Secure-by-component: A System-of-systems Design Paradigm for Securing Space Missions

Arun Viswanathan
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA, USA
arun.a.viswanathan@jpl.nasa.gov

Brandon Bailey
Aerospace Corporation
West Virginia, USA
brandon.bailey@aero.org

Kymie Tan
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA, USA
kymie.tan@jpl.nasa.gov

Gregory Falco
Dept. of Mechanical and Aerospace Engineering
Cornell University
Ithaca, NY, USA
gfalco@cornell.edu

***Abstract*—Space missions face increasing adversarial threats, making security a more critical concern than ever before. As space becomes congested and contested, the success and safety of these missions rely heavily on the security and resilience of complex systems. Unfortunately, most standards, guidance, and frameworks for space cybersecurity often fall short in emphasizing security as a primary consideration during the initial design phases and are typically applied as an afterthought once the mission is deployed. A secure-by-design approach for space missions should address the wide diversity of missions and the unique characteristics of each one. To tackle this challenge, we introduce *secure-by-component*, a system-of-systems approach to thinking about secure-by-design for space missions. Our design strategy involves the concept of *secure blocks* as foundational building blocks for securing space missions. These blocks can be flexibly combined to create secure architectures tailored to meet the unique requirements of each space mission. We demonstrate the usability of our approach by applying it to a critical component of a spacecraft, specifically the star tracker. We discuss the practicality, flexibility, and scalability of our strategy and its applicability to the forthcoming IEEE technical standard on space system cybersecurity. Our proposal is designed to enhance, not replace, top-down approaches to security by complementing existing system engineering strategies. Furthermore, we emphasize that our approach can be readily adopted by individual space organizations and adapted to other domains that include systems-of-systems, highlighting its potential for broad application beyond space missions.**

***Index Terms*—Secure-by-design, space cybersecurity, mission cybersecurity, system of systems security**

I. Introduction

Space missions have traditionally been scientific and exploratory endeavors. Today, however, growing commercial access to space has catalyzed a global appreciation of space as a critical resource. Space technologies and assets are integrated into almost all essential sectors and functions, including defense, agriculture, transportation, energy, and telecommunications. This serves to underscore the imperative that the security and resilience of space missions be addressed and prioritized. The current threat landscape [1]–[7], further argues in favor of addressing security in today's missions, an effort that has until recently been largely ignored within the traditional lifecycle of these flight projects.

Space organizations worldwide are now working to address the significant technical debt through a combination of published requirements, guidelines, best practices, and standards [8]–[14]. While these efforts are commendable and helpful, current strategies often rely on implementing security controls and mitigations as an afterthought to compensate for initial design shortcomings. However, emerging space ventures find themselves in a unique position to redefine the systems that will play vital roles in the years to come. Embracing a *secure-by-design* approach offers an opportunity to move away from depending solely on security controls as reactive measures for poor design choices. Further, the advent of the 'new space' sector has brought exponential launch capacity and assets to orbit, already outnumbering the legacy systems in space. The resurgence of this sector can take advantage of decades of security research in related industries, all while establishing secure systems from the beginning. This is in contrast to the prevailing approach which relies on persistent patching, firmware updates, and other band-aids.

The *secure-by-design* approach emphasizes the integration of security from the start of the design phase of systems, products, or processes, a concept recently highlighted by publications from the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) in the USA, and UK's National Cyber Security Centre [15]. We acknowledge that the term secure-by-design has been interpreted variously in the literature, including referring to the use of formal methods in system design [16]. However, our definition is rooted in system engineering and is based on the guidelines provided by publications from NIST and CISA. These publications, especially NIST's 800-160 volumes 1 and 2 [17], [18], and CISA's guidelines [6], advocate for embedding cybersecurity throughout all stages of system engineering and design, promoting a proactive rather than reactive approach to security. While the concept of secure-by-design is informative, it lacks the necessary level of detail for space system architects to implement it effectively. For instance, specific questions such as the depth of security required, the level of abstraction within the computing stack, and whether different space missions demand distinct security principles, are still left unanswered for system designers.

Space missions vary significantly in scope, size, and purpose, and as we argue in Section III, a one-size-fits-all approach to security is impractical. Consequently, a fundamental challenge involves developing a secure-by-design strategy that is practical, flexible, and scalable, taking into account the diversity of missions and the unique aspects of each mission.

Space systems are the canonical system-of-systems, where each segment of a space system (user, space, ground, and link) can be decomposed into subsystems and further broken into components and subcomponents. In this work, we introduce *secure-by-component*, a system-of-systems approach to thinking about secure-by-design for space missions. Fundamentally, our design strategy involves the concept of *secure blocks* as foundational elements of security in a complex system. The strategy, as discussed in Section IV, results in the creation of secure blocks that can be flexibly combined to form secure architectures, customized to meet the distinct needs of each space mission.

We emphasize that our proposal is designed to complement, and not replace, existing top-down system engineering strategies for security analysis. Additionally, we do not assert that simply creating secure blocks and integrating them into a system will inherently yield a secure system, as previously shown in literature [19]. Our bottom-up approach is intended to assist system engineers in specifying concrete and detailed security requirements for low-level system components. This approach should be integrated with a top-down analysis grounded in mission priorities for the entire system to establish high-level requirements tailored to a specific space mission. Such analysis will form the framework for selecting and assembling the secure blocks. We briefly discuss a strategy that combines top-down and bottom-up analyses in Section VI.

Contributions In this paper, we make several key contributions: (1) we introduce *secure-by-component*, a system-of-systems design paradigm for securing space missions, that is practical, flexible, and scalable; (2) we introduce *secure blocks* as foundational elements for building secure architectures in complex system-of-systems; (3) we provide a detailed rationale of our strategy, emphasizing how it builds upon previous work and detailing the areas in which it differs and enhances these existing approaches; and (4) we showcase the practical application of our strategy by implementing it on a low-level component of the space segment.

Furthermore, our proposed methodology serves as the cornerstone of the forthcoming international, technical IEEE Standard on Space System Cybersecurity [20], [21] (see Section II-C).

The rest of the paper is structured as follows. Section II discusses the existing standards and guidance for space cybersecurity and their limitations. Section III discusses the challenges in building a secure-by-design strategy for missions, and presents the rationale for our approach. Section IV presents our overall secure-by-component strategy. Section V presents a detailed application of the approach to a component of the space segment. Section VI discusses the benefits of our approach. Section VII concludes the paper.

II. Background and Related Work

In this section, we first discuss some of the popular space cybersecurity standards, followed by their limitations. We then delve into existing guidance on secure-by-design, and discuss how and where our approach differs. Finally, we end this section by briefly discussing the upcoming IEEE Standard on Space System Cybersecurity.

A. Space Cybersecurity Standards and Guidance

The domain of space cybersecurity has seen a substantial increase in guidelines and frameworks recently, with numerous entities, including international space agencies, establishing guidance for various space-related topics. Below we discuss some of the key initiatives in this area.

NIST 800-53, while not exclusively for space systems, is a notable document that provides a comprehensive set of security controls for information systems and organizations [22]. The controls within NIST 800-53 are categorized into families, tackling different elements of information security and risk management. Agencies such as the National Aeronautics and Space Administration (NASA) have adapted these controls to enhance the security of space mission ground systems. There is also a *Space Platform Overlay*, supplementing NIST 800-53B as part of CNSSI 1253, which adapts the NIST controls for space vehicles [23]. In addition to establishing controls, NIST has generated profiles for their Cybersecurity Framework onto the Satellite Command and Control use case that helps organizations understand their risk with respect to identifying, protecting, detecting, responding, and recovering from cyber events [24], [25].

NASA has created and issued the Space System Protection Standard, which sets forth mandatory high-level protection requirements for NASA missions [10]. NASA also recently released the *Space Security: Best Practices Guide (BPG)* which serves as a conduit, translating NIST 800-53's controls to NASA's operational context [14]. It outlines principles and controls relevant to both spacecraft and ground systems, converting technical jargon into practical terms for mission implementation.

Internationally, other organizations have also developed similar guidelines for space protection. The German Federal Office for Information Security (BSI) has published the IT-Grundschutz Profile for Space Infrastructures, suggesting a basic level of security for satellite information systems that considers the entire satellite lifecycle and the impact of cyber-attacks [11]. In Japan, the Ministry of Economy, Trade and Industry (METI) provides guidelines for securing commercial space assets, detailing risk scenarios and mitigation strategies for subsystems [12]. Furthermore, The European Cooperation for Space Standardization (ECSS), a joint effort among the European Space Agency (ESA), the space industry, and national agencies, has created a unified set of standards aimed at ensuring the quality of space engineering processes and products [13].

Additionally, the Consultative Committee for Space Data Systems (CCSDS), which includes members from space agencies worldwide, has issued publications analyzing overarching threats to space missions and describing a general security architecture for space data systems [8], [9]. These comprehensive efforts underscore the international commitment to safeguarding space assets from evolving cybersecurity threats.

Limitations While there is no shortage of cybersecurity guidelines for space missions, we note the following shortcomings in existing work.

- *Most frameworks are used post-deployment*: The proposed risk frameworks are informative for operators, but are not necessarily used by developers during the early phases of a mission. Instead, they are often used for evaluating risk management procedures and controls, after deployment.
- *High-level and abstract*: Some of the existing guidance is comprised of high-level requirements that, although important, are too vague and not detailed enough to be practically implementable.
- *Non-technical*: There is an abundance of non-technical guidance. Despite the critical contributions of non-technical security practices such as training, and information sharing, technical security details unique to highly technical space systems are necessary to serve developers instead of policymakers.
- *Fragmented Approach*: Space systems are complex, consisting of interconnected ground, user, link, and space segments. Current cybersecurity guidance tends to focus on specific segments or subsystems, or it is only relevant to certain mission classes, leading to a piecemeal approach.
- *Reliance on Non-Space Cybersecurity Standards*: Due to the lack of a comprehensive technical standard for space cybersecurity, there is a tendency to repurpose general cybersecurity guidelines for space missions. This is known to be insufficient due to the substantial technical knowledge gaps it introduces and the failure to address the uniqueness of space systems in a cyber context [26].

B. Secure-by-Design Practices

The *secure-by-design* approach is a proactive and strategic method to develop systems, products, or processes with security considerations integrated from the very beginning of their design phase. While the core principles of this approach have been recognized for some time, they have recently gained increased prominence, thanks in part to publications by NIST and CISA. NIST's special publications, especially the 800-160 volume 1 [17] and volume 2 [18] outline high-level frameworks for engineering secure and resilient systems, emphasizing the integration of cybersecurity across all phases of the systems engineering process. Additionally, the CISA publication offers overarching principles and tactics, encouraging software vendors to prioritize security integration into their system design life cycles [27]. This collective guidance underscores the importance of a proactive approach to security, ensuring that it is an integral part of the design and development process, rather than an afterthought.

Although the publications from NIST and CISA represent a significant step forward for secure-by-design, they primarily offer broad and abstract principles, processes, and guidelines that are not immediately implementable by a mission designer. For instance, the NIST 800-160 publications emphasize the integration of security requirements in the early stages of the engineering lifecycle. However, they do not provide specific details on what these security requirements should entail. This lack of clarity can pose challenges for system engineers in understanding and implementing these guidelines effectively.

Our proposed design strategy is tailored to address the specific challenges and unique aspects of the system-of-systems that comprise a space mission. The goal of this strategy is to produce detailed security requirements that are clear and straightforward for system engineers to implement within their engineering processes. Furthermore, the proposed strategy is central to the forthcoming IEEE Standard for Space System Cybersecurity [21], as we discuss next.

C. IEEE Standard on Space System Cybersecurity

The need for a comprehensive, international, space-focused cybersecurity standard was perceived due to the limitations and challenges with existing guidelines, as discussed earlier, coupled with the international supply chain that forms our space ecosystem. In today's rapidly evolving space and threat environment, a well-planned, systematic approach is essential for addressing the unique cybersecurity challenges of space missions thoroughly and technically. The proposed IEEE standard [21] aims to unite the international space systems community in establishing a comprehensive technical standard, that will specify technical cybersecurity requirements for all segments of a space system.

Unlike existing guidelines, the IEEE standard's objective is to offer a thorough and practical *secure-by-design* approach for protecting space missions, encompassing the ground, space, user, and link segments, including an integration layer. It prioritizes security as a fundamental aspect of the design and development process, rather than as a secondary consideration. Additionally, this standard recognizes the diversity, complexity, and uniqueness of space missions, promoting a strategy that is both flexible and scalable to different mission requirements.

III. Challenges for Secure-by-design Strategy for Space Missions

Space missions vary significantly in scope, size, and purpose. For example, human space flight, navigation satellites, Earth observation satellites, communication satellites, and deep space missions vary significantly in their requirements and design. Even within the above mission categories, each mission has a distinct set of requirements, influenced by a multitude of factors, as we discuss below. Consequently, a fundamental challenge involves developing a secure-by-design strategy that is practical, flexible, and scalable, taking into account this extensive diversity of missions and the unique aspects of each mission.

One approach for such a strategy could involve developing secure-by-design reference architectures tailored to a set of mission categories, profiles, or classes, as is often seen in existing guidelines [9], [12], [24], [25]. In this approach, the initial step would entail defining a set of mission classes with security as a central consideration, followed by the development of a secure-by-design reference architecture tailored to each mission class. However, as discussed below, this approach may be unnecessarily rigid, limited in scalability, and challenging to apply effectively.

A. Limitations of categorizing missions into classes

Categorizing space missions into a finite set of classes for security purposes is challenging due to their inherent variety. Each mission's unique objectives, budget, design, technology, operations, and environment create distinct security needs.

The objectives of a mission dictate specific needs; a scientific exploration mission, for instance, has different security requirements compared to a human space flight mission. Budget constraints also play a critical role. Missions smaller in scope may need to prioritize cost-effective security solutions, while larger missions might have more resources but also higher stakes. Design limitations, such as the size and weight of satellites, or compute and storage resources, may further influence the security measures that can be implemented. For example, cutting-edge encryption technologies might be suitable for a high-profile mission with more resources at their disposal but may not be viable for smaller projects. Operational parameters, such as mission duration, orbits, and range, also play a vital role in determining the security strategy. A long-duration deep space mission may require more robust and durable security measures compared to a shorter-term Earth orbit mission. Further, Earth-orbiting missions may be subject to a different threat profile as compared to deep-space missions.

The resulting array of security requirements for various missions is diverse and extensive, making it challenging to categorize them into a finite set of standardized architectures. This is, in part, a function of how space systems are system-of-systems, where systems are assembled to meet the mission constraints and priorities described above. It is important to recognize that there is no single, universally applicable secure-by-design architecture or a fixed set of architectures that can satisfy the security needs of all missions. Even if we were to prescribe a finite set of security architectures along with design recommendations or controls for different mission profiles, there would still be a significant level of uncertainty for system engineers. Such an approach would not cater to the unique requirements of every mission. In summary, attempting to use a "one-size-fits-all" approach to security in the context of space missions is not practical or effective.

B. Rationale for Our Approach

Considering the challenges discussed earlier, we propose an approach to secure-by-design for space missions called *secure-by-component*. Our approach moves away from categorizing missions into classes or recommending a uniform reference architecture or a set of reference architectures. Instead, we adopt a system-of-systems perspective when considering secure-by-design for space missions, given that each segment of a space system can be decomposed into subsystems and further broken into components and subcomponents. Secure-by-component centers on addressing the complexity and diversity of space systems by prioritizing the security of their fundamental building blocks. These foundational components, referred to as *secure blocks*, can be flexibly combined to create secure architectures tailored to the specific requirements of each unique space mission. The secure-by-component strategy offers several advantages.

- When planning a new space mission, secure blocks can be selected and arranged to best suit the mission's unique requirements, objectives, and constraints. This modular strategy enables the creation of a bespoke architecture for each mission, ensuring that security is seamlessly integrated at a fundamental level and optimized for the specific mission context.
- This method also accommodates the evolving nature of space missions. As new technologies emerge and mission parameters change, the secure blocks can be updated, replaced, or reconfigured, ensuring that the security architecture remains robust and relevant.

This approach represents a significant shift from traditional, rigid security planning to a more dynamic, component-based strategy that accommodates modular systems-of-systems. We next discuss our strategy in detail.

IV. Secure-by-component Design Strategy for Space Missions

The secure-by-component strategy is focused on building secure blocks. When applied to a space system, the output of the strategy will be a comprehensive list of secure blocks spanning space, ground, user, and link segments of a space system. The overall steps of the strategy are summarized in Figure 1, with the details discussed below.

Step 1: Identify the relevant low-level components and data flows for the system at a consistent level of abstraction.

We first begin by decomposing the system into suitable low-level components. These low-level components, or the individual building blocks of the system, can contribute to key capabilities, and represent functions, services, protocols, or hardware entities within the system. They can be detailed (like the *star tracker* hardware and software in a space vehicle) or broader (like the entire Command and Data Handling (C&DH)

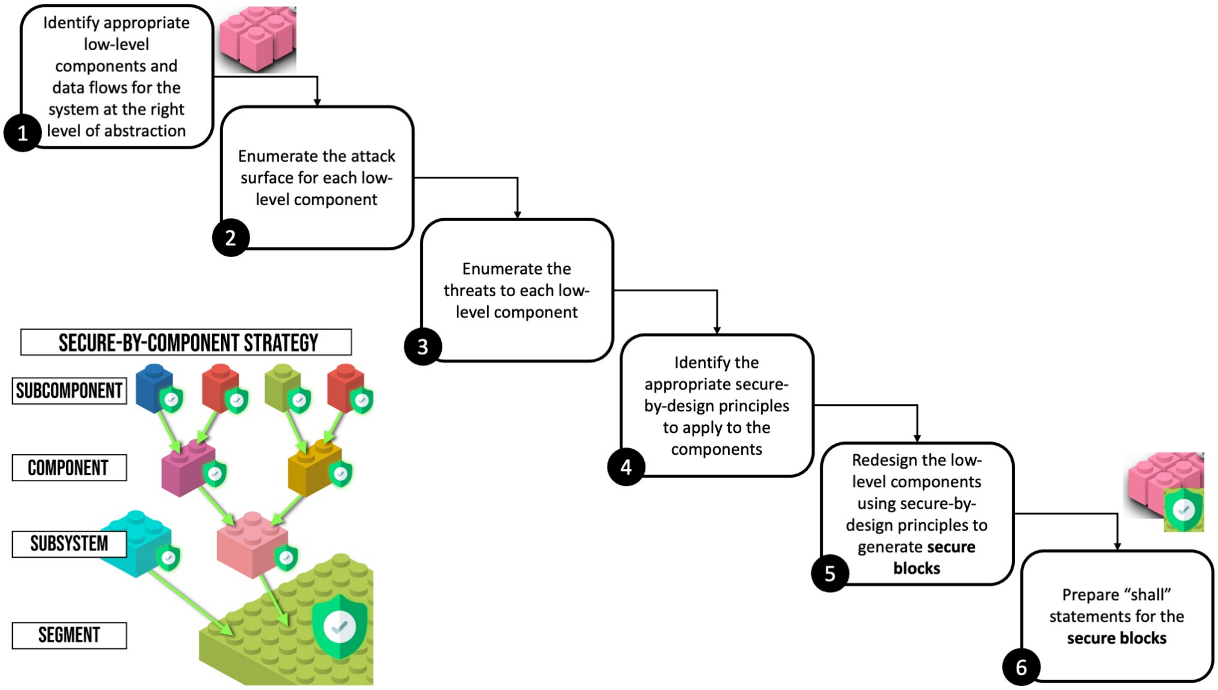
Identify appropriate low-level components and data flows for the system at the right level of abstraction
1
Enumerate the attack surface for each low-level component
2
Enumerate the threats to each low-level component
3
Identify the appropriate secure-by-design principles to apply to the components
4
Redesign the low-level components using secure-by-design principles to generate **secure blocks**
5
Prepare "shall" statements for the **secure blocks**
6
SECURE-BY-COMPONENT STRATEGY
SUBCOMPONENT
COMPONENT
SUBSYSTEM
SEGMENT

Fig. 1. The figure shows the high-level steps of the *secure-by-component* design strategy are used to create *secure blocks* from low-level components of the space system. The bottom left figure conceptually demonstrates the overall idea behind the strategy.

function), depending on the context. Given the scale and complexity of a space system, it is essential to strike a balance between low-level detail and maintaining a sufficient level of abstraction.

Step 2: Enumerate the attack surface for each of the low-level components

Enumerating the attack surface for each low-level component in a system involves identifying and documenting all potential entry points or vulnerabilities that could be exploited by malicious actors. The attack surface for each low-level component essentially comprises the component's inputs, outputs, and dependencies. These can be identified by: (a) analyzing how data and control flow in and out of the component; (b) identifying interfaces, which may include APIs, network connections, user interfaces, and communication channels; and (c) identify any external dependencies the component relies on, such as other system components or capabilities. This step also captures any inter-segment, inter-system interactions, or dependencies between the low-level components.

Step 3: Enumerate threat techniques for each of the low-level components

In this step, we employ threat modeling to identify threats and specific threat techniques for each low-level component. These threats and techniques can be determined using various methods, such as STRIDE [28], Aerospace SPARTA [29], or MITRE ATT&CK [30]. Leveraging SPARTA and ATT&CK as a source for threat-informed techniques offers benefits by providing a correlation between attacks with defense strategies. We've chosen to use the Aerospace SPARTA matrix [29] for the space segment, MITRE ATT&CK Enterprise [30], ICS [31] and ATLAS [32] frameworks for the ground and user segments, and SPARTA and MITRE FiGHT [33] for the link segment.

Step 4: Identify secure-by-design principles

The next step involves selecting secure-by-design principles to redesign low-level components and mitigate identified threats. Examples of such principles include the principle of least privilege, separation of concerns, complete mediation, and defense-in-depth. In Section V, we demonstrate how to choose relevant principles for a space segment component based on its threat profile.

As part of the development of the IEEE standard, we plan to compile a comprehensive list of these principles from existing literature and frameworks. Some principles, particularly those that serve as countermeasures, are already incorporated in resources like the Aerospace SPARTA [29] and MITRE D3FEND [34]. Additionally, we will integrate new principles from sources like NIST 800-160 vol. 2 [18], enriching our approach to secure-by-design for space system components.

Step 5: Redesign the low-level components using secure-by-design principles to generate secure blocks

In this phase, we revisit and modify the low-level components to create secure blocks, aligning them with the secure-by-design principles outlined in Step 4. Our objective is to address the threats identified in Step 3.

A redesign of the low-level components would result in a "maximum-security design" that would be crafted to mitigate all the identified threats in the previous step. But, a maximum-security design may not always be feasible within the context of every mission. For example, a low-cost CubeSat mission may not have the resources for full encryption of its internal bus and may be unnecessary given the objectives of the mission. Thus, a key challenge here is in rigorously scoping the requirements for a secure block with respect to the high-level objectives and priorities of a mission. We briefly discuss a top-down approach in Section VI-H that facilitates defining a minimum set of requirements for secure blocks tailored to a particular mission. A comprehensive explanation of our approach can be found in Falco et al. [35].

Step 6: Prepare shall statements for the secure blocks

Finally, we draft the detailed technical *shall* statements for the secure blocks generated in the previous step.

V. Example Application of the Approach

In this section, we demonstrate our approach by applying it to a component of the space vehicle.

Step 1: Identify the appropriate low-level components for the space vehicle

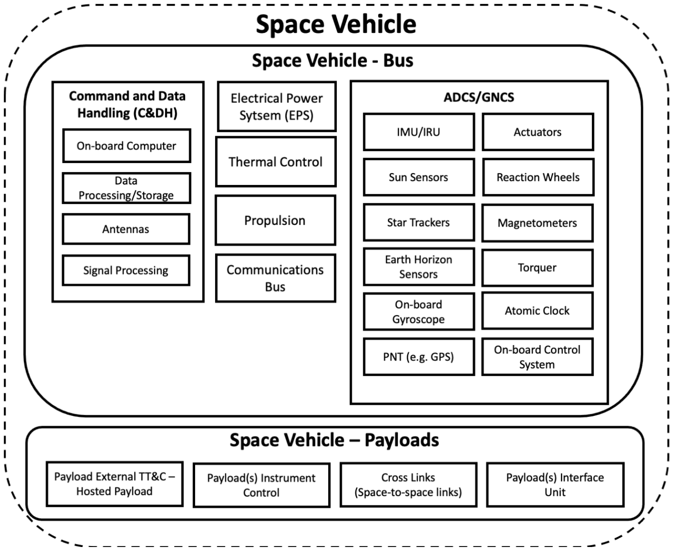

Fig. 2. Decomposition of a space vehicle into its low-level components.

Figure 2 shows a high-level decomposition of a space vehicle into its low-level components. We omit the data flows in this figure for simplicity and clarity. For this example, we will focus on "Star Tracker," a low-level component within "ADCS / GNCS". The Attitude Determination and Control Subsystem (ADCS) is a core system on a spacecraft responsible for determining and controlling its orientation to achieve mission goals. ADCS relies on sensors like sun sensors, star trackers, magnetometers, and gyroscopes to ascertain the spacecraft's attitude with respect to celestial objects, Earth's magnetic field, and rotation. Star trackers, in particular, identify stars in the sky to precisely determine the spacecraft's orientation. They capture star images and use star catalogs to calculate orientation based on star positions. Star trackers are essential for scientific missions and spacecraft requiring highly accurate pointing.

Step 2: Enumerate the attack surface for the star tracker

The attack surface for the star tracker comprises the inputs, outputs, and dependencies as defined below.

Inputs The inputs to the star tracker consist of: (a) *starlight* from celestial objects; (b) *star catalog database* that contains information about the positions and characteristics of known stars; (c) *attitude control system data* which provides information about the spacecraft's attitude and orientation from the attitude control system; and (d) *sun sensor data* which detects and excludes the presence of the Sun in the field of view.

Outputs The outputs of the star tracker consist of: (a) *attitude information*, which is sent to the spacecraft's control systems and other relevant subsystems; (b) *star IDs* which are identification numbers or labels corresponding to known stars in the catalog; (c) *housekeeping telemetry*, which indicates the status of the star tracker, such as whether the solution is valid, whether the tracker is tracking stars successfully, or if certain conditions are met; and (d) *time stamp*, which indicates the time of the attitude determination.

Dependencies The star tracker depends on: (a) *sun sensors*, to avoid interference, sensor saturation, and inaccurate measurements from the Sun; (b) *thermal control*, as the star tracker's performance can be affected by temperature variations; (c) *communication interface*, since the star tracker must be able to communicate information to the spacecraft bus and applicable sub-systems; (d) *electrical power system*, as the star tracker requires a stable and reliable power supply to operate its components; and (e) *ADCS / Navigation*, as the star tracker may rely on data from spacecraft navigation systems to improve accuracy.

Step 3: Enumerate the threats to the star tracker

In this paper, we employ a dual approach, integrating the STRIDE [28] framework for outlining high-level threats, and the Aerospace SPARTA [29] framework for detailing specific threat techniques relevant to space systems. However, due to limited space, we only present a subset of the threats to the star tracker, and the corresponding attack techniques.

High-Level Threats First, we apply the STRIDE framework to the inputs, outputs, and dependencies of the star tracker component, as identified in Step V. This approach helps us enumerate a comprehensive list of potential threats. In this paper, we focus on three illustrative threats:

- *Spoofing:* An adversary could spoof the star tracker's inputs, leading to incorrect spacecraft orientation.
- *Tampering:* An adversary could alter inputs to the star tracker, inducing errors in spacecraft orientation.
- *Denial-of-Service (DoS):* An adversary might prevent the star tracker from providing attitude information, potentially leading to mission failure.

Attack Techniques We next examine specific techniques an adversary might use to execute these threats in a space system. The corresponding SPARTA IDs are shown in parentheses.

- *Spoofing Techniques:* Spoof sensor data, such as inputs from the sun sensor (EX-0014.03), or spoof data on the main or secondary bus of the spacecraft, sending false inputs to the star tracker (EX-0014.02).
- *Denial-of-Service Techniques:* Inject noise/data/signal into the star tracker's inputs (EX-0013.02), or flood the star tracker with valid commands to overwhelm its computing capabilities (EX-0013.01).
- *Tampering Techniques:* Maliciously modify the star catalog input to the star tracker through unauthorized memory writes (EX-0012.03), or modify onboard values like registers that control the star tracker's configuration (EX-0012.01), or target the onboard values of the ADCS, affecting spacecraft orientation (EX-0012.08).

Step 4: Identify "secure-by-design" principles for the star tracker

We leverage Aerospace SPARTA's built-in correlation between techniques and potential countermeasures, to generate a set of secure-by-design principles for the star tracker. We arrive at several principles for redesigning the star tracker for the set of threats and techniques identified in the previous section, a subset of which are shown below.

- *Principle of least privilege:* Implement the principle of least privilege by permitting only essential authorized processes that are necessary for completing specific tasks aligned with the system's functions.
- *Process whitelisting:* Simple process ID whitelisting on the firmware level could impede attackers from launching unauthorized processes that could impact the spacecraft.
- *Segmentation:* Identify the key system components or capabilities that require isolation through physical or logical means. Information should not be allowed to flow between partitioned applications unless explicitly permitted by security policy.
- *Onboard Intrusion Detection and Prevention System:* Utilize an onboard intrusion detection/prevention system that monitors the mission-critical components or systems and audits/logs actions.
- *On-board message encryption:* It is recommended to encrypt the spacecraft bus, to protect the confidentiality of the data traversing the bus.

Step 5 & 6: Redesign the star tracker into a secure block using identified principles and identify detailed security requirements

Our analysis leads us to design that includes principles such as the "Principle of least privilege," "Segmentation," "Process whitelisting," "On-board message encryption" and "Onboard Intrusion Detection and Prevention System". These principles are not customized to the specific context of an individual mission but rather are the result of a comprehensive analysis that assumes maximum security for the component.

After selecting design principles, we develop the corresponding security requirements. We use the SPARTA framework to create a baseline set of requirements, which are then refined and expanded based on an analysis of the attack surface, as explained in Step V. The analysis results in a set of 35 requirements. We present five example security requirements for the star tracker below.

- The star tracker shall employ the principle of least privilege, allowing only authorized processes that are necessary to accomplish assigned tasks.
- The star tracker data within partitioned applications shall not be read or modified by other applications/partitions within the spacecraft.
- The star tracker shall protect the availability of resources by allocating resources based on priority, quota, or both.
- The star tracker shall only use communication protocols that enable authenticated encryption.
- The star tracker shall implement cryptographic mechanisms to detect changes to the star map.

To summarize the example, we began by selecting a critical low-level component of a spacecraft and conducted an attack surface analysis. We identified potential threat techniques and developed a set of secure design principles specifically tailored for redesigning this component into a secure block. This process led to the creation of precise "shall" statements for detailed security requirements. This library of requirements serves as a guide for system designers, enabling them to select a design that aligns with their specific mission's unique needs and constraints while incorporating an appropriate level of security. As we discuss later in the next section, our process needs to be combined with a top-down approach to select requirements that are tailored to a particular mission.

VI. Discussion

In this section, we discuss the benefits of our strategy. We will also examine its application to the forthcoming IEEE Standard on Space System Cybersecurity. Furthermore, we will discuss how individuals can adapt and implement this strategy within their organizations, and explore its potential applicability to various other domains.

A. Practicality of the approach

The secure-by-component strategy offers practical benefits in at least two ways. First, it simplifies the task of securing complex space missions by focusing on securing lower-level components, instead of tackling the complexity of the entire system. This approach makes the problem more tangible for system designers. Second, our approach generates concrete and detailed technical requirements instead of just providing guidelines. This makes it easier to integrate into the existing system engineering process for space missions.

B. Flexibility of the approach

Our approach is highly flexible in several ways. First, it adapts to various definitions of a "low-level component" within the system, whether at the hardware level or a higher level of abstraction like functions or services. For example, the star tracker component, which includes both hardware and firmware elements, and the spacecraft's C&DH system, which may be analyzed as a single functional component, are accommodated as per context.

Second, secure blocks can be tailored to the unique requirements of each mission. Whether it's a low-budget scientific CubeSat mission or a critical military spacecraft, our approach enables mission-specific integration of security measures.

Finally, the approach is inherently extensible to adapt to evolving technologies and changing mission parameters. As space and the threat landscape evolve, the secure blocks can be easily revised, replaced, or reconfigured, ensuring the approach remains resilient and effective against emerging challenges.

C. Scalability of the approach

As discussed earlier, a one-size-fits-all approach does not suit the diversity of space missions. Our strategy, based on the concept of secure blocks, offers scalability to adapt to different mission scopes and complexities. For instance, consider a billion-dollar Mars mission with thousands of components across ground, link, and space segments. Now, consider another billion-dollar mission to Jupiter's moon with similar complexity but distinct objectives. While their architectural configurations differ, both these missions might share lower-level components like a star tracker or a C&DH component. Our modular strategy allows the independent development of secure blocks, which can then be selected and arranged to fit a mission's unique requirements, creating a bespoke architecture for optimal security. Furthermore, our approach scales to encompass components across the user, space, link, and ground segments, addressing inter-segment interactions and dependencies as captured during the attack surface analysis. This holistic strategy tackles the challenges inherent in securing complex system-of-systems.

D. Verification and Validation

By decomposing systems into secure, independently verifiable building blocks, the secure-by-component strategy simplifies the security verification and validation of the overall system. Furthermore, the clear specification of security properties within each secure block facilitates the construction of robust assurance cases to demonstrate its ability to meet intended security objectives. This makes it easier for projects to validate and integrate secure blocks developed by external vendors and partners, including increasingly used commercial off-the-shelf (COTS) systems.

E. Application of the strategy within the IEEE Standard

As mentioned previously, the secure-by-component design strategy presented in this paper is central to the forthcoming IEEE International Technical Standard on Space System Cybersecurity [20], [21]. The standard will focus on applying this strategy to several common low-level components found within the user, space, ground, and link segments of space missions. The output of this technical standard will be the creation of a catalog of secure blocks for space missions. As part of our future work, the standard will also include appropriate guidance for designers to choose the right level of security requirements for their system, including rigorous definitions for minimum and maximum standards for security. This catalog will encompass in-depth technical requirements for the components, which can be integrated into the developmental phases of the system development cycle.

F. Adapting the strategy to individual organizations

Space organizations, including companies, can readily embrace the proposed strategy and, if desired, integrate it alongside the IEEE standard, customizing both to suit the specific requirements of their organization. For instance, an organization could develop a library of secure blocks tailored to the specific nature of the missions it undertakes. This customization ensures that the secure blocks are directly relevant to the organization's unique mission profiles and needs.

G. Applying the strategy to other domains

The secure-by-component strategy, initially designed for securing space missions, seamlessly scales to other complex system-of-systems like the Smart Grid, airplanes, and autonomous systems. These systems face similar security challenges and can benefit from our approach. It is entirely conceivable to develop technical standards for these domains using the secure-by-component strategy to create customized catalogs of domain-specific secure blocks.

H. Integration with a top-down approach

While our strategy emphasizes practicality, flexibility, and scalability, it's important to clarify that secure building blocks alone do not guarantee an overall secure system. Our bottom-up approach assists system engineers in defining detailed security requirements for low-level components. However, this needs to be combined with (a) consideration of secure architectures and engineering practices, and (b) a top-down approach that considers the security priorities of a specific mission. Established secure architectures, such as those outlined in CCSDS [36] and system security engineering practices such as those outlined in ECSS [37] would complement this approach.

We present a methodology that combines a top-down, mission-centric system engineering approach with our bottom-up secure-by-component approach. We summarize our approach here and refer readers to Falco et al. [35] for a comprehensive discussion.

- *Identify high-level failure modes*: We begin by identifying critical failure modes, such as "permanent loss of spacecraft control" for a particular mission.
- *Perform fault tree analysis:* Using the identified failure mode, we perform a fault tree analysis. This involves identifying low-level components across all five segments (space, user, ground, link, and integration) that could contribute to the top-level failure if compromised. These components can vary in abstraction depending on the specific system.

- *Identify threat techniques and weaknesses:* We then shortlist the specific threat techniques that could compromise these low-level components, leading to top-level failure. These techniques are mapped to Common Weakness Enumerations (CWEs), which are then mapped to secure-by-design principles to address those weaknesses in the lower-level components.
- *Customized secure block requirements:* This process results in a set of principles and requirements for the secure building blocks, customized to the mission's context.

VII. Conclusion

A fundamental challenge in securing space systems involves developing a secure-by-design strategy that is pragmatic, flexible, and scalable, taking into account the complexity, diversity, and unique aspects of each mission. To address these challenges, we introduced *secure-by-component*, a design strategy for thinking about secure-by-design for complex system-of-systems such as space missions. This strategy yields *secure blocks*, which are fundamental secure elements that can be combined in various configurations to create security architectures tailored to each mission's specific requirements. We illustrated this approach using the example of a space system's star tracker component. We discussed how our strategy complements top-down, mission-centric, system engineering approaches to create requirements tailored to mission contexts. We further discussed the benefits of our strategy, how it simplifies verification and validation, and how other system-of-systems could adapt it. Our strategy is central to the upcoming IEEE International Technical Standard for Space System Cybersecurity. We envision our approach not only enhancing security but also establishing a foundation for resilience, ensuring future space missions are well-equipped to face the ever-evolving threat landscape.

Acknowledgement

A portion of this research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration (80NM0018D0004). We acknowledge Nicolò Boschetti for the "lego" conceptualization of the secure-by-component strategy, as shown in the bottom-left corner of Figure 1. We also acknowledge the members of the IEEE P3349 working group for various discussions and insights.

References

[1] K. Zetter, "Report: Hackers seized control of computers in nasa's jet propulsion lab," 2012.
[2] J. Francis, "Briefing 8: Ghostsec hackers target satellite networks via gnss receivers," 2023.
[3] USCC, "2011 Report to Congress," *112th Congress*, 2011.
[4] J. A. Guerrero-Saade and M. Van Amerongen, "AcidRain - A Modem Wiper Rains Down on Europe," 2022.
[5] T. Malik, "Elon musk says spacex focusing on cyber defense after starlink signals jammed near ukraine conflict areas," 2022.
[6] Center for Strategic and International Studies (CSIS), "Space Threat Assessment 2023," 2023.
[7] Defense Intelligence Agency (DIA), "Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion," 2022.
[8] Consultative Committee on Space Data Systems (CCSDS), "Security Architecture for Space Data Systems," 2012.
[9] ——, "Security threats against space missions," February 2022.
[10] Office of the NASA Chief Engineer, "Space System Protection Standard," 2022.
[11] Federal Office for Information Security (BSI), "IT-Grundschutz profile for Space Tnfrastructures," 2022.
[12] Japanese Ministry of Economy, Trade and Industry, "Cybersecurity guidelines for commercial space systems," 2023.
[13] "European cooperation for space standardization (ecss)," https://ecss.nl/, 2023, accessed: 19 Jan 2024.
[14] NASA, "Space Security: Best Practices Guide (BPG)," October 2023.
[15] U.K. National Cyber Security Center, "Secure by Default," November 2018.
[16] K. Nienhuis, A. Joannou *et al.*, "Rigorous engineering for hardware security: Formal modelling and proof in the cheri design and implementation process," in *IEEE Symposium on Security and Privacy*. IEEE, 2020, pp. 1003–1020.
[17] National Institute of Standards and Technology (NIST), "Engineering trustworthy secure systems," Nov. 2022.
[18] ——, "Developing cyber-resilient systems: A systems security engineering approach," Nov. 2022.
[19] P. G. Neumann, "Toward Total-System Trustworthiness," June 2022.
[20] G. Falco, W. Henry *et al.*, "An international technical standard for commercial space system cybersecurity-a call to action," in *ASCEND 2022*, 2022, p. 4302.
[21] IEEE P3349 Working Group, "IEEE Standard for Space System Cybersecurity," https://sagroups.ieee.org/3349/, To be published in 2025.
[22] National Institute of Standards and Technology (NIST), "Nist 800-53 rev.5: Security and privacy controls for information systems and organizations," 2020.
[23] Committee of National Security Systems (CNSS), "Security Categorization and Control Selection for National Security Systems," 2021.
[24] National Institute of Standards and Technology (NIST), "NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations," July. 2023.
[25] ——, "NISTIR 8441: Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)," September 2023.
[26] B. Unal, "Cybersecurity of NATO's Space-based Strategic Assets," Chatam House - International Security Department, July 2019.
[27] Cybersecurity and Infrastructure Security Agency (CISA), "Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software," Oct. 2023.
[28] A. Shostack, "Threat Modeling: Designing for Security," https://shostack.org/books/threat-modeling-book, 2014.
[29] The Aerospace Corporation, "SPARTA: Space Attack Research and Tactic Analysis," https://aerospace.org/sparta, 2022.
[30] MITRE, "MITRE ATT&CK Framework," https://attack.mitre.org/.
[31] ——, "MITRE ATT&CK ICS Matrix," https://attack.mitre.org/matrices/ics/.
[32] ——, "MITRE ATLAS Framework," https://atlas.mitre.org/.
[33] ——, "MITRE FiGHT Framework," https://fight.mitre.org/, 2023.
[34] ——, "MITRE D3FEND Framework," https://d3fend.mitre.org/.
[35] G. Falco, N. Boschetti, A. Viswanathan *et al.*, "Minimum Requirements for Space System Cybersecurity - Ensuring Cyber Access to Space," in *IEEE SMCIT*, 2024.
[36] Consultative Committee on Space Data Systems (CCSDS), "Space Communications Cross Support - Architecture Requirements Document," 2015.
[37] European Cooperation for Space Standardization (ECSS) Secretariat, "Space engineering – security in space systems lifecycles," 2024.