful telecommand messages could function, how the software for component Y was developed, and how vulnerabilities in that software stack could emerge. For instance, the likelihood of such a vulnerability could vary significantly depending on whether the software was developed in traditional C or a more secure language like Ada. Factors such as adherence to coding standards, the software architecture, and even the development methodology must be considered during the assessment.

This detailed approach has been formalized by MITRE in the MITRE ATT&CK framework [30], though competing frameworks such as the Cyber Kill Chain also exist. Notably, frameworks like SPARTA and ESA SpaceShield have already adapted the MITRE ATT&CK framework for space systems, offering valuable insights into how to implement this process effectively.

The goal of the overall exercise is to define two key aspects:

*a) Risk of the attack:* The objective here is to assess whether a given attack scenario can cause a significant risk to justify implementing specific security mitigations. This process of calculating the risk involves assessing the likelihood of the attack as well as the expected impact it may have. Performing this assessment poses a significant challenge and de-

mands extensive collaboration among security experts, system designers, and implementers. Additionally, it requires a broad range of expertise, including skills in exploit development and hardware security.

While this approach introduces substantial overhead and increases costs during system development, the investment is expected to pay off over the system's lifecycle. By tailoring the system and security controls to realistic scenarios, organizations can achieve reduced development costs, lower long-term expenses in security management, and, most importantly, a more secure system with all the associated benefits.

*b) Mitigation:* The aim is to define security mitigations as close to the source of the risk as possible, while minimizing their impact on the overall system design. Tailoring security controls—whether they are specific security measures or detailed requirements—should be treated as a multi-disciplinary engineering task. Security risks must be mitigated in a way that aligns with the overall system design and fits within the defined system parameters. In essence, security risk mitigation should be integrated as a standard part of the system design process and balanced alongside other engineering considerations, such as thermal and mechanical design. Just as these domains require trade-offs to achieve an optimal solution, so too does cybersecurity engineering.

### D. Critical Recap

Using standardized solutions for known risks can often be highly effective, and this approach should be applied wherever feasible. Hence, not every security risk needs to be analyzed in detail, nor does every security measure need to be custom-tailored to a specific system. For example, deploying a Linux-based system on a satellite introduces several well-known attack vectors, posing significant security risks to the space system. However, it also enables the use of established security solutions such as SELinux or immutable systems to mitigate potential attacks. Depending on the overall system design, critical assets, and mission goals, this trade-off may be justified.

Similarly, organizations like ESA are exploring the application of IP-based security solutions for space communications. While this approach comes with notable drawbacks, leveraging the established security principles of secure internet communication could offer substantial benefits for various space applications. Even with this standard-driven approach, security engineering will still be essential to fine-tune the provided solutions and address design considerations. As a counterintuitive sidenote, a security approach based on standardized solutions can not just be effective for low-cost systems but may be a necessity for high-security systems. In low-cost systems, the trade-offs are generally acceptable, while in high-security systems, detailed threat modeling may become impractical due to its complexity. In such cases, security risks can be mitigated using approved, pre-certified solutions, such as components with established security certifications.

### E. Validation, Verification and Security Testing

In a well-specified space system, the most effective way to validate the security design may be to define all security mitigations as requirements and verify them as part of the standard engineering process. However, this approach only confirms the design team's assumptions regarding the system's security posture. Therefore, it is crucial to involve third-party entities that can simulate the adversarial behavior of cyber attackers to independently validate the system's security. Security testing [31], as detailed in Section III, is not a one-time task. Specialized procedures, such as fuzzing interfaces, conducting security code reviews for critical software, or reviewing cryptographic algorithm implementations, often require highly specialized expertise. Section III emphasizes the white-box penetration testing approach, which leverages existing knowledge of the system. This method effectively complements the security design by helping to verify whether the assumptions made during scenario modeling and the implemented mitigations are valid. However, only black-box testing, where the tester has little to no prior knowledge of the system, truly compels testers to think creatively and challenge the core security assumptions. Given the inherent risks and high costs of black-box testing, it is unlikely to see widespread use in space system development, though it may be beneficial for specific subsystems or components.

The test results must be carefully analyzed to determine whether they represent isolated issues requiring targeted fixes or indicate deeper, systemic security flaws in the developed system.

## V. Cyber Resiliency

Securing the link between the ground segment and the satellite is essential to protect the satellite from cyber attacks. Solutions including end-to-end encryption can help avoid attacks like spoofing and reply attacks. However, developers of on-board software should not assume that a satellite environment is secure, especially in an era where a satellite will serve as an execution service for 3rd party software, which can be malicious [32]. Also, commercial Off-the-Shelf (COTS) hardware [33] is widely used in space systems due to its low cost. Fig. 3 illustrates an example of using the COTS Xilinix Zynq board with ARM A9 processors in the ScOSA project [34]. COTS may have vulnerabilities including malicious hardware which make them a backdoor for advanced cyber attacks. Virtualization solutions using, e.g., Sandboxing [35] or Hypervisors [36], can provide guarantees on isolating applications. However, these solutions themselves can be a target for some cyber attacks [37]. The third motivation for cyber resiliency in space systems is the Denial of Service (DoS) attacks, which are less complicated than other attacks and harder to foresee. Mainly, the sensor-disturbing DoS attacks [38] can have a deep impact on the software stack [39].

Hence, efficient intrusion detection systems (IDS) are essential for monitoring network traffic and system behavior to identify malicious activities in real-time [40]. Additionally, an effective intrusion response mechanism must be in place to

ensure that the satellite can continue functioning even under attack. This requires a fail-operational mode that guarantees essential systems remain operational while isolating and neutralizing compromised components. Given the constraints on computational resources in space systems, these security solutions must be optimized for low-latency response and minimal resource consumption, all while ensuring high reliability and resilience against evolving cyber threats.

Intrusion Detection Systems (IDSs) can be categorized based on the source of collected data and the installation location of the IDS. The main types include:

- Host-based IDS (HIDS): Monitors data collected by the operating system of a single host to detect suspicious activities. This data may include metrics such as memory usage, execution times of various software components running on the host, system calls, and other relevant information.
- Network-based IDS (NIDS): Monitors network traffic to identify potential attacks. It must be deployed at a strategic point in the network where it can observe all traffic exchanged between network hosts.
- Hybrid IDS: Combines both host-based and network-based approaches to analyze data across multiple interconnected hosts in a networked environment. One implementation of this approach is the Distributed Intrusion Detection System (DIDS), which integrates HIDS and NIDS for comprehensive threat detection.

There are two primary methods used in designing IDSs:

- Knowledge-based Intrusion Detection: Also known as the signature-based or misuse-based method, this approach relies on predefined rules derived from accumulated knowledge of known attacks. It compares observed events against these rules to identify potential security incidents. The key advantage of this method is its high accuracy in detecting known attacks, with a very low false positive rate. However, its primary limitation is the inability to effectively detect zero-day attacks, which are previously unknown threats.
- Behavioral-based Intrusion Detection: Also referred to as the anomaly-based method [41], this approach detects potential attacks by identifying deviations from normal behavior. It uses an offline-defined model representing the system's typical behavior, and any significant inconsistencies are flagged as possible threats. Unlike knowledge-based systems, behavioral-based methods excel at detecting unknown vulnerabilities and zero-day attacks. However, their major drawback is a higher false positive rate, meaning that legitimate activities may occasionally be incorrectly flagged as malicious.

Detecting an intrusion using an IDS is not sufficient to guarantee the safety and security of a system; appropriate responses must be implemented to counter the detected attack. An Intrusion Response System (IRS) is designed to generate these responses, manage the identified malicious or suspicious actions, and minimize potential damage to the system.

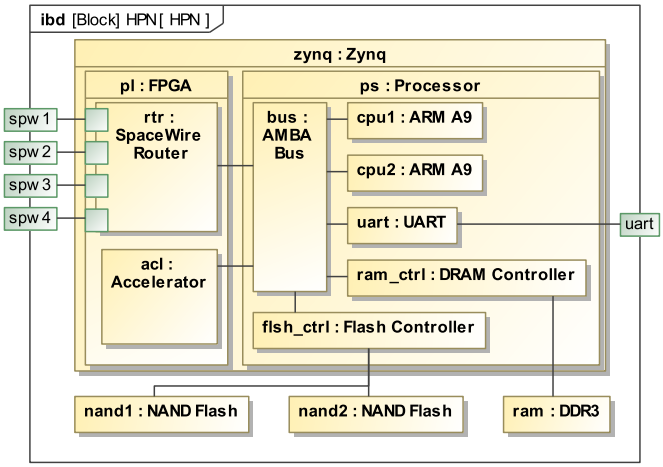


Fig. 3. COTS CPU in a space system - ScOSA project [34].

Bringing the system into a safe-mode state and sending a telemetry to the ground station can be the most straightforward solution. However, more autonomous decision can be taken as response to the detected intrusion. Such a respond should be as generic as possible to not overload the system with many different responses. Reconfiguration-based responses, which is not uncommon in space systems as a fault-tolerance mitigation [32], can be used as an intrusion response system, e.g., as in [42].

## VI. Standardization of Cybersecurity in Space

Planning security for every aspect of a space mission presents a significant challenge across the industry. This is particularly true for new space companies with little to no cybersecurity experience, but it also affects governmental and academic missions [43]. The application of standards in space projects poses numerous challenges, particularly regarding implementation:

- Lack of easy-to-use, space-specific standards.
- Lessons from traditional IT show that without standardized security levels, comparing and enforcing security measures becomes difficult.
- In the absence of clear standards, critical security aspects are often overlooked or ignored.

Existing standards were primarily developed for general IT environments and not tailored to the unique requirements of space systems [43]. As a result, companies have struggled to adapt these standards to their space projects, which traditionally did not prioritize information and cybersecurity. Introducing and adapting standards for space-specific requirements can help improve system security and ensure competitiveness, especially as regulatory requirements evolve.

Nevertheless, a universal set of security standards addressing information security in space is still lacking. Current measures do not sufficiently cover threats specific to space environments [43]. This gap particularly impacts small institutions, start-ups, and research organizations, though established

industry players also face difficulties [43]. Many companies feel overwhelmed by the complexity and effort required for proper implementation.

To enhance the current state of cybersecurity in space and make its implementation more practical, the German Federal Office for Information Security (BSI) has established an expert group focused on space cybersecurity. This group operates under the Alliance for Cyber Security and brings together experts from government institutions, industry, and academia to collaborate on improving information security for space systems. The expert group focuses on several key areas, including the identification of security requirements, monitoring international developments related to norms and standards, assessing the impact of government regulations, and addressing emerging threats linked to new technologies. Their goal is to enhance information security in both space systems and supporting infrastructures.

In a collaborative effort, and leveraging existing standards, the expert group has developed a series of documents aimed at mitigating cyber threats in both space and ground segments. These guidelines are tailored to the various lifecycle phases of a space mission, ensuring they are adaptable to the specific scope and complexity of different projects. Additionally, the group is responsible for identifying new technologies and regulatory changes that could influence cybersecurity in space. The expert group carefully considers both national and international advancements in information security and integrates these developments into its space security guidelines. Among its many tasks, the group produces documents that facilitate the application of well-established security frameworks, such as ISO 27001 and BSI-Grundschutz (English: basic protection), to space missions. These documents serve as practical tools to help ensure that security standards are accessible and applicable for both industry and government stakeholders. To date, the expert group has published three key documents addressing cybersecurity in the space and ground segments, with additional publications planned for the future.

### A. BSI Profiles for Space

The objective is to offer a comprehensive portfolio of IT-basic-protection profiles as reference scenarios for various fields of application. By using these IT-Grundschutz profiles, users can significantly reduce the time and effort required to develop tailored security solutions by adapting the provided security considerations to their specific operational context.

An IT-Grundschutz profile documents the key steps of a security process for a defined area of application, including:

- Defining the area of application.
- Conducting a generalized structural analysis, determining protection requirements, and creating models for the specified area.
- Selecting and customizing IT-Grundschutz modules to be implemented.
- Describing specific security requirements and corresponding measures.

All documents developed by the expert group cover the entire lifecycle of space systems, which generally includes: Conception and Design, Production, Testing, Transport, Commissioning, and Decommissioning.

Adjustments may be necessary depending on the scope or specific characteristics of individual subsegments

*1) Profile for Space Infrastructures:* The *IT Basic Protection Profile for Space Infrastructures — Minimum Protection for Satellites Throughout the Entire Lifecycle*[3] — targets those responsible for information security within space facilities, specifically in the areas of production and operation.

Decision-makers and project managers hold the responsibility for information security and delegate the implementation to the relevant departments, following a top-down approach.

The primary objective of this document is to assist users in implementing information security while adapting it to the satellite-specific requirements of the project scope. The technical scope of the document focuses on the satellite platform.

Based on the BSI IT-Grundschutz approach, this document provides a generic, satellite-specific structural analysis, which can be used as a template for tailoring the security measures to the respective project. The project can use this structural analysis to perform basic protection modeling, capturing relevant components. This initial analysis has already been completed in the profile and is intended to guide users in customizing it to meet the needs of their specific project. Additional satellite-specific details are addressed and described in the concluding chapters.

*2) Profile for the Ground Segment:* The profile *IT-Grundschutz Profile for the Ground Segment of Satellites—Minimum Protection for the Ground Segment Throughout the Entire Lifecycle*[4]—serves as a guide for users in creating a structured information security concept for ground segments. Based on the basic protection methodology, the aim is to meet the protection objectives of confidentiality, availability, and integrity.

The ground segment encompasses the overall system, which includes the operational ground segment (Mission Control Centre - MCC), the Satellite Control Centre (SCC), and the Telemetry, Tracking, and Command (TTC) ground stations. Those responsible for information security in these areas can use this document to help implement and continuously improve their information security system.

Using an exemplary ground segment, the document presents the creation of a security concept throughout the entire lifecycle, providing measures derived as examples. It outlines the identified lifecycle phases for the ground segment, including:

- A list of relevant target objects (applications, IT systems, and buildings/premises) that need to be protected.

[3]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf

[4]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Systems_GroundSegment.pdf

- An assignment of corresponding IT baseline protection modules with requirements and implementation instructions.
- General requirements that go beyond basic protection due to space-specific processes.

*3) Technical Guideline Space:* The *Technical Guideline BSI TR-03184 Information Security for Space Systems - Part 1: Space Segment*[5] is a derivation of the profile for space infrastructures. It describes security for the platform based on the bottom-up principle.

Relevant applications are mapped to the identified business processes. These applications are assessed for potential risks, and management measures must be assigned to address the recognized risks. The management measures outline the actions that must be taken; however, the specific design of these measures must be defined by the project team or the individual responsible for the project.

The document provides a comprehensive, customizable table of applications, associated hazards, mitigation measures, and implementation guidelines.

The documents developed by the expert group assist industry stakeholders and users in implementing robust information security measures. An industry-specific minimum standard also ensures fair competition while maintaining a strong security posture, preventing cost considerations from compromising security.

The expert group is actively working in various areas to create and regularly update these documents. In the future, it will offer multiple levels of certification options for space products.

These efforts will enable industry players and system operators to implement comprehensive information security measures and provide their products with a recognized seal of quality. All of these initiatives will be harmonized and aligned with both current and future national and international regulations.

## VII. Open challenges

In this section, we summarize some of the open challenges that need to be addressed to ensure secure design of space systems.

- **Comprehensive threat analysis and risk assessment methodology:** Developing a standardized and widely adopted Threat Analysis and Risk Assessment methodology for space systems remains an open challenge. This methodology should comprehensively identify and assess realistic and critical threats early in the system development lifecycle. It must provide actionable insights to prioritize mitigation strategies while avoiding an overemphasis on unrealistic attack scenarios lacking practical entry points.
- **Continuous testing:** In addition to safety and functional testing, cybersecurity testing is essential and must always be considered. However, in complex and safety-critical systems, such as space systems, cybersecurity testing must be applied at the component level, the system level, and the system-of-systems level. Achieving this requires well-defined tools, frameworks, and methodologies that are specifically designed for these purposes.
- **Multi-layer defense mechanisms**: Recognize that every part of a space mission can face risks, no matter where it is. It is important to create a strong security plan with multiple layers of defense. Each layer should be designed to block or slow down threats and reduce the risk of further harm at different stages of the system's life cycle. These layers could include testing and threat modeling during the design and implementation phases, firewalls and intrusion detection systems (IDS) during operation, and recovery mechanisms to respond to and recover from attacks.
- **Cybersecurity acceptance:** All stakeholders in space projects must recognize cybersecurity as an integral factor, just like thermal, radiation, or safety factors. Integrating cybersecurity will increase costs, require more resources, and might impact system performance. These impacts need to be addressed from the very beginning of the project.
- **Future technology consideration:** Projects should plan for future technologies and the threats they might bring. It's important to study new technologies to understand both their benefits and risks. For example, using post-quantum cryptography [44] can help protect systems from the risks of quantum computing, ensuring they stay secure as technology advances.
- **Advancing the Cybersecurity Operations Center:** Although ESA is making progress toward establishing a Cyber Safety and Security Operations Center (C-SOC), the center must incorporate advanced technologies to enhance its capabilities. Automation and faster processing of collected alerts are essential to improve situational awareness of ongoing attacks and reduce response and recovery times. Additionally, effective methods and mechanisms for privacy-aware sharing threat intelligence between different C-SOCs are needed.

## VIII. Conclusion

The paper has provided a comprehensive overview on secure engineering, testing methodologies, cyber resiliency strategies, and the role of standardization in designing secure space systems. Each of these pillars plays a crucial role in ensuring that space assets can withstand the ever-growing array of threats in the cyber domain. Safeguarding space systems is a multi-faceted challenge that requires a comprehensive and collaborative approach. Addressing cybersecurity at every phase of the lifecycle is imperative, from conceptual design to decommissioning.

[5]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf

## REFERENCES


[1] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in new space," *International Journal of Information Security*, vol. 30, pp. 287–311.

[2] L. Vessels, K. Heffner, and D. Johnson, "Cybersecurity risk assessment for space systems," in *2019 IEEE Space Computing Conference (SCC)*, pp. 11–19, IEEE.

[3] P. Martinez, "Challenges for ensuring the security, safety and sustainability of outer space activities," *Journal of Space Safety Engineering*, vol. 6, no. 2, pp. 65–68.

[4] J. G. Oakley, *Cybersecurity for Space*. Apress L. P., 2020.

[5] G. Falco, "Cybersecurity principles for space systems," *Journal of Aerospace Information Systems*, vol. 16, no. 2, pp. 61–70.

[6] S. K. Khan, N. Shiwakoti, A. Diro, A. Molla, I. Gondal, and M. Warren, "Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions," *International Journal of Critical Infrastructure Protection*, vol. 47, p. 100724.

[7] N. Boschetti, N. Gordon, and G. Falco, "Space cybersecurity lessons learned from the viasat cyberattack," in *AIAA Ascend*, 2022.

[8] European Union Aviation Safety Agency, "2022-02r3 : Global navigation satellite system outage and alterations leading to communication / navigation / surveillance degradation." https://ad.easa.europa.eu/ad/2022-02R3. Accessed: 2024-12-20.

[9] M. Langbroek, "The flyby of usa 326 by kosmos 2558 on august 4: a post-analysis." https://sattrackcam.blogspot.com/2022/08/the-flyby-of-usa-326-by-kosmos-2558-on.html. Accessed: 2024-12-20.

[10] C. Vasquez, "Cisa researchers: Russia's fancy bear infiltrated us satellite network." https://cyberscoop.com/apt28-fancy-bear-satellite/. Accessed: 2024-12-20.

[11] International Organization for Standardization, "ISO21434: Road vehicles – cybersecurity engineering," 2021.

[12] M. Hamad and V. Prevelakis, "SAVTA: A hybrid vehicular threat model: Overview and case study," *Information*, vol. 11, no. 5, p. 273, 2020.

[13] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "A review of threat analysis and risk assessment methods in the automotive context," in *Computer Safety, Reliability, and Security: 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 21-23, 2016, Proceedings 35*, pp. 130–141, Springer, 2016.

[14] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, IEEE, 2017.

[15] M. B. Garino and M. J. Gibson, "Space system threats," in *AU-18 Space Primer*, p. 273–281, 2009.

[16] K. Bingen, K. Johnson, M. Young, and J. Raymond, "Space threat assessment 2023," Apr. 2023. Online: https://www.csis.org/analysis/space-threat-assessment-2023.

[17] Consultative Committee for Space Data Systems (CCSDS) , "Security threats against space missions," 2022. INFORMATIONAL REPORT. Online: https://public.ccsds.org/Pubs/350x1g3.pdf.

[18] G. Falco, R. Thummala, and A. Kubadia, "WannaFly: An approach to satellite ransomware," in *2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, pp. 84–93, 2023.

[19] J. Vivero, "Space missions cybersecurity modelling," in *31st AIAA International Communications Satellite Systems Conference*, American Institute of Aeronautics and Astronautics, 2013.

[20] Committee on National Security Systems (CNSS), "Committee on National Security Systems (CNSS) Glossary," 2022. Online: https://www.cnss.gov.

[21] VisionSpace, "List of publicly disclosed vulnerabilities for space systems." https://visionspace.com/category/cyber. Accessed: 2024-12-20.

[22] S. R. Mugu, B. Zhang, H. Kolla, S. R. A. Balaji, and P. Ranganathan, "Lessons from the crowdstrike incident: Assessing endpoint security vulnerabilities and implications," in *2024 Cyber Awareness and Research Symposium (CARS)*, pp. 1–10, 2024.

[23] "CVE-2024-23113.." Available from MITRE, CVE-ID CVE-2024-23113., Nov. 11 2024.

[24] "CVE-2024-9463.." Available from MITRE, CVE-ID CVE-2024-9463., Oct. 10 2024.

[25] "CVE-2024-20432.." Available from MITRE, CVE-ID CVE-2024-20432., Feb. 2 2024.

[26] "Microsoft Security Development Lifecycle (SDL)." https://learn.microsoft.com/en-us/compliance/assurance/assurance-microsoft-security-development-lifecycle. Accessed: 2025-01-16.

[27] "OWASP Software Assurance Maturity Model (SAMM)." https://owasp.org/www-project-samm/. Accessed: 2025-01-16.

[28] "National Institute of Standard and Technology (NIST) - Cybersecurity Framework." https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework. Accessed: 2025-01-16.

[29] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, 2017.

[30] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK risk using a cyber-security culture framework," *Sensors*, vol. 21, no. 9, 2021.

[31] M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu, and A. Pretschner, "Chapter one - security testing: A survey," vol. 101 of *Advances in Computers*, pp. 1–51, Elsevier, 2016.

[32] A. Lund, Z. A. H. Hammadeh, P. Kenny, V. Vishav, A. Kovalov, H. Watolla, A. Gerndt, and D. Lüdtke, "ScOSA system software: the reliable and scalable middleware for a heterogeneous and distributed on-board computer architecture," *CEAS Space Journal*, May 2021.

[33] N. Yadav, F. Vollmer, A.-R. Sadeghi, G. Smaragdakis, and A. Voulimeneas, "Orbital shield: Rethinking satellite security in the commercial off-the-shelf era," in *2024 Security for Space Systems (3S)*, pp. 1–11, 2024.

[34] D. Lüdtke, T. Firchau, C. G. Cortes, A. Lund, A. M. Nepal, M. M. Elbarrawy, Z. H. Hammadeh, J.-G. Meß, P. Kenny, F. Brömer, M. Mirzaagha, G. Saleip, H. Kirstein, C. Kirchhefer, and A. Gerndt, "ScOSA on the way to orbit: Reconfigurable high-performance computing for spacecraft," in *2023 IEEE Space Computing Conference (SCC)*, pp. 34–44, 2023.

[35] G. Marra, U. Planta, P. Wüstenberg, and A. Abbasi, "On the feasibility of cubesats application sandboxing for space missions," in *Second Workshop on the Security of Space and Satellite Systems (SpaceSec)*, 2024.

[36] C. Wulf, M. Willig, and D. Göhringer, "A survey on hypervisor-based virtualization of embedded reconfigurable systems," in *2021 31st International Conference on Field-Programmable Logic and Applications (FPL)*, pp. 249–256, 2021.

[37] G. Pék, L. Buttyán, and B. Bencsáth, "A survey of security issues in hardware virtualization," *ACM Comput. Surv.*, vol. 45, July 2013.

[38] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *27th USENIX Security Symposium (USENIX Security 18)*, (Baltimore, MD), pp. 1545–1562, USENIX Association, Aug. 2018.

[39] A. Roberts, M. Malayjerdi, M. Bellone, R. Sell, O. Maennel, M. Hamad, and S. Steinhorst, " Analysis of Autonomous Driving Software to Low-Level Sensor Cyber Attacks ," in *2025 IEEE/ACM 20th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, (Ottawa, Canada), IEEE Computer Society, April 2025. to appear.

[40] M. Hamad, A. Finkenzeller, M. Kühr, A. Roberts, O. Maennel, V. Prevelakis, and S. Steinhorst, "REACT: Autonomous intrusion response system for intelligent vehicles," *Comput. Secur.*, vol. 145, Nov. 2024.

[41] M. Hamad, Z. A. H. Hammadeh, S. Saidi, V. Prevelakis, and R. Ernst, "Prediction of abnormal temporal behavior in real-time systems," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, SAC '18, (New York, NY, USA), p. 359–367, Association for Computing Machinery, 2018.

[42] Z. A. H. Hammadeh, M. Hasan, and M. Hamad, "Securing real-time systems using schedule reconfiguration," in *2024 IEEE 27th International Symposium on Real-Time Distributed Computing (ISORC)*, pp. 1–10, 2024.

[43] G. Falco, "The vacuum of space cyber security," in *2018 AIAA SPACE and Astronautics Forum and Exposition*, 2018.

[44] J. Jayakanth, V. Rajasekar, and V. Sarveshwaran, "Post-quantum cryptographic approach for cyberspace security," in *Cyber Space and Outer Space Security*, pp. 217–237, River Publishers, 2024.