Critical Software

Report - Cybersecurity Survey

CYBERSECURITY FOR SPACE

CONTRACT REFERENCE: NOT APPLICABLE.

DATE: 2024-07-31
PROJECT CODE: CSEC4SPACE
DOC. REF.: CSW-2024-TNR-03904
STATUS: APPROVED
PAGES: 41
INFORMATION CLASSIFICATION: PUBLIC
VERSION: 1.1

DISCLAIMER -

The work described in this report was performed under the Master's degree research titled "Cybersecurity for space domain". Responsibility for the contents resides in the author or organization that prepared it.

PARTNERS:

Polytechnic University of Coimbra

APPROVAL

VERSION	NAME	FUNCTION	SIGNATURE	DATE
1.1	Nuno Silva	Industry Supervisor		2024-07-31
1.1	João Carlos Cunha	Academic Supervisor		2024-07-31

AUTHORS AND CONTRIBUTORS

NAME	DESCRIPTION	DATE
Pedro Miguel Sousa	Author	2024-06-07
Nuno Silva	Reviewer	2024-07-31

COPYRIGHT

REVISION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR
0.1	2024-06-07	First revision of the technical note.	Pedro Sousa
1.0	2024-07-31	Updated the report contents with the review feedback. Document approved for delivery.	Pedro Sousa
1.1	2024-11-16	Minor update.	Pedro Sousa

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1. INTRODUCTION

Our reliance on space-based technologies continues to expand, making safeguarding these applications against cyber threats paramount. It's no longer just a matter of technological prowess but a critical element in preserving the integrity, functionality, and security of space missions.

Cybersecurity has emerged as a key focus in space software development and operations in recent years. This is reflected in the ongoing updates to software development and verification and validation (V&V) standards.

For example, the European Cooperation for Space Standardization (ECSS) has been actively incorporating cybersecurity requirements into the set of European Space Standards. This is particularly evident in the upcoming versions of ECSS-E-ST-40 and ECSS-Q-ST-80, which will include a significant number of cybersecurity-related requirements and outputs.

1.1. OBJECTIVE

This reports aims to depict the perspectives of space engineers on the vulnerabilities and threats faced by space systems, along with potential mitigation strategies and solutions to address the identified/known cybersecurity threats. Ultimately, the survey's goal was to contribute to the development of more secure space systems and this report provides the essential outcomes of the “Cybersecurity challenges and solutions for space systems” survey.

This report’ objective is also to share the collected information with the research and engineering communities to better tackle the cybersecurity challenges that lie ahead of the space domain (and other similar critical systems domains).

1.2. SCOPE

This study focuses on cybersecurity vulnerabilities, threats, and mitigation strategies within space systems. The scope encompasses the three primary segments of space systems:

- **Space Segment**: This includes physical components like satellites, launchers, rovers, and probes.
- **Ground Segment**: This encompasses launchpad control facilities, ground stations, control centres, and associated databases.
- **User Segment**: This covers user/operator terminals and related databases.

The study also considers communication links between these segments (**Link Segment**) as an integral part of the system. Furthermore, it includes both hardware and software components, along with their configurations, throughout the development and operational phases of the systems.

1.3. AUDIENCE

The audience of this report includes: Critical Software S.A., Coimbra Institute of Engineering, and Engineers/Researchers interested in the field of cybersecurity.

1.4. DEFINITIONS AND ACRONYMS

Table 1 presents the list of definitions used throughout this document.

NAME	DESCRIPTION
Availability	Ensuring timely and reliable access to and use of information.

NAME	DESCRIPTION
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Attack Vector	Attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server to deliver a payload or malicious outcome.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, and confidentiality.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Infrastructure	Critical infrastructure refers to the systems, facilities and assets that are vital for the functioning of society and the economy.
FuzzTesting	Fuzz testing or fuzzing is an automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
PenTest	Penetration Testing, a security test that launches a mock cyberattack to find vulnerabilities in a computer system.
Quid Pro Quo Attack	A quid pro quo attack is a type of baiting method. However, instead of trying to get someone to fall for something out of their own curiosity or fear, cyber actors offer them something in return.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Threat Actor	Threat actors, also known as cyberthreat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems by exploiting vulnerabilities in computer systems, networks and software.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Reference Document	A document is considered a reference if it is referred but not applicable to this document. Reference documents are mainly used to provide further reading.

Table 1: Definitions

Table 2 presents the list of acronyms used throughout this document. The acronyms presented in [AD-1] are also applicable.

ACRONYM	DESCRIPTION
AI	Artificial Intelligence
AOCS	Attitude and Orbit Control System operations
ASAT	Anti-Satellite
CRC	Cyclic Redundancy Check
CSF	Cybersecurity Framework
CSW	Critical Software, SA
CCSDS	Consultative Committee for Space Data Systems
CLC	CENELEC
COTS	Commercial-Off-The-Shelf
CWE	Common Weak Enumeration
CyBOK	Cybersecurity Body of Knowledge
DDOS	Distributed Denial of Service
ECSS	European Cooperation for Space Standardization
EITCA	European IT Certification Academy
EOS	Earth Observation Satellite
ESA	European Space Agency
FAA	Federal Aviation Administration
FDIR	Fault Detection, Isolation, and Recovery
FMEA	Failure Mode and Effects Analysis
FTP	File Transport Protocol
GPS	Global Positioning System
ID	Identification
IP	Internet Protocol
ICD	Interface Control Document
ISA	International Society of Automation
ISO	International Organization for Standardization

ACRONYM	DESCRIPTION
IEC	International Electrotechnical Commission
ISS	International Space Station
ISMS	Information Security Management System
ISVV	Independent Software Verification and Validation
JAXA	Japan Aerospace Exploration Agency
JPL	Jet Propulsion Laboratory
MITRE	Massachusetts Institute of Technology Research Establishment
ML	Machine Learning
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OWASP	Open Worldwide Application Security Project
OSS	Open-Source Software libraries
SANS	SysAdmin, Audit, Network and Security
S/C	Spacecraft
SAT	Satellite
STD	Standard
STIX	Structured Threat Information Expression
USB	Universal Serial Bus
SP	Special Publication
SDLC	Secure Development Life Cycle
TC	Telecommand
TM	Telemetry
TUV	Technischer Überwachungsverein
V&V	Verification and Validation

Table 2: Acronyms

1.5. DOCUMENT STRUCTURE

Section 1 (Introduction) presents this document.

Section 2 explores the current landscape of cybersecurity threats and vulnerabilities in space systems.

Section 3 showcases specific examples of cyberattacks targeting space infrastructure and discusses potential vulnerabilities.

Section 4 details the design and development of the survey used to gather data.

Section 5 analyses and presents the findings obtained from the survey.

Section 6 outlines recommendations and strategies for addressing the identified cyber threats in space systems.

Section 7 summarizes the key findings and reiterates the report's main points.

Appendix A provides a complete list of the survey questions used for the research.

1.6. REFERENCE DOCUMENTS

Table 3 presents the list of reference documents.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-1] Microsoft Forms – Survey on Cybersecurity challenges and solutions for space systems	https://forms.office.com/Pages/DesignPageV2.aspx?origin=NeoPortalPage&subpage=design&id=3k5T2LIZX0KB90mjtcu_CD84rRRVFchOvwBdlmX7k2lURTNVVkQ4TVVXMElTT0RUSE1DMksyV1lCUi4u, visited on 2024-05-21.
[RD-2] VICE – The Mystery of the Creepiest Television Hack	https://www.vice.com/en/article/pgay3n/headroom-hacker, visited on 2024-05-21.
[RD-3] Falco, Gregory & Boschetti, Nicolò. (2021). A Security Risk Taxonomy for Commercial Space Missions	A Security Risk Taxonomy for Commercial Space Missions (researchgate.net), visited on 2024-05-21.
[RD-4] Falco, Gregory. (2018). Cybersecurity Principles for Space Systems. Journal of Aerospace Information Systems	Cybersecurity Principles for Space Systems (researchgate.net), visited on 2024-05-21.
[RD-5] Researchgate – Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight	Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight (researchgate.net), visited on 2024-05-21.
[RD-6] Spacesecurity – Space Attacks Open Database Project	https://www.spacesecurity.info/en/space-attacks-open-database/, visited on 2024-06-05.
[RD-7] Yumpu – Satellite Hacking: A Guide for the Perplexed	https://www.yumpu.com/en/document/read/38464408/satellite-hacking-a-guide-for-the-perplexed-international-, visited on 2024-06-05.
[RD-8] TN04 – Space System Threats and Vulnerabilities	CSW-2024-TNR-01468, v. 1.0
[RD-9] Via Satellite – Satellite Operators Respond to Cyber Threats in a Rapidly Changing Environment	https://interactive.satellitetoday.com/via/october-2022/satellite-operators-respond-to-cyber-threats-in-a-rapidly-changing-environment/, visited on 2024-06-05.
[RD-10] The Maritime Executive – Mass GPS Spoofing attack in Black Sea?	https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea,visited on 2024-06-05.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-11] Resilient Navigation and Timing Foundation – GPS Jammer Delays Flights in France.	https://rntfnd.org/2017/09/15/gps-jammer-delays-flights-in-france/, visited on 2024-06-05.
[RD-12] VICE – It´s Surprisingly Simple to Hack a Satellite	https://www.vice.com/en/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite, visited on 2024-06-05.
[RD-13] The Register – German Space Center Endures Cyberattack	https://www.theregister.com/2014/04/15/dlr_attacked_china_apt_trojans/, visited on 2024-06-05.
[RD-14] Via Satellite – Satellite Operators Respond to Cyber Threats in a Rapidly Changing Environment	https://interactive.satellitetoday.com/via/october-2022/satellite-operators-respond-to-cyber-threats-in-a-rapidly-changing-environment/, visited on 2024-06-05.
[RD-15] Expert insights – The Most Significant Password Breaches of 2021	https://expertinsights.com/insights/the-most-significant-password-breaches/, visited on 2024-06-05.
[RD-16] NIST – The CSF 1.1 Five Functions	https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions, visited on 2024-06-05.
[RD-17] MITRE – ATT&CK	https://attack.mitre.org/, visited on 2024-06-05.
[RD-18] MITRE - Engage	https://engage.mitre.org/defenders/, visited on 2024-06-05.
[RD-19] MITRE - Defend	https://engage.mitre.org/defenders/, visited on 2024-06-05.
[RD-20] MITRE - Caldera	https://caldera.mitre.org/, visited on 2024-06-05.
[RD-21] MITRE - STIX	https://stix.mitre.org/language/version1.1.1/, visited on 2024-06-05.
[RD-22] MITRE – Common Weakness Enumeration	https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html, visited on 2024-06-05.
[RD-23] OWASP Foundation	https://owasp.org/, visited on 2024-06-05.
[RD-24] University of Bristol – CyBOK	https://www.cybok.org/knowledgebase1_1/, visited on 2024-06-05.
[RD-25] NIST CSF	https://www.nist.gov/cyberframework, visited on 2024-06-05.
[RD-26] ECSS-E-ST-40C - Software	https://ecss.nl/standard/ecss-e-st-40c-software-general-requirements/, visited on 2024-06-05.
[RD-27] ECSS-Q-ST-80C – Software Product Assurance	https://ecss.nl/standard/ecss-q-st-80c-rev-1-software-product-assurance-15-february-2017/, visited on 2024-06-05.
[RD-28] ISA/IEC 62443 Series of Standards	https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards, visited on 2024-06-05.
[RD-29] ISO/IEC 27000 Family – Information Security Management	https://www.iso.org/standard/70918.html, visited on 2024-06-05.
[RD-30] NASA Standards	https://standards.nasa.gov/, visited on 2024-06-05.

Table 3: Reference documents

2. BACKGROUND

Advancements in technology, particularly in computing with smaller sizes, lower energy demands, and increased processing power, have led to a significant rise in the number of satellites orbiting Earth. This, in turn, has elevated the likelihood of cyberattacks.

Figure 1 illustrates this trend. The red line shows the exponential growth in the number of operational satellites between 1958 to 2018, with the red numbers on the top and right axis representing the years and the corresponding number of satellites. The blue bars represent the number of satellites cyberattacks. Both datasets exhibit a substantial leap around the year 2000, coinciding with the widespread adoption of the internet in organizational IT, or, in other words, the surge in digitalization.

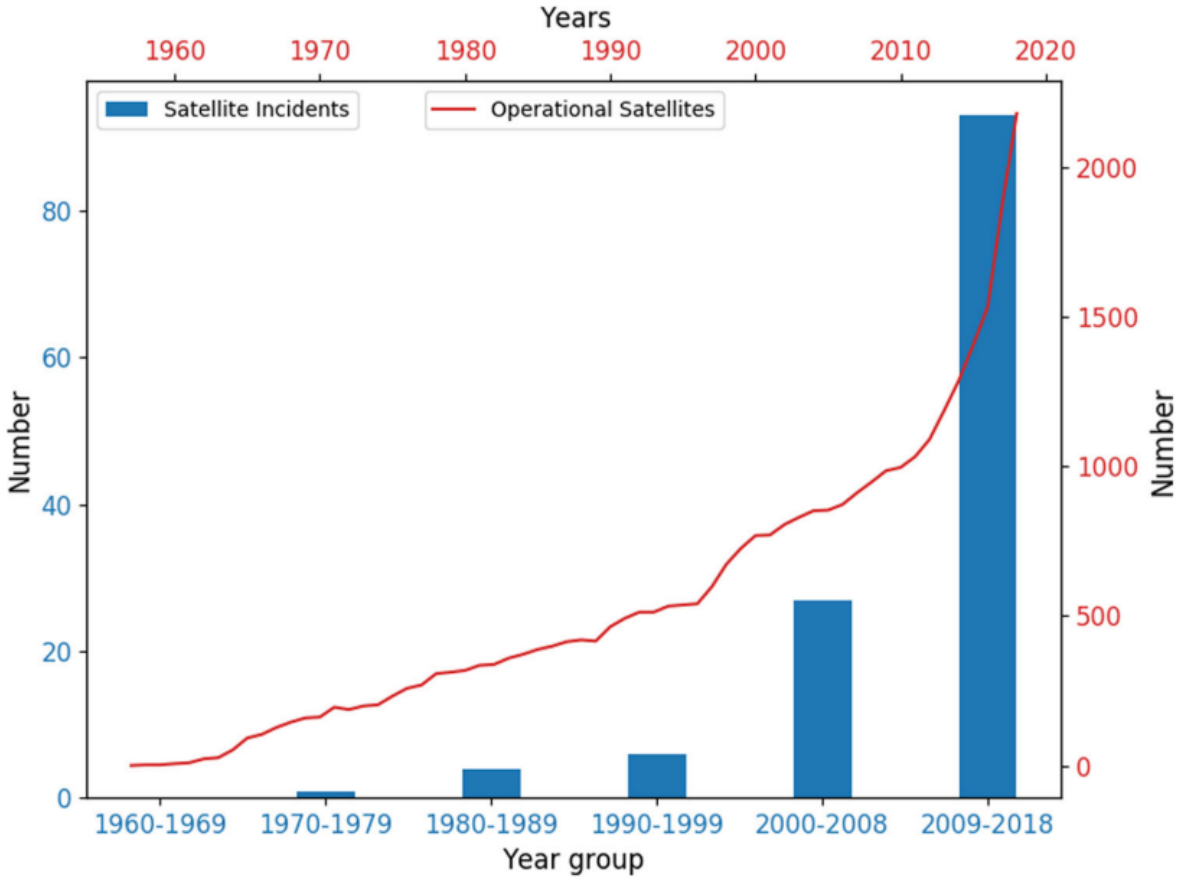

Figure 1: Number of satellites attacks and number of operational satellites [RD-5]

Despite considerable efforts to enhance cybersecurity for critical infrastructure on Earth, space systems have become a relative blind spot. While terrestrial infrastructure receives increasing cybersecurity focus, space systems have been largely overlooked. This neglect stems from several key factors:

- **Misguided Perception of Security**: Initially, a perception existed that space systems were too complex or remote for attackers to target. This perception, however, has proven to be misguided as cyber threats to space systems become increasingly real.
- **Prioritization in the Space Industry**: The rapid expansion of private companies in the space industry has prioritized rapid development and affordability. This focus on speed and cost-effectiveness may have inadvertently led to a lower emphasis on robust cybersecurity measures.
- **Challenges of Legacy Systems**: Upgrading legacy systems, which have been operational for a long time, adds another layer of complexity. Modernizing these systems can be expensive and technically challenging.

- **Gaps in Standards and Enforcement**: Two key gaps hinder effective cybersecurity in space systems. First, there's no established method to enforce the use of existing cybersecurity standards within the space industry. Second, there's a lack of dedicated standards specifically tailored to address the unique risks faced by space systems.
- **Complex supply chain**: Space systems comprise numerous components, and the space program often utilizes a multi-layered contract structure. Lower-tier companies (subcontractors) specializing in technology manufacture their products which are then sent to the prime contractor, responsible for managing procurement and integrating all system components. This supply chain complexity extends beyond physical aspects to encompass cybersecurity considerations.

3. ATTACKS AND VULNERABILITIES OF CYBERSECURITY FOR SPACE SYSTEMS

A literature analysis revealed numerous cyberattacks with severe impacts on the different space architecture segments mentioned in section 5.7. As illustrated in Figure 2, the number of attacks targeting these three segments has grown by decade, from 1980 to August 15, 2020.

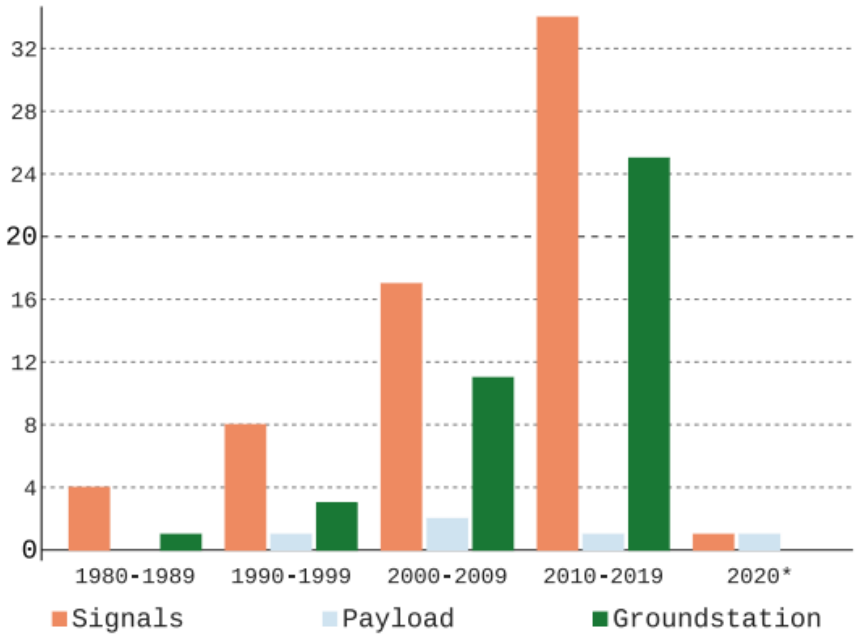

Figure 2: Attacks on space architecture [RD-5]

The following cyberattack examples are grouped by target segments. For a more comprehensive list of attacks, access the “Space Attacks Open Database” maintained by a group of researchers [RD-6]:

Space Segment:

- **2008 Terra EOS AM-1 Hijacking**: In 2008, the Terra EOS AM-1 Earth observation satellite was hijacked twice for short durations. While believed to be the work of Chinese hackers, no commands were reportedly issued to the satellite [RD-4].
- **2008 ISS attack**: In 2008, unconfirmed reports of a trojan horse infecting a computer system at the Johnson Space Centre which provide an uplink to the ISS to attackers, disrupting several systems on board. This was aided by the out-of-date software in use onboard the ISS [RD-7].

Ground/User Segment:

- **2014 German Space Center Attack**: In 2014, the German space research center in Cologne was compromised by a malware attack targeting researchers' machines working on sensitive technologies. The malware included self-destructing Trojans and dormant programs for potential later activation [RD-13].
- **2017 APT33 Supply Chain Attack**: A 2017 attack by the Iranian group APT33 targeted organizations in various sectors, including aviation and energy. They used spear phishing emails with malicious attachments to gain access to systems [RD-27]. This incident highlights the importance of strong cybersecurity practices.
- **2021 SolarWinds Attack**: The 2021 SolarWinds supply chain attack is another reminder of cyber vulnerabilities. Hackers are believed to have gained access through a weak password used by an intern [RD-15].
- **2022 Viasat KA-SAT Ground Station Attack**: At the beginning of the invasion of Ukraine by Russia, an attack targeted Viasat's KA-SAT ground station. This attack compromised tens of thousands of modems across Ukraine and parts of Europe, disrupting critical services [RD-14].

Link Segment:

- **2007 Turla Data Exfiltration**: In 2007, a Russian group called Turla used satellite internet signals to exfiltrate data from malware infections. By using a ground antenna, they could detect user IP addresses and initiate connections with minimal traceability [RD-4].
- **2015 Iridium Satellite Vulnerability**: Researchers demonstrated a potential vulnerability in the Iridium satellite communication system in 2015. They were able to analyse and potentially access readable information within Iridium pager traffic [RD-12].
- **2017 GPS Spoofing Attack**: In 2017, the U.S. Maritime Administration reported a GPS spoofing attack targeting ships in the Black Sea. The attack disrupted navigation systems, causing ships to lose their location data [RD-10].
- **2017 Nantes Airport Jamming**: An unusual case of jamming occurred in 2017 at Nantes Airport in France. A parked car with an operational GPS jammer caused interference with aircraft tracking systems and flight delays [RD-11]. While not a sophisticated attack, it highlights the potential risks of readily available jamming devices.

Some of the attacks identified below were made possible due to the fact of serious vulnerabilities remained undetected or were left unpatched. The following examples represent vulnerabilities that enabled such attacks:

1. **Access Control Vulnerabilities**: These vulnerabilities arise from weaknesses in managing access to critical systems and data. This could include inadequate password policies, a lack of multi-factor authentication, or improper user privilege management. A successful exploit could allow unauthorized individuals to take control of a system, steal sensitive data, or disrupt operations.
2. **Verification & Validation (V&V) Vulnerabilities**: Inadequate V&V processes during software development can leave security flaws undetected. This could involve incomplete code reviews, insufficient testing of security features, or overlooking potential attack vectors. Unidentified vulnerabilities can be exploited by attackers to compromise the functionality or integrity of space systems.
3. **Communication Link Encryption/Protection Vulnerabilities**: Weak encryption or lack of proper security measures for communication links between ground stations and space systems can expose sensitive data in transit. This could allow attackers to eavesdrop on communications, manipulate transmitted data, or even inject malicious commands.
4. **Open-Source Software/Libraries/Operating Systems/COTS Vulnerabilities**: Integrating open-source components or readily available COTS solutions can introduce vulnerabilities if their security posture is not thoroughly assessed and managed. Unpatched vulnerabilities in these components can be exploited by attackers to gain unauthorized access to space systems.

4. SURVEY PREPARATION PROCESS

As the survey aimed to capture feedback from space engineers on cyber threats, vulnerabilities, and mitigation strategies, the questions were crafted around these three key aspects. It was crucial to ensure the questions were carefully constructed, highly specific, and easy to answer. This is because survey participation can be limited (due to respondents' availability), and the objective was to encourage serious and thoughtful responses.

A first version of the survey was created using Microsoft Excel. This version consisted of seven questions. Each question was accompanied by a rationale to facilitate understanding for the respondents. The questions addressed the following topics:

- Identification of up to five cyber threats.
- Identification of up to five vulnerabilities.
- Identification of both technical and procedural mitigation strategies.
- Standards and other cybersecurity resources used.
- Selection of the space segment most vulnerable to cyberattacks.
- Anticipated future cybersecurity concerns and trends affecting the space sector.

To assess the survey's structure and completion time, a pilot test was conducted internally at Critical Software. Initial feedback regarding the survey structure was positive. The time to complete the survey was approximately 30 minutes, as expected. However, some confusion arose concerning the rationale for questions 3 and 4, which focused on technical and procedural mitigations. Respondents had difficulty distinguishing between the two concepts. To address the confusion around technical and procedural mitigations (questions 3 and 4), the survey was revised. Following a thorough review, the definitive version, detailed in Annex A, was ready for distribution to the participants of the survey.

To enhance accessibility and user experience, the survey was migrated from Microsoft Excel to Microsoft Forms. This transition made the survey more visually appealing and easier to complete.

A targeted list of potential participants was created, consisting primarily of European space engineers. This approach leveraged Critical Software's collaboration history with the European Space Agency (ESA) and helped contacting individuals from ESA to take part. Additionally, the survey was sent to participants from NASA JPL, JAXA and Brazil, for example.

To broaden participation further, the survey link was made publicly available on LinkedIn for anyone interested in responding. The following text is the publication made on LinkedIn.

"Help Shape the Future of Space Cybersecurity!

Hi Space Domain Experts, Pedro Sousa, a Master's student at ISEC, Polytechnic of Coimbra, Portugal is conducting a thesis research on cybersecurity challenges and solutions for space systems, in collaboration with Critical Software (Dr. Nuno Silva) and supported by Professor @João Carlos Cunha (ISEC).

Your expertise is valuable! We are seeking your insights through a short 30-minute survey to understand the current landscape and future directions of space cybersecurity.

Why should you participate?
-> Help Shaping the future: Your insights will directly contribute to the research and influence the development of secure space systems.
-> Stay informed: You'll receive a copy of the survey report for a unique perspective on the space industry's cybersecurity landscape.
-> Confidentiality assured: All responses are completely anonymous, protecting your individual and institutional information.

Who should participate?

This survey is particularly relevant for anyone with expertise in:

-> Space systems engineering
-> Cybersecurity
-> Aerospace industry
-> Satellite communications

Join the discussion by completing the survey:

Online: https://lnkd.in/dPcVJQdj
Deadline (Extended): March 8th, 2024

If you know someone who might be interested, please share this message!

Feel free to contact us if you have any questions.

Thank you very much!

hashtag#cybersecurity hashtag#security hashtag#spacetechnology hashtag#criticalsystems hashtag#research hashtag#survey hashtag#spaceindustry hashtag#spacestandards hashtag#criticalsoftware hashtag#isec

P.S. Share this post with your network to help reach more experts!"

5. SURVEY RESULTS

This section delves into the key areas explored by the survey questions.

5.1. OVERVIEW OF RESULTS

The survey received a total of 21 responses from space engineers over a period of 5 months, between February 1, 2024, and June 1, 2024. The originally planned closing date was extended due to a lower-than-anticipated response rate. The average time to complete the survey was 21 minutes.

A variety of responses were provided for each question, with the number of different answers ranging from 19 for standards and resources to 39 for technical mitigations.

- **Perceptions of Vulnerabilities and Threats**: Engineers named a diverse range of potential vulnerabilities (35) and threats (33) to space systems.
- **Mitigation Strategies**: Respondents offered a broad spectrum of technical mitigation strategies (39) and processual mitigation strategies (31) to address identified vulnerabilities and threats.
- **Most Vulnerable Segment**: The ground segment was perceived as the most vulnerable to cyberattacks, with 20 respondents selecting it. Link and space segments received 2 and 12 votes, respectively.
- **Future Cybersecurity Concerns**: Engineers expressed various concerns and predicted trends about future cybersecurity challenges in the space sector, with 19 different responses provided.

5.2. VULNERABILITIES

Table 4 presents the 35 vulnerabilities identified by the experts, sorted from most frequently mentioned to the least frequent. The categorization of each vulnerability was based on the Common Weakness Enumeration (CWE) list. However, it's important to note that not all categorizations will achieve complete consensus. Therefore, these classifications should be considered a **preliminary attempt to organize** the vulnerabilities using a standardized taxonomy. Note: The “Response Frequency %” column represents the percentage of respondents that mentioned each listed vulnerability.

#	Answers	Response Frequency %	Category
1	**Access control vulnerabilities**: this may lead to unauthorized access to sensitive information. e.g. (1) during system development or during S/C (Spacecraft) flight operations. (2) neglect the design of ground-on-board protocol to prevent unauthorized access. (3) missing authentication in the Ground Operation System, in which untrained people can access the facilities, command functions in satellite, and access sensitive data.	38.10	•CWE-287 - Improper Authentication
2	**V&V vulnerabilities - most of testing is done blindly based on traces to requirements and not based on a proper testing strategy.** e.g. cover extra situations, performance, stress, volume, security situations, combinations, not necessarily stated in the requirements. (2) **Test campaigns not sufficiently covering requirements and beyond**, out of bounds and unspecified cases. (3) **Insufficient / incomplete testing activities** (not only having interfaces, code coverage or requirements coverage-based tests, but ensure security-based tests and coverage of all possibilities) (4) **Prioritizing speed over thoroughness in the validation process** can lead to incomplete testing. (5) **do not test conditions that prevent the on-board system** to receive erroneous TCs. (6) **non reporting of abnormal situations** during testing.	33.33	•Several

#	Answers	Response Frequency %	Category
3	**Communication link encryption/protection vulnerabilities**	28.57	•CWE-311 - Missing Encryption of Sensitive Data CWE-327 - Use of a Broken or Risky Cryptographic Algorithm CWE-326 - Inadequate Encryption Strength
4	**Open-source software/libraries/Operating Systems/COTS vulnerabilities**	28.57	•CWE-1395 - Dependency on Vulnerable Third-Party Component CWE-1357 - Reliance on Insufficiently Trustworthy Component
5	**Software design not protected against fuzzed inputs**	19.05	•CWE-20 - Improper Input Validation
6	**Reuse of software/system not thoroughly tested or trusted wrongly.** e.g. (1) lead to strange problems such crashes, hands, buffer overflow.	19.05	•Several
7	**Use of tools that are not mature enough for software development, testing.** (e.g. static code analysis tool)	19.05	•Several
8	**Software bugs with security impacts.** e.g. (1) bugs in code that lead the system to execute commands (in ground station) and/or telecommands (on-board of satellite) that open access to malicious attacks. (2) Hidden backdoors in application deployment	19.05	•CWE-94: Improper Control of Generation of Code ('Code Injection')
9	**Lack of basic security services in the space segment** (e.g. lack of basic authentication and access control, lack of any form of partitioning or segmentation of functions)	19.05	•CWE-276: Incorrect Default Permissions
10	**Using of weak/sloppy development process** (e.g. Agile methodologies should be forbidden, analysis, requirements, design, implementation, testing)	14.29	•NVD-CWE-Other
11	**Read and write operations in memory (stack overflow)**	14.29	•CWE-657 - Violation of Secure Design Principles
12	**Insufficient safety and security analysis done in the initial phases** (prior to requirements baseline) (1) **poor requirements** (2) **Lack of security assessment and analysis** to derive requirements	14.29	•CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
13	**Overly complex software/system.** (1) **Bad design**, when people do not do design and instead generate it from code that might be flawed.	14.29	•CWE-657 - Violation of Secure Design Principles
14	Software updates: **S/C systems allow software updates during its lifetime**. This way, **hackers might inject malicious code** that can lead to the system failure, to spy flight data, or even to affect/destroy other missions.	14.29	•Several
15	**Software development environments not protected** enough (allowing to get access to key Software artifacts)	9.52	•Several
16	**Debug ports not protected** (e.g. Access to the target memories through debug ports)	9.52	•Several
17	**Ignore code smells and other code rules violations** provided by commercial static analysis tools.	9.52	•CWE-284: Improper Access Control
18	**Updates and Operations phase- lack of tests to verify the stability of a modification and impact on the rest of the system/components/functions,** which will lead to patches and updates that might cause problems in the future (side problems not	9.52	•CWE-710: Improper Adherence to Coding Standards

#	Answers	Response Frequency %	Category
	easily identifiable during installation); **lack of operator training due to incomplete user/operation manual** (for example not referring to the limitations of the system + security problems/precautions)		
19	**Acceptance - No security acceptance plan exists,** usually acceptance is based on a subset of the tests, and tests, as we all know are not necessarily covering security and odd situations (this also represents a contractual limitation because the subcontractor needs to have specific scope defined and will hide contractually behind that while affecting security, yes, this is also a vulnerability, contracts represent a vulnerability because they will "lead" to only do what is written...) (2) accepting based on already provided test results by the supplier, instead of going deep into an acceptance set of activities (audit, documentation scrutiny, independent assessment/V&V, and specific tests for security situations)	9.52	•Several
20	**Installation -** incorrect or modified versions installed, virus on installation machines, informal patches installed, lack of verification of the installed system… (2) incomplete configurations during uploading on-board software, telecommand lists, or during storing payload data in cloud storage banks. (3) leaving undesired installations or configurations, lack of installation logs and records	9.52	•NVD-CWE-Other
21	**Documentation, Code, Electronic ICDs and database contents** are **shared** between official entities with resource to **unusual communication means or through 3rd party providers** (e.g.: email, SharePoint, FTP).	4.76	•CWE-922 - Insecure Storage of Sensitive Information
22	**Possibility to inject failures**	4.76	•CWE-754 - Improper Check for Unusual or Exceptional Conditions
23	Not secure **boundary parameters**	4.76	•CWE-754 - Improper Check for Unusual or Exceptional Conditions
24	**Hardware devices access poorly protected or no protected at all.**	4.76	•CWE-287 - Improper Authentication
25	**Weak passwords policies**	4.76	•CWE-287 - Improper Authentication
26	**Use of outdated languages, tools and libraries.**	4.76	•NVD-CWE-Other
27	**High turnover of contractors** - opportunities for attacks of social engineering	4.76	•NVD-CWE-Other
28	**Bad design**, when people do not do design and instead generate it from code that might be flawed.	4.76	•CWE-94 - Improper Control of Generation of Code CWE-657 - Violation of Secure Design Principles
29	**Updates and Operations -** open ports or interfaces, giving too much functionality for the operator (in operations manuals)	4.76	•CWE-284: Improper Access Control
30	**Use dynamic memory in space systems.**	4.76	•Several
31	**Deserialization of untrusted data**	4.76	•CWE-345 - Insufficient Verification of Data Authenticity CWE-913 - Improper Control of Dynamically Managed Code Resources
32	**Integer overflow of wraparound**	4.76	•CWE-682 - Incorrect Calculation

#	Answers	Response Frequency %	Category
33	**Improper/insufficient monitoring of the ground and space segments for anomalies and attacks.**	4.76	•CWE-223: Omission of Security-relevant Information
34	**Lack of training/awareness in cybersecurity subjects** (for management, development/technical, and installation, maintenance, and operations).	4.76	•NVD-CWE-Other
35	**Poor management of the exchanged data** between ground and space segments. (1) **Limit the amount** of telecommands received in batch.	4.76	•CWE-269: Improper Privilege Management

Table 4: Vulnerabilities identified

The experts Top 5 most often cited vulnerabilities are:

- **Access control vulnerabilities:** These vulnerabilities exploit weaknesses in the mechanisms that control access to systems and data.
- **Verification and validation (V&V) vulnerabilities:** These vulnerabilities stem from flaws in the processes used to ensure that systems meet their intended requirements.
- **Communication link encryption/protection vulnerabilities:** These vulnerabilities compromise the encryption or protection mechanisms safeguarding communication links between space and ground segments.
- **Open-source software/libraries/operating systems/COTS (Commercial-Off-The-Shelf) vulnerabilities:** These vulnerabilities reside within software components obtained from external sources, including open-source libraries, operating systems, and COTS products.
- A set of 5 vulnerabilities tied in 5th place: **Software design not protected against fuzzed inputs, Reuse of software/system not thoroughly tested or trusted wrongly, Use of tools that are not mature enough for software development, testing, Software bugs with security impacts, Lack of basic security services in the space segment.**

Beyond the top five vulnerabilities, the survey identified other noteworthy issues that deserve further exploration.

One critical concern raised by the experts (Item 34) is the need for a strong cybersecurity culture across not just the space sector, but also in other critical sectors. This can be achieved through training programs that raise awareness of cybersecurity best practices and empower personnel to act as the first line of defence against cyberattacks.

The survey also suggests a potential vulnerability associated with using agile methodologies for critical systems (Item 10). Experts raised concerns about the evolving nature of requirements in agile development, which could introduce vulnerabilities if not carefully managed.

Finally, the importance of clear and comprehensive user and installation manuals was highlighted (Items 18 & 20). Poorly written documentation can lead to misconfigurations and improper use, potentially creating openings for malicious actors to exploit vulnerabilities within the system. These points emphasize the need for a holistic approach to cybersecurity that goes beyond simply identifying and patching technical flaws.

5.3. THREATS

Table 5 presents the 33 threats identified by the experts, sorted from most frequently mentioned to the least frequent. The categorization of each threat was based on the taxonomy proposed by Gregory Falco and Nicolò Boschetti in their paper [RD-3] and the Technical Note 04 Space System Threats and Vulnerabilities [RD-8].

#	Answers	Response Frequency %	Category
1	**Jamming of** communications channel/Satellite.	42.86	Electromagnetic - Man-Made
2	**Malware and ransomware**	23.81	Cyber - Technical
3	**Distributed Denial of Service** (DDOS)	23.81	Cyber - Technical
4	**The middle-man threats** in ground operations of space asset (e.g. bad configuration management on the flight parameters of Ariane 5 took the satellite into wrong orbit which caused the use of fuel to correct the orbit with the consequent reduction in satellite lifetime).	19.05	Cyber - Technical
5	**Data being stolen on ground stations** (e.g. USB ports used to steal data and introduce virus/trojans).	19.05	Cyber - Technical
6	**Space weather/solar storms**	14.29	Electromagnetic - Environmental
7	Hacking into space networks (**eavesdropping**) seems to be quite impossible, but in here one could divide the security problem between the uplink (sending telecommands (TC)) and the downlink (receiving telemetry (TM)). For the uplink, it will be difficult to bypass the encryption units normally onboard, besides the need to have a tracking ground station and other physical problems, but satellite orbits are public and you can build your own tracking GS (see Satnogs project). For the **downlink you can always try to decode the information received from the spacecraft specifically if it is not encrypted**.	14.29	Electromagnetic - Man-Made
8	**Insider attacks** (1) **Attacking the development/validation environment** with the objective of introducing undetected vulnerabilities/bugs. (2) **Software patch to exclude commandability** from correct ground station.	14.29	Cyber - Technical
9	**Spoofing** (1) Sending malicious TCs/TMs to/from spacecraft/ground segment. (2) Third parties sending commands to satellite.	14.29	Cyber - Technical
10	**Tampering with source code/ binary to introduce accidental or malicious code** that could either prevent the correct operation or could allow unauthorized parties to interact with the SW.	9.52	Cyber - Technical
11	**Supply chain attacks**	9.52	Organizational - Management
12	Network vulnerabilities are also a threat since most of the space systems collect data that ends up somewhere on earth for further processing. The data is quite important and expensive and should not be lost or hijacked. **Cloud security and other types of security measures could be under threat.**	4.76	Cyber - Technical
13	**Change the S/C configuration** (e.g., switch on or off equipment, switch a camera off in a moment when it should shoot a specific target, change S/C direction, grab the wrong target (ClearSpace-1), change FDIR configurations, removing detection mechanism)	4.76	Cyber - Technical
14	**Hijacking** S/C (AOCS operations) and change its direction.	4.76	Cyber - Technical
15	**Identity theft** (cc)	4.76	Cyber - Social Engineering
16	**Bad design**, when people do not do design and instead generate it from code that might be flawed	4.76	Cyber - Technical
17	**Speed up development / pressure** - not doing things properly like design, code analysis, testing, will always leave issues in the final product	4.76	Organizational - Management

#	Answers	Response Frequency %	Category
18	**Lack of certification of space system**s (not that FAA certification or TUV for railways are perfect, but they try)	4.76	Regulatory - Legal
19	**No Software vulnerabilities analysis / Threats analysis** are performed before closing the system and software requirements that they should actively contribute too (like a FMEA for cybersecurity)	4.76	Cyber - Technical
20	**Malicious states agents**	4.76	Organizational - Production
21	Keyboards, especially wireless keyboards may be **logging keystrokes** and transmitting them, similar for screens.	4.76	Cyber - Technical
22	**Stealing of IP** (working from home)	4.76	Cyber - Technical
23	**Stealing of encryption keys**	4.76	Cyber - Technical
24	**Electromagnetic Pulse**	4.76	Electromagnetic - Man-Made
25	**Blinding sensors by Lasers**	4.76	Physical - Non-Kinetic
26	**ASAT testing**	4.76	Physical - Kinetic
27	**Electronic warfare in the outer space.**	4.76	Electromagnetic - Man-Made
28	**Exploiting development tools**	4.76	Cyber - Technical
29	**Unmitigated errata**	4.76	Cyber - Technical
30	**Electronic attacks against space-based services at the transmission site, the satellite, and the user' s equipment.**	4.76	Electromagnetic - Man-Made
31	**Physical attacks against actual launchers, satellites, and spacecrafts.**	4.76	Physical - Kinetic

Table 5: Threats identified

Figure 3 illustrates the distribution of threats across various categories identified by space engineers. Analysis of this data reveals that the "Cyber-Technical" category holds the most relevance compared to others. This emphasis likely stems from the fact that cyber-technical threats directly target vulnerabilities within the software, hardware, and communication systems of space assets. This highlights the critical need for tailored cybersecurity standards specifically designed for space systems.

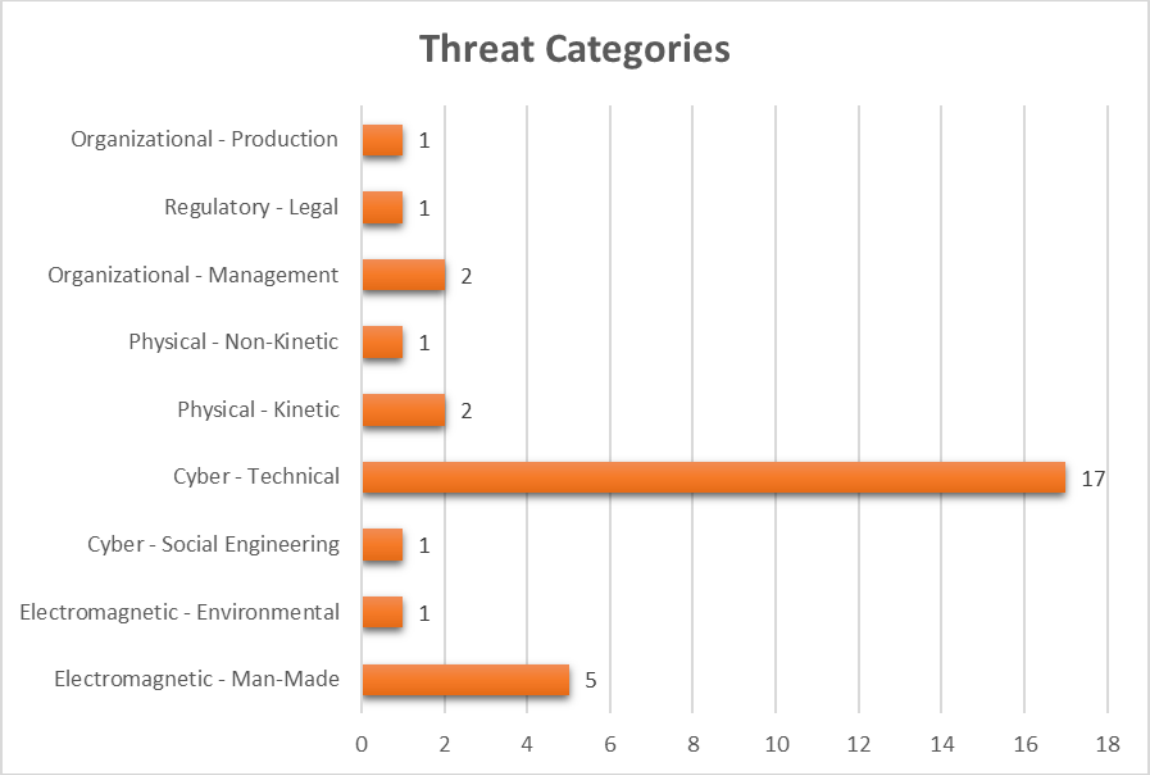

Figure 3: Threat categories

The experts Top 5 most often cited threats are:

- **Jamming of communication channels/satellites**: This threat involves disrupting communication between space and ground systems.
- **Malware and ransomware**: These are malicious software programs that can damage, encrypt, or steal data from space or ground systems.
- **Distributed Denial-of-Service (DDoS) attacks**: These attacks overwhelm systems with traffic, making them unavailable to legitimate users.
- **Man-in-the-middle attacks during ground operations**: This threat involves attackers intercepting or modifying communication between ground stations and space assets.
- **Data theft from ground stations**: This threat involves unauthorized access and exfiltration of sensitive data from ground stations.

While the top five vulnerabilities stood for the most often mentioned concerns, the survey also showed other interesting threats.

One such concern is the pressure to speed up development processes (Item 17). While efficiency is desirable, sacrificing critical steps like security testing can have severe consequences. Rushing through development can lead to security vulnerabilities that may manifest as costly mission failures. This can also contribute to poorly designed systems (Item 16), further undermining overall security.

Interestingly, the survey results showed a relatively low frequency of mentions regarding supply chain attacks. This is somewhat surprising given the inherent complexity of the space sector's supply chain, with numerous components moving through various stages before satellite construction.

5.4. TECHNICAL MITIGATIONS

Table 6 presents the 39 technical mitigations identified by the experts, sorted from most frequently mentioned to the least frequent. The categorization of each mitigation technique was based on the five functions of the NIST Cybersecurity Framework [RD-16]:

- **Identify**: focuses on understanding the systems, assets, data, and threats that an organization needs to protect. It involves activities like asset discovery and inventory, data classification, and identification of potential vulnerabilities.
- **Protect**: implementing safeguards to deter, prevent, or mitigate the impact of cyberattacks. Common protective measures include secure configurations, data encryption, access controls, and network segmentation.
- **Detect**: activities that help identify and report security incidents in a timely manner. It encompasses security monitoring, anomaly detection, log analysis, and intrusion detection systems.
- **Respond**: procedures for acting in response to a security incident. It includes activities like containment, eradication, remediation, and recovery.
- **Recover**: focuses on restoring systems and data to a functional state after a security incident. It involves activities like data backup and restoration, disaster recovery planning, and business continuity exercises.

#	Answers	Response Frequency %	Category
1	Advanced **encryption** in the communication link and data storage.	52.38	Protect
2	**Extensive code analysis** (static analysis with cybersecurity rules)	23.81	Protect
3	**Intrusion detection mechanisms** and tools (1) Monitoring and anomaly detection (2) **Robust FDIR configuration** that could detect and recover from injected failures	19.05	Detect
4	**Proper authentication methods and access control**	14.29	Protect
5	**CRCs for all data transmission.** e.g. (1) In transmissions that involve sending information in multiple TCs/TMs, implement a Checksum that applies to all the data transmitted as a whole (e.g., checksum for a file that was transmitted in multiple TCs/TMs).	14.29	Protect
6	**Secure-by-design approach** (Zero trust solutions)	14.29	Protect
7	**Protect routing and distribute controls**, considering Inter-Satellite Links (ISLs) routing. e.g. (1) **Give an ID to every entity in the system** and **validate** that the communication is being performed between allowed entities.	9.52	Protect
8	**Firewall**	9.52	Protect
9	**Strong password policies**	9.52	Protect
10	**Penetration testing** (e.g. Explicit penetration testing of exposed systems and interfaces)	9.52	Protect
11	**Zero code smells and zero warnings objective** (from static analysis tools)	9.52	Protect
12	**Secure Protocols to protect attacks during uploads and downloads.** (1) **Handshake protocols** between ground and satellite.	9.52	Protect

#	Answers	Response Frequency %	Category
13	**Telecommands acceptance is subject to validation** by either SW or HW, which reduces or eliminates most attempts of commanding by unauthorized parties.	4.76	Detect
14	**Periodically change the CRC/checksum/cryptography algorithms** being used.	4.76	Protect
15	**Use of certified tools** (Software development processes can look for SW vulnerabilities within the code being developed, using static analysis tools and other type of SW assisted tools with proper certifications).	4.76	Identify
16	**Usage of secure hardware**	4.76	Identify
17	**Protection of software development environments**	4.76	Protect
18	**Authentication on software patch**	4.76	Protect
19	**Protect debug port** accessed	4.76	Protect
20	**Defensive programming** of the embedded software	4.76	Protect
21	**Extensive V&V** of the embedded device **against fuzz inputs**	4.76	Protect
22	**Enforce patch management**	4.76	Protect
23	**HW tokens for key storage**	4.76	Protect
24	**Plan and strategy to ensure the security best practices,** for example by having technical activities to ensure OWASP top 25 are assessed	4.76	Protect
25	**Specific security assessment of the design/code** (for example with tools such as Absint or Astrée) and fixing of the deviations (soon in the process and not only at the end) - report also the results of these analysis to the customer	4.76	Protect
26	**Built-in or self-tests** to **ensure application and data integrity**	4.76	Detect
27	**Better languages and libraries.**	4.76	Identify
28	**Network segmentation**, protecting ground assets.	4.76	Protect
29	**Availability insurance** under extreme conditions.	4.76	Protect
30	**Accept telecommands** and download telemetry **only when flying above certain regions.**	4.76	Protect
31	**Radio transmitters operate in different frequencies.**	4.76	Protect
32	**Avoid equipment from foreign sources (untrusted sources)**, especially in key components: networks, keyboards, screens, storage.	4.76	Identify
33	Use **cryptographic keys** instead of passwords.	4.76	Protect
34	**Advanced interference mitigation, e.g. with filters**	4.76	Respond
35	**Use security zones in the architecture and prevent data flows**	4.76	Protect

#	Answers	Response Frequency %	Category
36	**Perform input validation**	4.76	Detect
37	**Integrity checks for all data, configurations, inputs to the system**	4.76	Detect
38	**Regular updates for ground systems**	4.76	Protect
39	**Redundance in ground systems to avoid operation disruption**	4.76	Protect

Table 6: Technical mitigations identified

Figure 4 illustrates the distribution of cybersecurity mitigations across various categories based on the NIST Cybersecurity Framework. The "Protect" category is the most prominent, accounting for 29 responses, followed by "Detect" with 5 mentions. This data suggests a strong emphasis on implementing preventative safeguards against cyberattacks, while also highlighting the importance of mechanisms to identify such attacks if they occur.

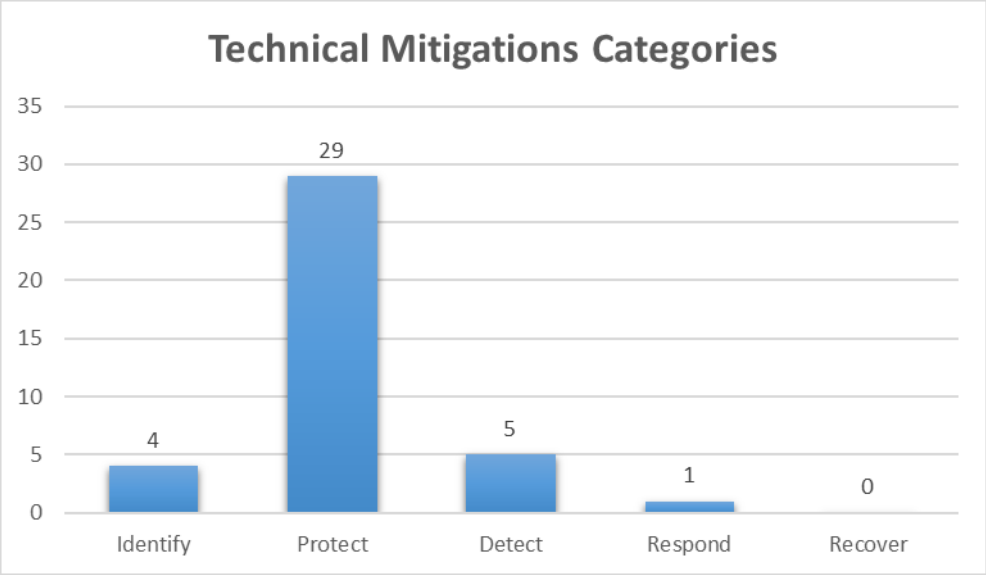

Figure 4: Technical mitigations categories

The survey data revealed the following top 5 most frequently cited technical mitigations identified by experts:

- **Advanced Encryption in Communication Links and Data Storage**: This emphasizes the importance of robust encryption to protect data confidentiality during transmission and while at rest.
- **Extensive Code Analysis** (Static Analysis with Cybersecurity Rules): This highlights the need for thorough code review using automated tools configured with cybersecurity best practices to find potential vulnerabilities.
- **Intrusion Detection Mechanisms and Tools**: This underscores the importance of implementing systems that can detect and alert security personnel to suspicious activity on the network.
- **Proper Authentication Methods and Access Control**: This emphasizes the need for strong authentication mechanisms to verify user identities and restrict access to systems and data based on proper permissions.
- **Secure-by-Design Approach** (Zero Trust Solutions): This highlights the importance of building security into the system from the very beginning, adopting a "zero trust" approach that assumes no user or device is inherently trustworthy and requires verification before granting access.

The survey also identified other valuable technical mitigations beyond the top 5. One such example is the importance of having a comprehensive plan and strategy to ensure ongoing adherence to security best practices

(Item 24). This strategy could involve utilizing resources like the OWASP Top 10 (a well-known list of web application security risks), maintaining an up-to-date vulnerability database, and employing tools to prevent the introduction of known vulnerabilities into new programs.

The survey also suggests a potential benefit in transitioning away from passwords and adopting cryptographic keys, often referred to as passkeys (Item 33). Passkeys leverage a combination of public key cryptography and biometrics (fingerprint, facial recognition) to provide secure authentication without the need to remember or manually enter complex passwords. This approach aims to eliminate the risk of weak or reused passwords and enhance overall security.

5.5. PROCEDURAL MITIGATIONS

Table 7 presents the 31 procedural mitigations identified by the experts, sorted from most frequently mentioned to the least frequent. The categorization of each mitigation technique was based on the five functions of the NIST Cybersecurity Framework [RD-16]:

- **Identify**: focuses on understanding the systems, assets, data, and threats that an organization needs to protect. It involves activities like asset discovery and inventory, data classification, and identification of potential vulnerabilities.
- **Protect**: implementing safeguards to deter, prevent, or mitigate the impact of cyberattacks. Common protective measures include secure configurations, data encryption, access controls, and network segmentation.
- **Detect**: activities that help identify and report security incidents in a timely manner. It encompasses security monitoring, anomaly detection, log analysis, and intrusion detection systems.
- **Respond**: procedures for acting in response to a security incident. It includes activities like containment, eradication, remediation, and recovery.
- **Recover**: focuses on restoring systems and data to a functional state after a security incident. It involves activities like data backup and restoration, disaster recovery planning, and business continuity exercises.

#	Answers	Response Frequency %	Category
1	**Enforcing security standards** (in satellite and ground systems)	33.33	Protect
2	**Security testing** (PenTest, FuzzTesting, Out-of-bounds, equivalence class partitioning test, buffer overflow, DoS tests, simulated attacks)	23.81	Protect
3	**Awareness trainings** to the developers (e.g. phishing, ransomware, and malware etc.)	23.81	Identify
4	**Conducting independent regular security audits**	23.81	Protect
5	**Ensure a SDLC (Secure Development Life Cycle) is integrated in the application development**	23.81	Protect
6	**Training on security aspects** considered within the different **domains and standards.** (1) **Training on V&V** of embedded systems from a hacker perspective. (2) **Training on security aspects** when **designing embedded systems**.	23.81	Identify
7	**Security requirements to be specified as early as possible** to avoid and detect potential vulnerabilities. These vulnerabilities might force design or architecture changes. For that reason, the soon the better.	14.29	Protect

#	Answers	Response Frequency %	Category
8	(1) **Check of OSS libraries** and other third-party SW for SW **vulnerabilities**. (2) For integrated components (reuse, OS, used tools, …) **do a deep analysis and test all interfaces** (Zero Trust model)	14.29	Protect
9	**Vulnerability / Threats Analysis done before requirements are closed.** (1) Comprehensive assessment of vulnerability in Satellite Data Centres, particularly to prevent attacks in cloud solutions for data storage	14.29	Protect
10	**(1) Maintenance Plan with security contents** (incident response) (2) **Have user manuals, maintenance, and incident** resolution plans (3) **Cover security in installation/operation/maintenance documentation**	14.29	Protect
11	**More secure information and deliverables flow.**	9.52	Protect
12	**Robustness testing**	9.52	Protect
13	**Every user involved** in activities related to the project shall be **subjected to user authentication. (Zero Trust model)**	4.76	Protect
14	**Errata analysis**	4.76	Protect
15	**Security reviews**	4.76	Protect
16	**Take security lessons learned from other projects/missions/domains** into account.	4.76	Protect
17	**Organizational security culture, resources** (e.g. tools, training, processes, templates) and assessment	4.76	Identify
18	**Restricted/Protected access** to software development tools, developments environments (Secure Development Life Cycle), hardware tools, …	4.76	Protect
19	**Scanning repositories**	4.76	Protect
20	**Hardening machines**	4.76	Protect
21	**Enforce patching**	4.76	Protect
22	**Security scans of nodes**	4.76	Protect
23	**Force baseline migrations**	4.76	Protect
24	**No agile methodology in security critical development**	4.76	Protect
25	**Clearer requirements with rationales -** goal should be simpler more robust software.	4.76	Protect
26	**Shorter feedback loops** to address ISVV findings in timely fashion.	4.76	Protect
27	**Have guidelines to integrate cybersecurity layer with central software interfaces / data processing layer.**	4.76	Protect
28	**Integrate cybersecurity in the validation simulator.**	4.76	Protect
29	**Nominate cybersecurity manager for a project.**	4.76	Protect

#	Answers	Response Frequency %	Category
30	**Simulated attacks sessions with specialists before launch/operations.**	4.76	Protect
31	**Define a set of approved libraries to be used by satellite manufacturers.**	4.76	Identify

Table 7: Procedural mitigations identified

Figure 5 depicts the distribution of processual mitigations across the NIST Cybersecurity Framework categories. Like the technical mitigations, the "Protect" category is the most prominent, with 27 responses. However, unlike the technical mitigations where there was a wider range of responses across categories, most of the remaining responses here fall under "Identify."

This data suggests a strong emphasis on two key areas:

- **Implementing preventative safeguards against cyberattacks** (aligned with the high number of responses in the "Protect" category).
- **Improving the understanding of cybersecurity risk management from an organizational perspective**. This includes managing risks to systems, people, assets, and data. By strengthening this understanding, organizations can prioritize efforts to build a robust risk management strategy that aligns with their business needs.

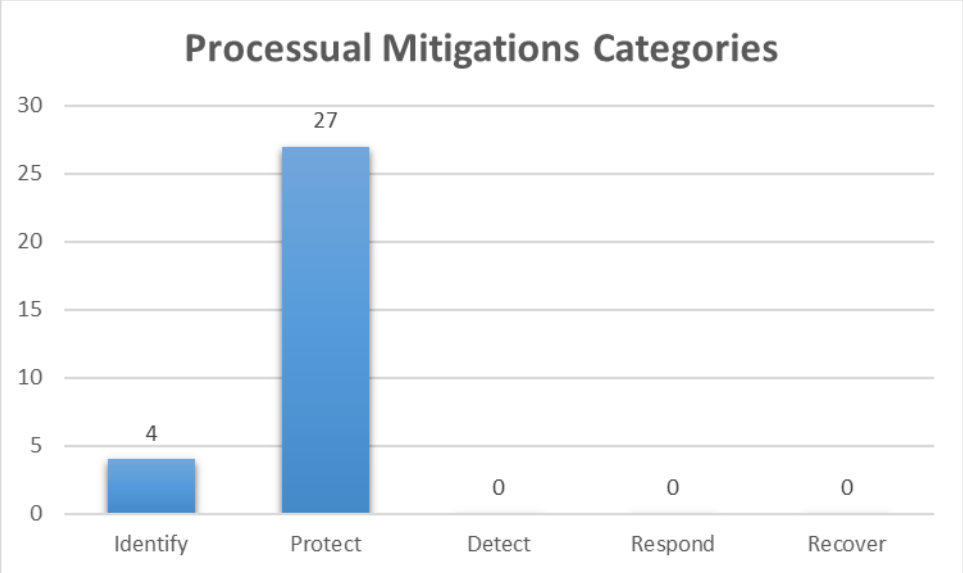

Figure 5: Processual mitigations categories

The survey data revealed the following top 5 most frequently cited processual mitigations identified by experts:

- **Enforcing Security Standards**: This emphasizes the importance of implementing and enforcing robust security standards across both satellite and ground systems.
- **Comprehensive Security Testing**: This highlights the need for a variety of security testing methods, including penetration testing, fuzz testing, out-of-bounds testing, equivalence class partitioning testing, buffer overflow testing, denial-of-service testing, and simulated attack scenarios.
- **Developer Security Awareness Training**: This underscores the importance of providing developers with regular security awareness training to educate them on current threats like phishing, ransomware, and malware, and how to develop secure code.
- **Independent Regular Security Audits**: Regular independent security audits conducted by qualified personnel are crucial for finding potential vulnerabilities in systems and processes.

- **Secure Development Lifecycle (SDLC) Integration**: This emphasizes the importance of integrating a secure development lifecycle (SDLC) methodology into the application development process. An SDLC incorporates security best practices throughout the development stages to find and mitigate vulnerabilities early on.

Beyond the top five most frequently cited processual mitigations, the survey identified some other interesting findings from the experts.

One noteworthy suggestion (Item 7) highlights the importance of clearly defining security requirements early and often throughout the project lifecycle. This helps to avoid discovering vulnerabilities later in the development process when they can be significantly more expensive and time-consuming to fix. Early detection allows for adjustments to the project architecture as needed, minimizing potential disruption and cost.

Another interesting point (Item 8) is the importance of thoroughly assessing third-party software for vulnerabilities before integrating it into projects. This involves avoiding unfamiliar software, components, and tools, and conducting deep analysis and testing to ensure their security.

Finally, Item 29 underscores the value of having a dedicated cybersecurity specialist on a project team. This dedicated individual can champion security best practices, ensure their implementation, and proactively identify and address potential security risks.

5.6. STANDARD AND RESOURCES

Table 7 presents the 19 cybersecurity standards and other resources identified by the experts, sorted from the most frequently mentioned to the least frequent. The categorization was done by separating the standards, procedures, tools and other resources.

#	Answers	Response Frequency %	Category
1	NIST (CSF, SP 800)	28.57	Standards/Norms
2	ESA (E40, Q80 + Handbook)	28.57	Standards/Norms
3	IEC 62443 (for control systems)	19.05	Standards/Norms
4	ISO 27000 Family (27001 and 27002)	19.05	Standards/Norms
5	NASA (STD-8739.8B, STD-2601, STD-1006A, among others)	14.29	Standards/Norms
6	CWE Top 25	14.29	Other Resources
7	MITRE tools - ATT&CK, Engage, D3FEND, CALDERA	9.52	Tools
8	CCSDS	4.76	Standards/Norms
9	CLC/TS 50701	4.76	Standards/Norms
10	ISO 21434	4.76	Standards/Norms
11	DO-326 (aviation cybersecurity)	4.76	Standards/Norms
12	Railways EN50129 and EN50701	4.76	Standards/Norms
13	SEI secure coding standards	4.76	Standards/Norms
14	SANS CWE Top 10	4.76	Other Resources
15	CyBOK	4.76	Processes

#	Answers	Response Frequency %	Category
16	EITCA/IS IT Security Academy	4.76	Standards/Norms
17	CLOUD SECURITY ALLIANCE	4.76	Standards/Norms
18	**Cryptography techniques** - Handshake, private key exchange, identification of persons with challenges, etc.	4.76	Processes
19	OWASP resources	4.76	Other Resources

Table 8: Cybersecurity standard and other resources

Figure 6 depicts the distribution of cybersecurity resources identified by space engineers according to four main categories: Standards/Norms, Processes, Tools and Other Resources.

- **Standards/Norms**: This category received the most mentions, showing a strong emphasis on adhering to proven cybersecurity guidelines and best practices specifically tailored for the space sector. Examples include recent revisions to ESA's E40 and Q80 standards to incorporate cybersecurity aspects, and NASA's STD-8739.8B and STD-2601 standards.
- **Processes**: One of the processes mentioned is CyBOK (Cybersecurity Body of Knowledge) [RD-24], a project by the University of Bristol that catalogs existing cybersecurity knowledge to enhance accessibility and education within the cybersecurity community.
- **Tools**: This category encompasses a variety of cryptography techniques used to protect data at rest (stationary) and in transit, such as handshakes and private key exchange. It also includes a reference to MITRE, particularly the ATT&CK framework [RD-17]. ATT&CK and related tools (Engage [RD-18], D3FEND [RD-19], CALDERA [RD-20], and STIX [RD-21]) provide a knowledge base of adversary tactics, countermeasures, and framework to automated security assessments.
- **Other Resources**: Finally, this category includes references to OWASP resources [RD-23] and top vulnerabilities listed by CWE (Common Weakness Enumeration) [RD-22].

Overall, Figure 6 highlights the importance of a multi-layered approach to cybersecurity in space systems. This approach combines established standards, knowledge resources, and practical tools to address potential threats.

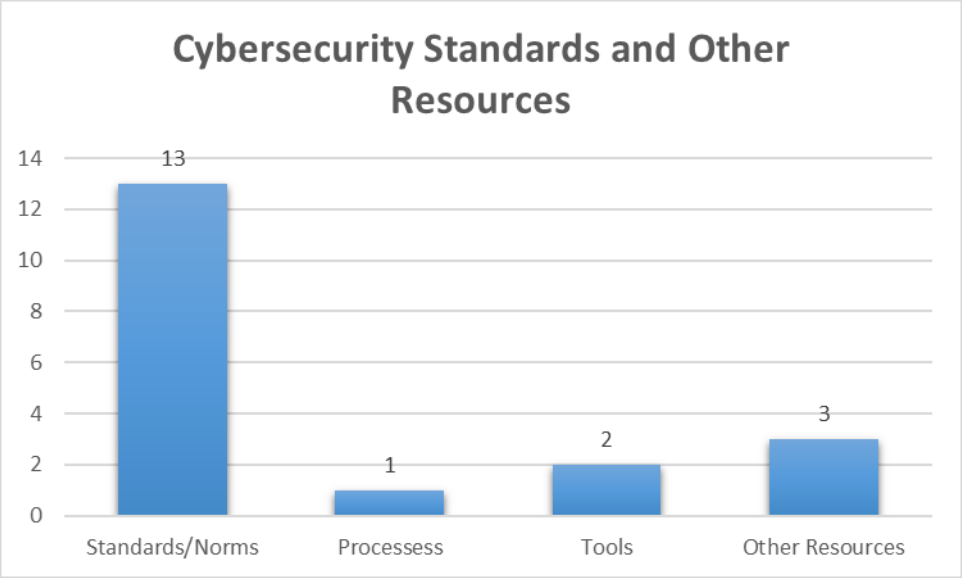

Figure 6: Cybersecurity standards and other resources categories

The survey data revealed the following top 5 most frequently cited cybersecurity standards and resources identified by experts:

- **NIST Cybersecurity Framework** (CSF) [RD-25] and Special Publication 800 (SP 800) series: These resources provide a comprehensive approach to managing cybersecurity risk.
- **ESA standards E40 [RD-26], Q80 [RD-27]**, and accompanying Handbook: These European Space Agency standards focus on space systems and projects.
- **IEC 62443** (for control systems) [RD-28]: This International Electrotechnical Commission standard addresses the specific security needs of industrial control systems.
- **ISO 27000 Family [RD-29]** (including standards 27001 and 27002): This international standard offers a framework for implementing an Information Security Management System (ISMS).
- **NASA standards [RD-30]** STD-8739.8B, STD-2601, STD-1006A, and others: These NASA-specific standards provide guidance for secure software development and secure coding practices.

These standards are a well-rounded selection, covering a variety of industries:

- The inclusion of IEC 62443 shows the importance of specialized standards for control systems.
- The ISO 27000 family provides a comprehensive approach to organizational cybersecurity posture.
- NIST publications are at the forefront of data security through robust cryptographic practices.

It's important to note that the survey also identified relevant standards from other sectors like aviation, automotive, and railway, indicating the growing emphasis on cybersecurity across various industries.

5.7. MOST VULNERABLE SEGMENT

Figure 7 depicts a simplified architecture of a space system. Each component within this architecture is considered a potential attack vector. Additionally, these components are often designed, manufactured, operated, and supported by different entities, introducing supply chain vulnerabilities.

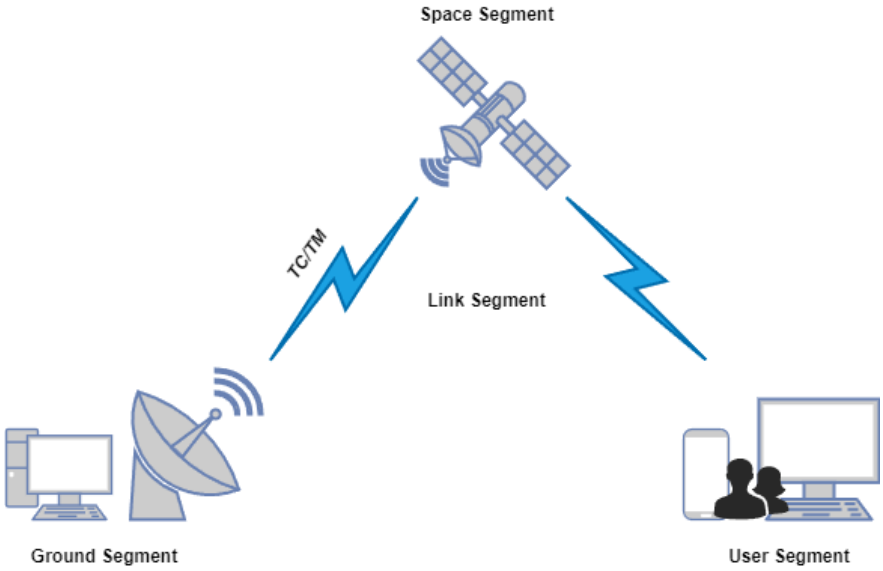

Figure 7: Common space system architecture

It is comprised of four segments: **Ground**, **Link**, **Space**, and **User**. This segmentation is most found in American papers. The European Space Agency (ESA) combines the User and Ground segments into one, resulting in a three-segment system: **Ground/User**, **Link**, and **Space**.

- **Space Segment**: The Space Segment consists of the physical spacecraft itself, orbiting Earth or venturing further out, and houses the dedicated equipment for the mission's purpose, called the payload.

- **Ground Segment**: These ground infrastructures monitor the spacecraft's health and location, analyse the received data, and send commands to control its operations. Launch facilities, where the spacecraft is prepared and launched into orbit, can also be considered part of this segment.
- **Link Segment**: The Link Segment acts as a bridge between the ground and user segments with the space segment. It encompasses the methods used to transmit information between them, primarily relying on communication channels that utilize radio waves of specific frequencies.
- **User Segment**: The User Segment comprises the entities or individuals who ultimately benefit from the data or services provided by the space system. For instance, travellers using GPS for navigation. In literature this segment is sometimes referred as part of the ground segment.

As illustrated in Figure 8, according to the experts, the segment that is considered the most vulnerable to cyberattacks/cyberthreats is the ground segment due to the accessibility and existing interfaces, therefore more exposure exists to all kind of attacks (e.g., social engineering, unauthorized access), followed by the link/signal segment, which can also be access through the first one and that allows control of the satellites or unauthorized access to data.

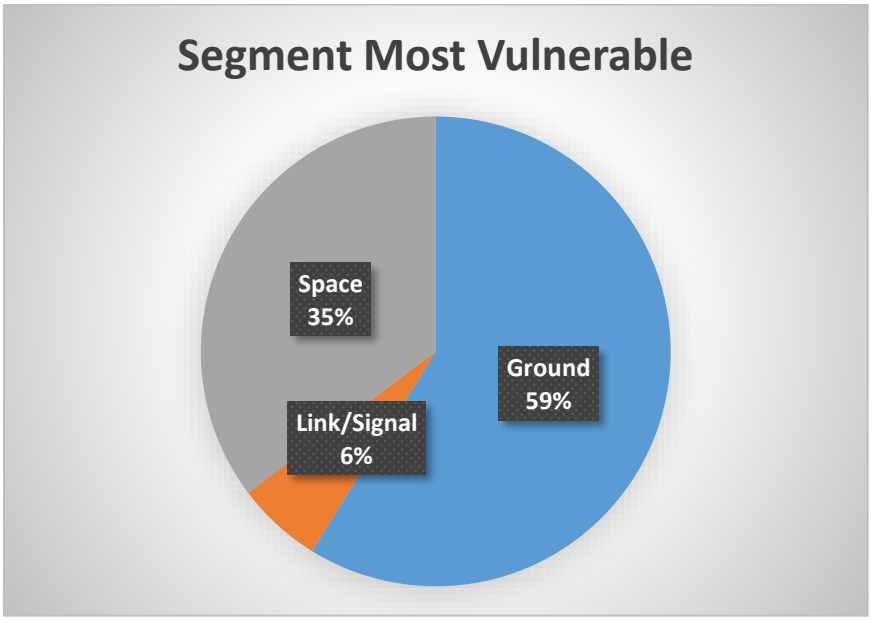

Figure 8: Segment most vulnerable results

5.8. FUTURE CYBERSECURITY CONCERNS/TRENDS

Table 9 presents the 19 cybersecurity concerns and trends identified by the experts, sorted from the most frequently mentioned to the least frequent. The categorization of each concern/trend was developed for this report, as follows:

- Technological Evolution: This category includes concerns related to the rapid pace of technological change and the need for space systems cybersecurity to keep up with these changes.
- Training/Awareness: This category includes concerns related to the need for better training and awareness programs for space system players and other personnel involved in space system development in what concerns cybersecurity impacts.
- Regulatory – Political: This category includes concerns related to the role of government regulations and policies in shaping cybersecurity for space systems.
- Policy: This category includes concerns related to the need for clearer policies and guidelines around cybersecurity for space systems, including issues related to data sharing, incident response, and risk management.

#	Answers	Response Frequency %	Category
1	Artificial Intelligence and Machine Learning use in cyber war.	33.33	Technology Evolution
2	Technical teams' acquaintance with cybersecurity concepts, analyses, and requirements. e.g. (1) Average programmer / architect not informed enough about cybersecurity and cryptography.	14.29	Training / Awareness
3	Political or geopolitical issues, causing cyberwarfare by powerful states/anarchists and climate fundamentalist movements	14.29	Regulatory - Political
4	Space debris and physical attacks (e.g. ASAT)	14.29	Regulatory - Political
5	Cybersecurity certification/legislation might become necessary (as for functional and safety)	9.52	Policy
6	International cooperation (especially in what concerns standards, best practices, methods, and tools)	9.52	Training / Awareness
7	The deployment of cybersecurity measurements may be cumbersome for the developers if not done properly	4.76	Training / Awareness
8	Security risk analysis is very important and needs to be fully documented	4.76	Policy
9	Threats Analysis should be performed and maintained like Hazard Analysis for safety critical systems.	4.76	Policy
10	Security shall be considered as a property of the system, as safety is considered today and thus part of the functional system	4.76	Training / Awareness
11	"Security is not an option" thus appropriate and formal processes need to be in place, as well as standards, testing, assessment…	4.76	Training / Awareness
12	Reuse of code - We tend to reuse more and more code, that sometimes is not developed according to the corresponding standards.	4.76	Policy
13	Autonomous systems	4.76	Technology Evolution
14	Tools need to be developed for both development and especially for testing cybersecurity requirements.	4.76	tools
15	IoT and emerging behaviours will clearly be targeted by hackers	4.76	Technology Evolution
16	We´ll only move forward in cybersecurity assurance when some large accident or incident happen. (reactive attitude)	4.76	Training / Awareness
17	Secure satellite communications (encrypted, protections against DoS, jamming or spoofing)	4.76	Technology Evolution
18	Supply chain security (development and V&V, use of static code analysis, threats and vulnerabilities analysis, use of expert's involvement, e.g. security specialists, security requirements specialists, penetration testers …)	4.76	Policy
19	A specific ECSS standard to deal with cybersecurity, covering: 1. Training and awareness 2. Analysis (threat and vulnerability analysis as contribution to requirements baseline) 3. Security Requirements incorporated in Technical Specifications 4. Secure Design principles 5. Secure Coding (including secure coding rules) 6. Security V&V	4.76	Policy

#	Answers	Response Frequency %	Category
	7. Acceptance/Qualification/Certification 8. Security Updates / Maintenance 9. Documentation 10. Methods / Processes / Tools		

Table 9: Future cybersecurity concerns/trends identified

As illustrated in Figure 9, the survey responses highlight a key concern among space engineers: the need for reinforced training and awareness of cybersecurity. Additionally, there is a strong emphasis on the importance of developing stricter standards that provide clear and robust security requirements.

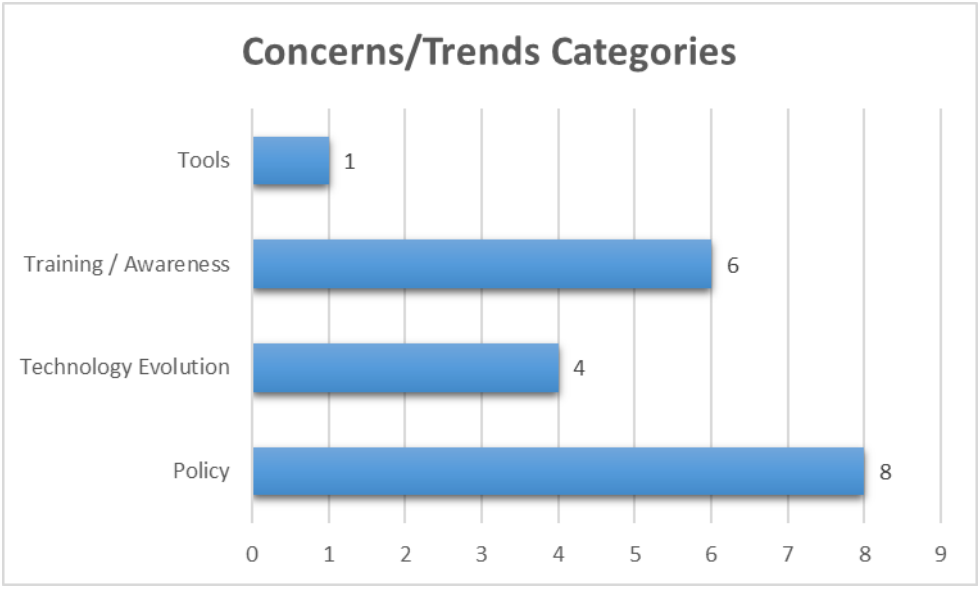

Figure 9: Concerns/Trends categories

The survey revealed a number of key cybersecurity concerns and trends named by space engineers/researchers. The top five most often cited issues are:

- **Integration of Artificial Intelligence (AI) and Machine Learning (ML) into cyberwarfare tactics:** Experts expressed significant concern about the potential use of AI and ML for malicious purposes.
- **Technical teams' lack of familiarity with cybersecurity concepts:** The survey highlighted a need for improved training and awareness of cybersecurity best practices among technical teams. This includes areas like vulnerability analysis, threat mitigation, and secure coding practices. (e.g., Average programmers and architects might not be informed enough about cybersecurity and cryptography).
- **Political and geopolitical motivations for cyberwarfare:** The survey showed concerns about cyberattacks launched by powerful states, anarchist groups, or climate activist movements.
- **Space debris and physical attacks (e.g., Anti-Satellite Weapons):** The possibility of physical attacks on space infrastructure through debris or dedicated anti-satellite weapons was also raised as a concern.
- **Need for stricter cybersecurity regulations and certifications:** Like functional safety standards, experts believe that there may be a need for mandatory cybersecurity certifications or legislation to enforce robust security practices.

The survey identified other interesting issues raised by the experts. One key concern was the need for a specific ECSS standard dedicated to tackling cybersecurity challenges in space systems. This aligns with item 19 of the survey responses, highlighting the importance of establishing clear guidelines to mitigate cyber risks. Additionally,

experts emphasized the need for a cultural shift towards security. Space systems should prioritize cybersecurity as a fundamental property, not an afterthought. This requires integrating security considerations throughout the entire development process, including adhering to established standards and best practices as mentioned in items 10 and 11 of the survey.

6. RECOMMENDATIONS

Space systems are critical infrastructure, yet many governments do not fully recognize them as such, yet. This lack of recognition creates a growing concern about their vulnerability to cyberattacks. Here's a breakdown of key cybersecurity recommendations to fortify these systems:

Technical Safeguards:

- **Encryption Everywhere**: Robust encryption should be implemented throughout the entire space system, protecting data at rest, in transit, and during processing.
- **Code Vulnerability Hunting**: Rigorous code analysis techniques should be employed to find and eliminate vulnerabilities before attackers can exploit them.
- **Intrusion Detection Systems**: Intrusion detection systems should be deployed to continuously check for suspicious activity within the space system.
- **Authentication and Access Controls**: Implement strong authentication methods and granular access controls to restrict unauthorized access to critical components.
- **Ground System Updates and Network Segmentation**: Regularly update ground systems with the latest security patches and implement network segmentation to isolate critical assets from potential threats.

Procedural Protections:

- **Security Standards and Testing**: Enforce well-defined security standards across all space systems. Conduct regular security testing to proactively find and remediate vulnerabilities.
- **Security-Aware Development**: Train developers on secure coding practices and current cyber threats to build security into the system from the ground up.
- **Independent Security Audits**: Schedule regular independent security audits to gain a fresh perspective on potential weaknesses in the system's defenses.
- **Secure Development Lifecycle**: Integrate a secure development lifecycle (SDLC) methodology throughout the development process to proactively address security risks at every stage.
- **Security Culture**: Clearly define security requirements early in the project and set up a culture of security awareness throughout the organization.

Standards and Resources:

- **Industry Standards**: Adhere to proven cybersecurity standards such as the NIST Cybersecurity Framework (CSF) and SP 800 series, ESA's E40 and Q80 standards, and IEC 62443 for control systems.
- **Threat Intelligence**: Use resources like the MITRE ATT&CK framework and the OWASP Top 10 to gain valuable insights into potential threats and best practices for mitigation.

Looking Ahead:

- **Training and Awareness**: Focus on improving training and awareness programs to ensure all technical teams involved with space systems own a strong understanding of cybersecurity concepts.
- **Space System Cybersecurity Standard**: Advocate for the development of a specific ECSS standard dedicated to addressing cybersecurity challenges unique to space systems.
- **Security as a Core Principle**: Promote a cultural shift where security is considered a fundamental property of a space system, embedded throughout the entire development lifecycle.
- **International Cooperation**: Emphasize the need for international cooperation to develop best practices, standards, and tools to combat the ever-evolving landscape of cyber threats.

7. CONCLUSION

This study has confirmed the critical need for robust cybersecurity measures in space systems. The research highlights a concerning reality: real threats and vulnerabilities exist, and they pose a significant risk to these increasingly crucial and critical pieces of infrastructure. By collecting and analyzing realistic threats, vulnerabilities, mitigations, and best practices, this study paves the way for a more secure future for space systems engineering.

The findings underscore the importance of integrating cybersecurity considerations throughout the entire development lifecycle, from the initial design to the verification and validation (V&V). This requires a collaborative effort among stakeholders in the space domain, ensuring critical infrastructure receives the necessary protection.

By acknowledging the evolving nature of cyber threats and the developing field of space cybersecurity, this study emphasizes the importance of ongoing research and collaboration. By managing potential limitations and fostering international cooperation, the space industry can build a future where critical space systems are secure and resilient.

Looking ahead, future work will leverage insights from the cybersecurity literature to craft a comprehensive report recommend adjustments and advancements to the existing space standards, particularly those established by ECSS which apply to the European space community.

For further information about this report or any referred material in it, please feel free to contact Critical Software at the following contacts:

Nuno Silva, Technical Manager: nsilva@criticalsoftware.com

Pedro Sousa, Cybersecurity Engineer: pedro.m.sousa@criticalsoftware.com

ANNEXES

ANNEX A. SURVEY QUESTIONS

The following text is the introductory text used in the survey titled "Cybersecurity Challenges and Solutions for Space Systems".

“As our reliance on space-based technologies continues to grow, safeguarding these applications against cyber threats becomes not only a matter of technological prowess but also a critical element in preserving the integrity, functionality, and security of space missions. Cybersecurity has been considered a key element of space software development and operations in the last years, reflected mostly in updated software development and V&V standards. For example, the ECSS have been considering and including more and more cybersecurity requirements in the set of European Space Standards, especially the upcoming versions of **ECSS-E-ST-40** and **ECSS-Q-ST-80**, which will already include significant amount of cybersecurity related requirements. The objective of this survey is to capture several stakeholders/experts view on the cybersecurity challenges, particularly in what concerns vulnerabilities, threats and mitigations / solutions to tackle the potential cybersecurity threats that affect space systems.
Note: if you do not work with space systems directly, please consider that "space systems" can also be interpreted as safety-critical embedded or ground systems.
Confidentiality Note: all answers will be anonymized and not relatable to any individual or institution, however, we recommend that you to not provide any confidential information in your answers.”

Table 10 depicts the questions presented in the survey titled “Cybersecurity challenges and solutions for space systems”.

Number	Question	Rationale
1	List up to 5 of the most common or severe vulnerabilities that you believe affect space or ground systems (or embedded real-time systems).	To collect the perception of the experts on which are the most common vulnerabilities that impact security of space systems.
2	List up to 5 cybersecurity threats that you consider relevant for space or ground systems (or embedded real-time systems).	To identify which are the main existing threats to space systems.
3	Identify up to 5 Technical Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.	To collect functional level solutions and mitigations related to security vulnerabilities and threats and to start creating a catalogue of security related mitigations.
4	Identify up to 5 Processual Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.	To collect process level solutions and mitigations related to security vulnerabilities and threats and to start creating a catalogue of security related mitigations in terms of process.
5	List the standards or cybersecurity resources used to ensure compliance and security of space or ground systems.	To identify which standards are being used, which are useful and which tools/resources are applicable and can serve as support to future cybersecurity assurance.
6	Select the segment of space systems that do you think are most vulnerable to cybersecurity threats. (Ground, Space or Link/Signal)	To identify which segment is more vulnerable.
7	Any other cybersecurity concerns/trends that you see in the short/middle term (up to 10 years from now) for safety-critical embedded systems, particularly space systems.	To identify potential emerging challenges or additional concerns not covered with the previous 5 questions.

Table 10: Questions of the "Cybersecurity challenges and solutions for space systems" survey

Critical software

We are CMMI Maturity Level 5 rated.

For a list of our certifications & standards visit our website.

www.criticalsoftware.com