Modular approach for ensuring smallsat cybersecurity

Gerling, Alexandra
IT Security Expert
TUV Informationstechnik GmbH
Essen, Germany
a.gerling@tuvit.de

Sarah Lehnhausen
IT Security Expert
TUV Informationstechnik GmbH
Essen, Germany
s.lehnhausen@tuvit.de

Matthias Petsch
Teamlead & IT Security Expert
TUV Informationstechnik GmbH
Essen, Germany
m.petsch@tuvit.de

***Abstract*— Small satellites largely rely on rapid development cycles and distributed ground segment services while using commercial off-the-shelf (COTS) components, which collectively introduce significant cybersecurity challenges. Constrained budgets, short mission timelines and limited onboard resources often prevent the adoption of security-by-design approaches traditionally used in larger space missions. Additionally, the use of COTS and standardized protocols makes the attack paths easier approachable than they have been thus increasing the need for secured satellites. This paper proposes a modular approach for strengthening small satellite cybersecurity that systematically addresses these constraints.**

The proposed methodology decomposes a typical small satellite system into functional and technical modules across space and communication segments, while the ground segment is treated as a "bought service". The modules are analyzed to identify security-critical components, such as onboard data handling units, communication links and command interfaces. For each identified module, potential threat vectors and corresponding security measures are derived, taking into account resource limitations and operational realities specific to small satellite missions providing an overview of security measures to protect the most critical components.

Furthermore, the paper analyzes a set of standards and guidelines, creating an understanding of availability, applicability and adequacy of structured methods for security assurance. This enables incremental improvements and informed trade-offs during system design, allowing mission designers to make educated decisions about their cybersecurity needs and options based on the mission-specific criticality of different modules. Particular emphasis is placed on the reuse of existing component certifications and standards where applicable, highlighting how modular certification can reduce development effort while increasing overall mission security.

By focusing on the most security-critical subsystems and adopting a modular, certification-aware framework, this approach supports practical and cost-effective cybersecurity implementation for small satellite missions.

Keywords—cybersecurity, security assurance, evaluation, certification

I. INTRODUCTION

The increase of small satellite (smallsat) missions has revolutionized access to space, enabling rapid deployment of diverse missions at a fraction of the cost and complexity associated with traditional, large-scale spacecraft. Smallsats leverage agile development cycles, distributed ground segment services, and commercial off-the-shelf (COTS) components to achieve operational flexibility and cost efficiency. However, these same characteristics introduce significant cybersecurity challenges. The reliance on COTS hardware and standardized communication protocols increases the attack surface, making smallsat systems more susceptible to cyber threats than their larger, custom-built counterparts [1], [4]–[6].

Compounding these risks are the inherent constraints of smallsat missions: limited budgets, compressed timelines, and restricted onboard resources often preclude the adoption of comprehensive security-by-design practices. As a result, smallsat developers must navigate a complex landscape where security requirements are frequently overshadowed by operational and financial imperatives. The growing use of standardized interfaces and third-party ground segment services further amplifies the need for robust, mission-tailored cybersecurity solutions [1], [7].

Despite the critical importance of cybersecurity in space systems, smallsat missions often lack structured methodologies for identifying and protecting their most vulnerable components. Existing standards and guidelines, while valuable, are not always directly applicable or sufficiently granular for the unique context of smallsat operations [1], [2], [7]. This gap underscores the necessity for practical, scalable approaches that can systematically address the security needs of smallsat missions without imposing prohibitive costs or development burdens.

In response to these challenges, this paper proposes a modular approach to smallsat cybersecurity. By decomposing the system into functional and technical modules across space and communication segments—and treating the ground segment as a "bought service"—the methodology enables targeted analysis of security-critical components such as onboard data handling units, communication links, and command interfaces. Potential threat vectors and corresponding security measures are identified, taking into account the resource limitations and operational realities specific to smallsat missions [1], [2], [6], [7].

Furthermore, the paper examines the landscape of existing standards and certification schemes, evaluating their availability, applicability, and adequacy for smallsat cybersecurity assurance [2], [7], [9], [11], [13], [14]. This analysis supports incremental improvements and informed trade-offs during system design, empowering mission designers to make educated decisions based on the mission-specific criticality of different modules. Emphasis is placed on the reuse of certified components and established standards, demonstrating how modular certification can streamline development while enhancing overall mission security [2], [7], [11], [13], [14].

By focusing on the most security-critical subsystems and adopting a modular, certification-aware framework, the proposed approach offers a practical and cost-effective

pathway to strengthening cybersecurity in small satellite missions.

II. Components Model

To identify the critical components from a cybersecurity perspective, we need to analyse how a satellite is constructed. The first step is to break the system down into subsystems and modules which are made from components. The decomposition can be seen in Figure 1.

A. Module Identification

The model divides the satellite system into its primary components: payload and platform. Given that the payload is highly variable and mission-specific, the analysis centers on the platform, which is further subdivided. The decomposition prioritizes components relevant to cybersecurity, determining the level of detail applied to each part. Consequently, certain elements are examined in greater depth than others. The complete hierarchical structure is illustrated in the following figure.

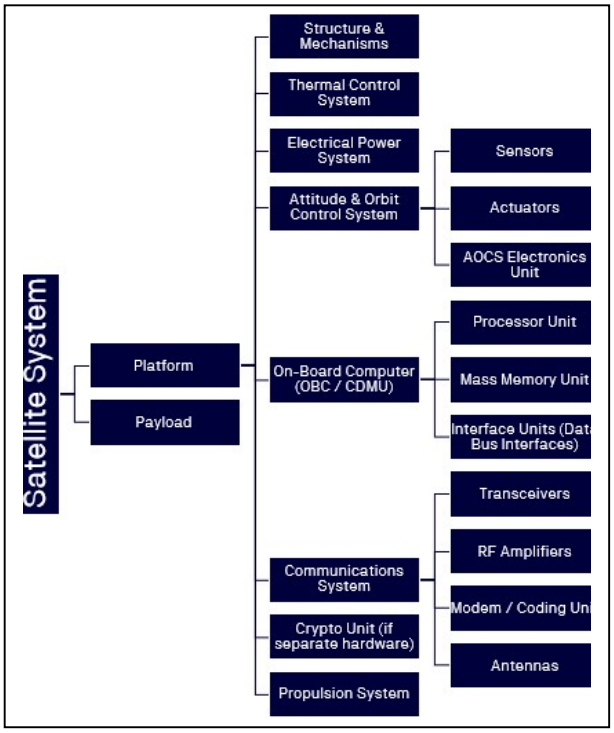

Figure 1: Component model on HW plane

B. Criticality Definition

The modular approach allows a categorization and grouping of modules based on their criticality for cybersecurity. The criticality can be influenced by mission specific parameters and is therefore to be validated and adjusted for each mission as needed. The categorization shown in this paper uses a generic approach which concentrates primarily on platform functionality.

For the presented model, the criticality is defined considering attack potential as well as potential impact of an attack. The levels are defined as critical (high impact), medium, low and no impact as shown in the table below.

TABLE I. Definition of Criticality

Criticality	*Impact*	*Colour coding*
High impact	Mission failure, loss of satellite, loss of confidential data Potentially dangerous impact on surrounding satellites	Red
Medium impact	Mission impact, impact on integrity of data Potential unwanted satellite movement	Yellow
Low impact	Loss of non-confidential data No impact on other satellites	Green
No impact	Potential (time limited) loss of connection	Grey

It is anticipated that only a limited number of modules exhibit a high impact on overall system security. Consequently, securing these critical modules can result in a substantial increase in security with relatively low effort, yielding a high return on investment. The majority of modules are expected to have no or low impact and may remain unchanged without compromising system security. Additionally, certain modules with medium impact could be selectively adjusted to further enhance security assurance with minimal additional effort, thereby contributing to an overall improvement in the system's security posture.

C. Criticality Mapping

The next step with the modular breakdown and the criticality definition in place, is to combine both approaches to achieve a mapping of criticality per module as not all of the building blocks of a satellite contribute equally to the cybersecurity of the whole system.

Modules for communication and cryptography are considered highly critical. Securing those modules will ensure the confidentiality and integrity of the data exchanged between the satellite and ground station and also secure the commanding of the satellite.

For an informed decision we assume that a red/black separation is implemented. This structure is shown in Figure 2. For the criticality mapping, it is assumed that externally accessible command and mission data paths are protected by cryptographic mechanisms. Therefore, the central component for satellite cybersecurity can be found in the crypto module.

While the exact implementation of satellite cryptography can vary widely between satellites, the communication model is valid across different architectures.

Figure 2: Red/Black separation of data in a satellite

With the crypto unit as the central component for security the satellites data and control, the other modules can be mapped according to their criticality.

The colour coding as defined in Table I is used to show the criticality for each module in the tree. The mapping has been done based on the potential attack impact as explained above.

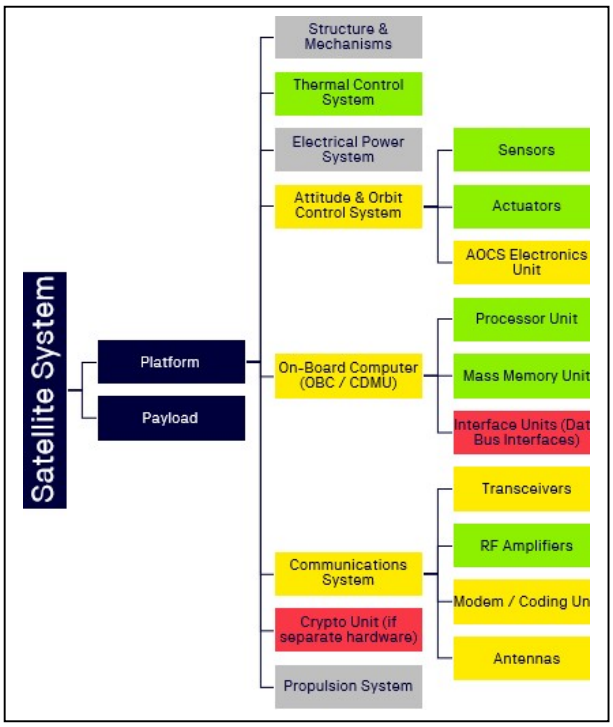

Figure 3: Criticality Mapping

Modules for communication and cryptography are considered highly critical. Securing those modules will ensure the confidentiality and integrity of the data exchanged between the satellite and ground station and also secure the commanding of the satellite.

III. Overview of Security Measures

Cybersecurity measures for satellite missions protect confidentiality, integrity, availability, authenticity, and accountability of commands, telemetry, payload data, onboard software, cryptographic material, and internal spacecraft interfaces [1], [2]. In small satellite missions, these measures must be selected under constraints in cost, development time, onboard processing capability, memory, bandwidth, power consumption, and verification effort [1], [2], [6]. A modular approach supports this selection by assigning security measures to spacecraft modules where they provide the highest security benefit [2], [3].

This section focuses on security measures for satellite and communication segments. The ground segment is treated as an externally procured service and is therefore not analyzed as an internal design element.

A. Communication and Command Protection

The command and communication path is one of the most security-critical parts of a satellite system. Unauthorized commands can alter spacecraft configuration, manipulate payload operation, change mission state, or cause loss of mission control [1], [4]–[6]. The RF link is exposed to interception, replay, spoofing, traffic analysis, and unauthorized frame injection [1], [4], [5]. Relevant controls include telecommand authentication, command validation, anti-replay protection, selected encryption, and logging of command execution events [2], [4], [5].

For small satellites, telecommand authenticity and integrity should normally be prioritized before telemetry confidentiality because unauthorized command execution usually has higher mission impact than passive observation of non-sensitive telemetry [1], [4]–[6]. Payload-data encryption should be applied according to mission sensitivity, commercial requirements, and regulatory constraints [1], [2], [4]. This measure has high security impact because it directly protects command authority and the exposed communication channel [1], [4]–[6].

B. Cryptographic Boundary and Key Protection

The cryptographic boundary separates externally exposed communication paths from trusted internal mission functions and performs authentication, replay protection, encryption, decryption, verification, and key handling [2], [4], [5]. In a modular architecture, the cryptographic unit is therefore the central cybersecurity-enforcing block: it controls the trust transition between the RF-facing domain and the internal spacecraft domain [2]–[5].

This principle corresponds to red/black separation. The black domain contains encrypted or externally exposed traffic, while the red domain contains plaintext commands, telemetry, payload data, internal control information, and mission state [2], [4], [5]. In large missions, this boundary may be implemented using dedicated cryptographic hardware, physical separation, certified equipment, and formal key-management infrastructure [2], [4], [5]. In small satellites, it may be implemented through logical separation, software partitioning, memory protection, secure elements, trusted execution features, restricted bus access, or a dedicated cryptographic microcontroller [2], [3], [6].

Key management is inseparable from this boundary. Critical keys include telecommand authentication keys, link encryption keys, software update verification keys, cryptographic module keys, and emergency access credentials [2], [4], [5]. Weak key handling can invalidate otherwise strong authentication or encryption [2], [4], [5]. Because the cryptographic unit has defined functions, interfaces, input-output behavior, and testable security properties, it is a strong candidate for module-level assurance and later certification reuse [2]–[5]. This category has high security impact because compromise of the cryptographic boundary can expose command authentication, link protection, key material, and the red/black separation between external communication and internal mission functions [2], [4], [5]

C. Trusted Software Lifecycle

Trusted software lifecycle measures protect onboard software from unauthorized modification from boot to update [2], [6]. They include secure boot, signed firmware, trusted execution, signed updates, anti-rollback protection, and recovery capability [2], [6]. Secure boot ensures that only authenticated and integrity-checked software is executed, while secure update mechanisms allow vulnerabilities to be corrected after launch without creating an unprotected path for modifying trusted code [2], [6].

Small satellites may implement this category through an immutable first-stage bootloader, signed firmware images, protected boot configuration, monotonic version counters, and a fallback image that preserves minimal commandability [2],

[6]. This measure has medium to high security impact because it reduces the risk of persistent onboard compromise and supports recovery from discovered vulnerabilities [2], [6].

D. Module Isolation and Access Control

Module isolation limits compromise propagation between spacecraft subsystems [2], [3]. Externally exposed communication functions should be separated from trusted mission functions wherever feasible [2]–[5]. Access between the onboard computer, payload controller, electrical power subsystem, AOCS, cryptographic unit, and internal buses should be restricted according to operational need [2], [3].

Relevant measures include software partitioning, memory protection, message filtering, bus access restrictions, allowlists, command privilege separation, and strict interface definitions [2], [3], [6]. This measure has medium security impact because it limits escalation from a compromised module to command authority, cryptographic material, or mission-critical control functions [2], [3], [6].

E. Security Monitoring and Telemetry

Security monitoring and telemetry provide evidence for detecting compromise, reconstructing events, and supporting operational response [1], [2]. Since spacecraft are normally physically inaccessible after launch, onboard evidence is essential for maintaining security awareness during operations [1], [2], [6]. Relevant events include command attempts, authentication failures, replay rejections, mode changes, software update activity, unexpected resets, cryptographic state changes, privileged function access, and anomalous interface behavior [1], [2], [4]–[6].

Small satellites should define a minimal security telemetry set because onboard storage, processing capability, and downlink bandwidth are limited [1], [2], [6]. The cryptographic unit is particularly important for monitoring because it can generate high-value events at the trust boundary, including authentication failures, replay detections, rejected frames, key-state changes, and verification failures [2], [4], [5]. This measure has only low impact because it enables detection and diagnosis, but does not prevent compromise by itself [1], [2].

F. Component and Supply-Chain Assurance

COTS components reduce cost and development time but introduce dependencies on external suppliers, firmware, software libraries, development tools, and undocumented implementation details [1], [2], [6]. Supply-chain measures include supplier assessment, component provenance checks, software bills of materials, firmware integrity checks, vulnerability monitoring, configuration baselines, and reuse of test or certification evidence [1], [2]. This measure has medium security impact because it reduces the likelihood that vulnerabilities, undocumented behavior, or weak assurance in reused components undermine the security assumptions of the overall satellite architecture [1], [2], [6]

For small satellite missions, deep assurance of every component is rarely feasible [1], [2], [6]. Assurance should therefore focus on components that affect command authority, cryptographic functions, software execution, timing, and communication security [1], [2]. The cryptographic unit should be a priority assurance target because it concentrates several high-impact functions: command authentication, link protection, key handling, red/black separation, and security-event generation [2], [4], [5].

Table II**Fehler! Verweisquelle konnte nicht gefunden werden.** summarizes the security measures discussed in this section using consolidated categories rather than individual controls. Threat modeling is treated as an enabling activity that informs the selection and tailoring of all measures. The qualitative impact assessment reflects the expected relevance of each category for modular small satellite missions, particularly with respect to loss of command authority, compromise of exposed communication paths, persistent onboard compromise, and leakage of cryptographic material.

TABLE II. COMPARATIVE IMPACT MATRIX

	Security measure	**Scope**	**Module**	**Relative impact**
1	Communication and command protection	Telecommands, telemetry, RF link	Crypto Unit, Communication system, interface units	High
2	Cryptographic boundary and key protection	Red/black separation, crypto functions, key material	Crypto Unit	High
3	Trusted software lifecycle	Boot chain, firmware, onboard software, updates	OBC, Crypto Unit	Medium - High
4	Module isolation and access control	OBC, communication system, internal buses	OBC, communication system, internal buses	Medium
5	Security monitoring and telemetry	Security-relevant onboard events	Crypto Unit, OCB	Low
6	Component and supply-chain assurance	COTS components, firmware, libraries, reusable modules	Crypto Unit, other potential COTS components	Medium

The most critical categories for small satellite missions are communication and command protection, cryptographic boundary and key protection, and the trusted software lifecycle [1]–[6]. These categories address attack paths that may lead to loss of control, unauthorized mission manipulation, data compromise, or persistent onboard compromise [1], [4]–[6]. A dedicated cryptographic unit can directly implement several of the highest-impact controls in these categories, including telecommand authentication, replay protection, encryption and decryption, key storage, key access control, and red/black boundary enforcement [2], [4], [5].

The cryptographic unit can also support other categories in the table, although it does not fully replace them. In the trusted software lifecycle, it can provide signature verification for secure boot and software updates, while the boot architecture and recovery strategy remain system-level functions [2], [6]. In module isolation and access control, it can enforce restricted cryptographic interfaces and limit access to key material, while broader partitioning and bus-access control remain architectural measures [2], [3]. In security monitoring and telemetry, it can generate high-value security events such as authentication failures, replay rejections, rejected frames, key-state changes, and verification failures [2], [4], [5]. In component and supply-chain assurance, it can serve as a bounded assurance target because its functions, interfaces,

cryptographic behavior, and key-handling requirements can be specified and tested more clearly than those of the complete satellite [2]–[5].

This concentration of high-impact functions motivates treating the cryptographic unit as a primary candidate for module-level assurance. Certification or structured assurance of this unit is more feasible than certification of the complete satellite because its boundary, interfaces, and expected behavior can be more clearly defined [2], [3]. In a modular smallsat architecture, assurance evidence for the cryptographic unit can therefore provide disproportionate value: it strengthens the most critical trust boundary while supporting reuse across missions with similar command, communication, and software-authentication requirements [2]–[5].

IV. Overview of Evaluation Methods

The implementation and testing of cybersecurity measures in space systems are typically the responsibility of the developer for each individual component. However, to enhance assurance in the security of these components, especially those intended for sale to multiple customers, independent evaluations and certifications are increasingly recognized as valuable. Such third-party assessments provide objective evidence of security robustness and facilitate trust across the space sector.

Evaluation methods can be applied at system, subsystem, and component level. At system level, evaluation focuses on the identification of security-relevant assets, interfaces, trust boundaries, threat scenarios, and residual risks [1], [2], [7]. At component level, evaluation can include design review, interface review, source-code review, vulnerability analysis, penetration testing, protocol-interface fuzzing, cryptographic verification, configuration assessment, and review of previously generated assurance evidence [2], [4], [5], [7]. These methods are especially applicable to modules with stable functions and interfaces.

Currently, there is no universally adopted standard for cybersecurity in space systems. Each mission may define its own requirements, or in some cases, lack explicit cybersecurity specifications altogether. This fragmented landscape has prompted ongoing efforts, particularly in Europe, to harmonize and advance standards for space system cybersecurity.

Several European and international cybersecurity standards, technical guidelines, and regulatory instruments are shaping the future of space cybersecurity.

Relevant standards/guidelines are:

- **ECSS Standards:** The European Cooperation for Space Standardization (ECSS) provides a framework for space mission requirements, recently enhanced by the ECSS-E-ST-80C standard [2]. These additions align security requirements across European missions, offering a common baseline for developers and evaluators. ECSS standards are supported by ESA and commonly used in ESA projects.
- **BSI TR-03184**: Information Security for Space Systems: Provides a system-level framework for information security in space systems and maps space-system security measures to potential threats [7]. It can be used to support requirement derivation, risk analysis, and evaluation of security measures at system, subsystem, and component level [7].
- **CCSDS security standards:** Provide technical standards and guidance for protecting space communication protocols, including authentication, encryption, replay protection, and protocol-layer security mechanisms [4], [5]. These standards are particularly relevant for evaluating communication interfaces, telecommand protection, telemetry protection, and cryptographic boundary behavior [4], [5].
- **National cybersecurity and space-security frameworks:** National frameworks may apply in parallel to European requirements, depending on the operator, mission type, procurement context, and national authorization process [8], [10], [12]. Examples include national critical-infrastructure requirements, national space-operations requirements, and space-specific cybersecurity guidance such as the CNES orbital system cybersecurity hygiene guide or BSI IT-Grundschutz profile for space infrastructures [8], [10], [12].

While relevant regulations/schemes are:

- **EU Cyber Resilience Act:** Introduces horizontal cybersecurity requirements for products with digital elements placed on the EU market [9]. For satellite-relevant components that qualify as products with digital elements, CRA requirements may affect product design, documentation, vulnerability handling, lifecycle support, and conformity assessment [9].
- **EU Cybersecurity Act and EUCC**: Establish the European cybersecurity certification framework and the European Common Criteria-based cybersecurity certification scheme for ICT products [11], [13]. EUCC can support CRA conformity where the product classification, assurance level, and certificate scope match the applicable requirements [9], [11], [13]. It is particularly relevant for security-enforcing ICT components such as cryptographic units, secure elements, security controllers, and trusted execution components [11], [13], [14].

This standards and regulation landscape supports a modular assurance model. If every mission implements its own security measures independently, evaluation effort is repeated for each satellite. If a security-enforcing component is evaluated or certified once and then reused, part of the assurance evidence can be inherited by multiple missions. The satellite developer still has to verify correct integration, configuration, interfaces, and operational use, but does not need to reproduce the complete component-level security evaluation for every mission [2], [7], [11]– [13].

This model is especially relevant for the cryptographic unit. Since the cryptographic unit concentrates several high-impact cybersecurity functions, certification of this component can provide reusable evidence for the most critical trust boundary of the satellite. Procurement of an evaluated or certified cryptographic unit can therefore increase trust in the satellite's cybersecurity posture while reducing mission-

specific evaluation effort. The resulting assurance argument is not that the complete satellite becomes certified through procurement of one component, but that a certified cryptographic unit provides reusable, independently assessed evidence for authentication, encryption, key protection, boundary enforcement, and related security functions [2], [4], [5], [7], [11]–[14].

To further leverage reusable assurance evidence, a dedicated Protection Profile for satellite cryptographic units could simplify and harmonize future EUCC evaluations.

V. Conclusion

The criticality mapping demonstrates that only a small subset of modules drives the majority of cyber risk. Among these, the cryptographic unit emerges as the central security-enforcing block: it concentrates telecommand authentication, replay protection, link encryption, key protection, red/black boundary enforcement, and the generation of high-value security events. Strengthening this unit therefore yields a disproportionate improvement of the overall security posture relative to the development effort required, while leaving the larger set of low- and medium-impact modules largely unchanged.

A modular architecture alone, however, cannot establish assurance. Implementations developed and self-tested by individual mission teams cannot provide the objective evidence increasingly demanded by operators, regulators, insurers, and the broader supply chain. Independent third-party evaluation is therefore essential to substantiate claims of security robustness, particularly for components — such as cryptographic units, secure elements, and security controllers — whose interfaces and expected behavior can be specified with sufficient precision to be evaluated against repeatable criteria. External evaluation also enables reuse: assurance evidence generated once for a well-bounded component can be inherited by multiple missions, amortizing evaluation cost across a fleet or product line and shortening the security-related schedule for any individual mission.

In this regulatory and technical context, the European Cybersecurity Certification Scheme on Common Criteria (EUCC) offers a particularly well-suited framework. EUCC provides a harmonized, mutually recognized basis for evaluating ICT security products at defined assurance levels, with documented scope, methodology, and certificate semantics, and it is explicitly intended to support conformity with horizontal regulatory regimes such as the Cyber Resilience Act. Applied to a satellite cryptographic unit, EUCC certification produces reusable, independently assessed evidence for the most critical trust boundary of the spacecraft, aligns smallsat practice with the wider European cybersecurity ecosystem, and reduces the marginal evaluation effort required for each subsequent mission that integrates the same component.

Future work should focus on three directions: the definition of a representative Protection Profile for satellite cryptographic units suitable for EUCC evaluation; the validation of the modular criticality mapping against operational mission data and incident reports; and the establishment of reference integration patterns that allow EUCC-certified components to be deployed in resource-constrained smallsat platforms without reproducing component-level evaluation effort for every mission.

References

[1] European Union Agency for Cybersecurity, *Space Threat Landscape*, 2025.

[2] European Cooperation for Space Standardization, *ECSS-E-ST-80C: Space Engineering — Security in Space Systems Lifecycles*, 2024.

[3] European Space Agency, *SAVOIR Functional Reference Architecture* and related SAVOIR avionics architecture material.

[4] **C**onsultative Committee for Space Data Systems, *Space Data Link Security Protocol*, CCSDS 355.0-B-2, Recommended Standard, Issue 2, 2022.

[5] Consultative Committee for Space Data Systems, *The Application of Security to CCSDS Protocols*, CCSDS 350.0-G-3, 2019.

[6] J. Willbold *et al*., "Space Odyssey: An Experimental Software Security Analysis of Satellites," in *Proc. IEEE Symposium on Security and Privacy*, 2023.

[7] German Federal Office for Information Security, *BSI TR-03184: Information Security for Space Systems*, Part 1: Space Segment and Part 2: Ground Segment.

[8] European Parliament and Council, *Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union*, NIS-2 Directive, 2022.

[9] European Parliament and Council, *Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements*, Cyber Resilience Act, 2024.

[10] CNES, *Orbital System Cybersecurity Hygiene Guide*, 2025.

[11] European Parliament and Council, *Regulation (EU) 2019/881*, Cybersecurity Act, 2019.

[12] German Federal Office for Information Security, *IT-Grundschutz Profile for Space Infrastructures*, 2022.

[13] European Commission, *Commission Implementing Regulation (EU) 2024/482 establishing the European Common Criteria-based Cybersecurity Certification Scheme (EUCC)*, 2024.

[14] ISO/IEC, *ISO/IEC 15408 — Information Security, Cybersecurity and Privacy Protection — Evaluation Criteria for IT Security*, Common Criteria.

[15] ISO/IEC, *ISO/IEC 15408 — Information Security, Cybersecurity and Privacy Protection — Evaluation Criteria for IT Security*, Common Criteria.

[16] German Federal Office for Information Security, *IT Security Act 2.0 / BSIG-related cybersecurity requirements for critical infrastructures and companies of special public interest*, 2021.