Critical Software

TN05: Proposals to Cope with Threats and Vulnerabilities

CYBERSECURITY FOR SPACE

CONTRACT REFERENCE: NOT APPLICABLE.

DATE: 2024-10-19
PROJECT CODE: CSEC4SPACE
DOC. REF.: CSW-2024-TNR-03939
STATUS: APPROVED
PAGES: 43
INFORMATION CLASSIFICATION: PUBLIC
VERSION: 1.0

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
1.0	Nuno Silva	Industry Supervisor		2024-10-19
1.0	João Carlos Cunha	Academic Supervisor		2024-10-19

AUTHORS AND CONTRIBUTORS

NAME	DESCRIPTION	DATE
Pedro Miguel Sousa	Author	2024-06-14
Nuno Silva	Reviewer	2024-07-31

COPYRIGHT

REVISION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR
0.1	2024-06-14	First revision of the technical note.	Pedro Sousa
0.2	2024-08-16	Second revision of the technical note.	Pedro Sousa
1.0	2024-10-19	Updated the technical note with the implementation of comments from the reviewers. Document approved for release.	Pedro Sousa

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1. INTRODUCTION

The space sector is experiencing a period of rapid growth, with increasing numbers of satellites and constellations being launched, as an example. This growth, however, presents new challenges in ensuring the security of these critical systems. Spacecrafts and ground systems are susceptible to a range of cyber threats and vulnerabilities that could potentially disrupt operations, cause data breaches, or even lead to physical damage.

This technical note, titled "Proposals to Cope with Threats and Vulnerabilities" aims to address these concerns by exploring effective methods to mitigate potential cyber risks of the space sector. We will delve into the existing threat landscape, identify key threats and vulnerabilities, and propose a comprehensive set of strategies and solutions to counter them. By proactively addressing these challenges, we can ensure the continued safe and secure operation of space systems, fostering a more robust and resilient space environment and operations.

1.1. OBJECTIVE

This technical note explores methods to mitigate threats and vulnerabilities in space sector systems, proposing solutions to guarantee and enhance overall security.

1.2. SCOPE

The scope of this technical note includes a thorough analysis of the current threat landscape in the space sector, including an assessment of the most common cyber threats and vulnerabilities that spacecraft and ground systems face. The note will explore existing methods and tools used to mitigate these risks and propose innovative solutions to counter emerging threats. Additionally, the note will provide recommendations on best practices for implementing these solutions and ensuring ongoing monitoring and risk management. The technical note will not cover physical security measures for space systems, but instead will focus solely on cyber risks and vulnerabilities.

1.3. AUDIENCE

The audience of this report includes: Critical Software S.A., Coimbra Institute of Engineering (ISEC), 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
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.
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.

NAME	DESCRIPTION
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.
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.
Availability	Ensuring timely and reliable access to and use of information.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Table 1: Definitions

Table 2 presents the list of acronyms used throughout this document.

ACRONYM	DESCRIPTION
ACM	Approximate Conditional Mean
AES	Advanced Encryption Standard
ATT	Antenna Array Techniques
CMMC	Cybersecurity Maturity Model Certification
COMINT	Communications Intelligence
COTS	Commercial-off-the-shelf
CREST	Council of Registered Ethical Security Testers
CSW	Critical Software, SA
DES	Data Encryption Standard
DNS	Domain Name System
DWT	Discrete Wavelet Transform
ECC	Error-correcting Codes

ACRONYM	DESCRIPTION
EEPROM	Electrically Erasable Programmable Read-only Memory
ELINT	Electronic Intelligence
ESA	European Space Agency
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection and Prevention Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Units
IOM	Installation, Operation, and Maintenance
ISAC	Space System Information Sharing and Analysis Center
ISEC	Coimbra Institute of Engineering (Instituto Superior de Engenharia de Coimbra)
LET	Linear Energy Transfer
MAC	Message Authentication Code
MBU	Multiple Bit Upset
MCU	Multiple Cell Upset
MFA	Multi-factor Authentication
MITM	Man-in-the-Middle
NASA	National Aeronautics and Space Administration
NICE	Workforce Framework for Cybersecurity
NIST	National Institute of Standards and Technology
NMA	Navigation Message Authentication
OWASP	Open Worldwide Application Security Project
PDF	Portable Document Format
QKD	Quantum Key Distribution

ACRONYM	DESCRIPTION
RSA	Rivest-Shamir-Adleman
SBOM	Software Bill of Materials
SCA	Static Code Analysis
SCRM	Supply Chain Risk Management
SDL	Security Development Lifecycle
SDR	Software-Defined Radio
SEU	Single Event Upset
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIGINT	Signals Intelligence
SMS	Short Message Service
SNR	Signal-to-noise Ratio
SPDX	Software Package Data Exchange
SPT	Signal Processing Techniques
SQL	Structured Query Language
SRAM	Static Random-access Memory
SSDF	NIST Secure Software Development Framework
SSDLC	Secure software development lifecycles
SSH	Secure Shell
SSL	Secure Sockets Layer
STFT	Short-Time Fourier Transform
TLS	Transport Layer Security
VPN	Virtual Private Network

Table 2: Acronyms

1.5. DOCUMENT STRUCTURE

Section 1 (Introduction) presents this document.

Section 2 (Proposals of cybersecurity Solutions gathering process) explains the process of presenting solutions to vulnerabilities and threats.

Section 3 (Threats and Mitigations) focuses on the proposed threat mitigation techniques.

Section 4 (Vulnerabilities and Mitigations) presents the proposed vulnerability mitigation techniques.

Annex A (Threats solutions Summary Table) provides a summary table of the threats mitigation techniques.

Annex A.2 (Vulnerabilities solutions Summary Table) provides a summary table of the vulnerabilities and threats mitigation techniques.

1.6. REFERENCE DOCUMENTS

Table 3 presents the list of reference documents.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-1] GIS Resources – Everything you need to know about GPS L1, L2, and L5 Frequencies	Everything You Need To Know About GPS L1, L2, and L5 Frequencies - GIS Resources, visited on 2024-06-25.
[RD-2] ESA – GPS Signal Plan	https://gssc.esa.int/navipedia/index.php/GPS_Signal_Plan, visited on 2024-06-25.
[RD-3] ResearchGate – How Modernized and Strengthened GPS Signals Enhance the System Performance During Solar Radio Bursts	https://www.researchgate.net/publication/349074047_How_modernized_and_strengthened_GPS_signals_enhance_the_system_performance_during_solar_radio_bursts, visited on 2024-06-25.
[RD-4] ResearchGate – A Security Risk Taxonomy for Commercial Space Mission	https://www.researchgate.net/publication/352960784_A_Security_Risk_Taxonomy_for_Commercial_Space_Missions, visited on 2024-06-25.
[RD-5] ResearchGate – Identifying Space Threats for Space Aware Resilience- a Spacecraft and Satellite Service Resilience Model	https://www.researchgate.net/publication/362615616_Identifying_Space_Threats_for_SpaceAware_Resilience-_a_Spacecraft_and_Satellite_Service_Resilience_Model, visited on 2024-06-26.
[RD-6] ResearchGate – CyberSecurity in New Space	https://www.researchgate.net/publication/341331628_Cyber_security_in_New_Space_Analysis_of_threats_key_enabling_technologies_and_challenges, visited on 2024-06-26.
[RD-7] IEEE Xplore – Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey	https://ieeexplore.ieee.org/document/9733393, visited on 2024-06-26.
[RD-8] ResearchGate – GPS Vulnerability to Spoofing Threats and a Review of Anti-Spoofing Techniques	https://www.researchgate.net/publication/258381922_GPS_Vulnerability_to_Spoofing_Threats_and_a_Review_of_Antispoofing_Techniques, visited on 2024-06-27.
[RD-9] ResearchGate – Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 years of spaceflight	https://www.researchgate.net/publication/361432917_Building_a_launchpad_for_satellite_cyber-security_research_lessons_from_60_years_of_spaceflight, visited on 2024-06-27.
[RD-10] Analog Devices – An Introduction to Spread-Spectrum Communications	An Introduction to Spread-Spectrum Communications | Analog Devices, visited on 2024-06-27.
[RD-11] IEEE Xplore – Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments	https://ieeexplore.ieee.org/document/10546924, visited on 2024-07-01.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-12] IEEE Xplore – Cyber-Space and Its Menaces	https://ieeexplore.ieee.org/document/8878848, visited on 2024-07-01.
[RD-13] IEEE Xplore – Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity	https://ieeexplore.ieee.org/document/9925759, visited on 2024-07-01.
[RD-14] Medium – IP Spoofing and it´s Countermeasures	https://medium.com/@namrata_khatwani/ip-spoofing-and-its-countermeasures-755fe0aa7116, visited on 2024-07-01.
[RD-15] Cyberbit – Cyber Range	https://www.cyberbit.com/platform/cyber-range/, visited on 2024-07-17.
[RD-16] ResearchGate – Cybersecurity Principles for Space Systems	https://www.researchgate.net/publication/329596980_Cybersecurity_Principles_for_Space_Systems, visited on 2024-07-02.
[RD-17] IEEE Xplore – A Comprehensive Taxonomy of Social Engineering Attacks and Defence Mechanisms: Toward Effective Mitigation Strategies	https://ieeexplore.ieee.org/document/10535157, visited on 2024-07-03.
[RD-18] TN01: Literature Review And State-of-the-Art Study on Cybersecurity for Space or Similar Domains	CSW-2024-TNR-01442, v. 1.1
[RD-19] ResearchGate – Security Challenges when Space Merges with Cyberspace	https://www.researchgate.net/publication/362230522_Security_Challenges_when_Space_Merges_with_Cyberspace, visited on 2024-07-05.
[RD-20] ResearchGate – Aerospace Supply Chains Using Blockchain Technology: Implications for Sustainable Development Goals	https://www.researchgate.net/publication/381122214_Aerospace_Supply_Chains_Using_Blockchain_Technology_Implications_for_Sustainable_Development_Goals, visited on 2024-07-05.
[RD-21] CISA – Securing the Software Supply Chain: Recommended Practices Guide for Developers	https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF, visited on 2024-07-05.
[RD-22] ResearchGate – Securing the Skies: A Comprehensive Analysis of Cybersecurity Measures in the Aviation Sector	https://www.researchgate.net/publication/378966499_Securing_the_Skies_A_Comprehensive_Analysis_of_Cybersecurity_Measures_in_the_Aviation_Sector, visited on 2024-07-05.
[RD-23] CISA – Recommendations to Space System Operators for Improving Cybersecurity	https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%285088%29.pdf, visited on 2024-07-05.
[RD-24] ResearchGate – Ground Station as a Service Reference Architectures and Cybersecurity Attack Tree Analysis	https://www.researchgate.net/publication/369246038_Ground_Station_as_a_Service_Reference_Architectures_and_Cyber_Security_Attack_Tree_Analysis, visited on 2024-07-08.
[RD-25] TN02: Analysis of Practices and International Standards Related to Cybersecurity	CSW-2024-TNR-01469, v. 1.0
[RD-26] TN04: Space Systems Threats and Vulnerabilities	CSW-2024-TNR-01468, v. 1.0

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-27] Report – Cybersecurity Survey	CSW-2024-TNR-03904, v. 1.1
[RD-28] CCSDS - Security Threats Against Space Missions	https://public.ccsds.org/Pubs/350x1g3.pdf, visited on 2024-04-22.
[RD-29] Cydrill - Secure design principles	https://cydrill.com/cyber-security/secure-design-principles/#:~:text=Saltzer%20and%20Schroeder%20described%208%20main,only%20imperfectly%20to%20computer%20systems%20%E2%80%9D.&text=Saltzer%20and%20Schroeder%20described,to%20computer%20systems%20%E2%80%9D.&text=Schroeder%20described%208%20main,only%20imperfectly%20to%20computer, visited on 2024-07-16.
[RD-30] OWASP - Insecure Design	https://owasp.org/Top10/A04_2021-Insecure_Design/, visited on 2024-07-16.
[RD-31] IEEE Xplorer - The protection of information in computer systems	https://ieeexplore.ieee.org/document/1451869, visited on 2024-07-16

Table 3: Reference documents

2. PROPOSALS OF CYBERSECURITY SOLUTIONS GATHERING PROCESS

Leveraging on previous technical notes [RD-18], [RD-25] and [RD-26], survey results [RD-27], and scientific paper analyses, this document lists the main threats, vulnerabilities, and identifies mitigation techniques to address them. The document is divided into separate sections for threats and vulnerabilities, with each item referencing its corresponding mitigation techniques and strategies. Identified threats and vulnerabilities without viable solution are listed and justified at the end of each respective section.

The process for gathering proposals of cybersecurity solutions can be broken down into the following steps (as see in Figure 1):

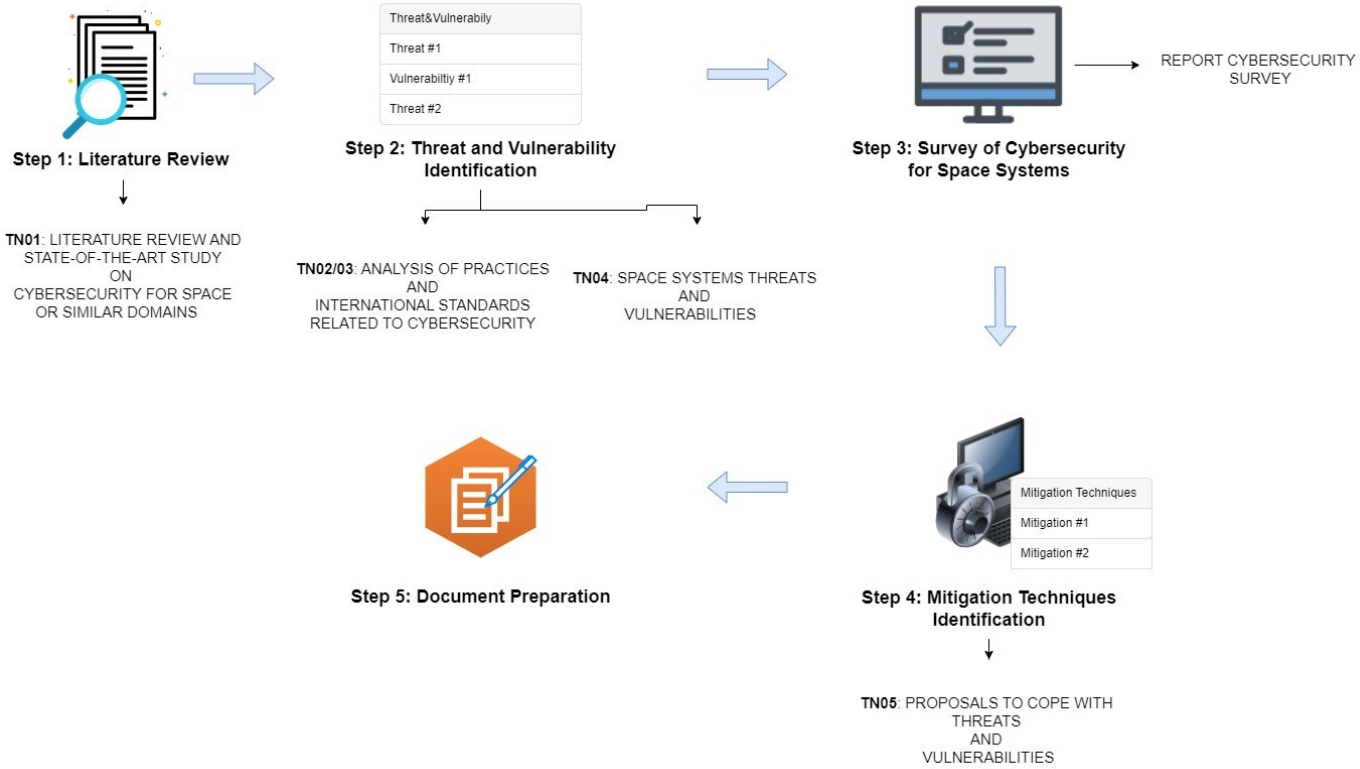

Figure 1: Process for gathering proposals of cybersecurity solutions

Step 1: Literature Review

The first step was to conduct a thorough literature review and scientific paper analyses related to cybersecurity in the space sector. This involved identifying the most relevant and recent sources and compiling them into a reference list (see [RD-18]).

Activities:

- Identify relevant literature and scientific papers.
- Compile a reference list of all the sources.
- Extract the relevant information from the selected literature.

Step 2: Threats and Vulnerabilities Identification

The second step involved identifying the main threats and vulnerabilities in the space sector. This included analysing the data gathered in the literature review and identifying common themes and trends (see [RD-25] and [RD-26]).

Activities:

- Analyse the data gathered in the literature review.
- Identify the main threats and vulnerabilities in the space sector.
- Consider also standards, processes, tools, best practices, lessons learned, etc.
- Categorize the identified threats and vulnerabilities.

Step 3: Survey of Cybersecurity for Space Systems

The third step involved creating, sharing and collecting expert's inputs on a cybersecurity for space systems survey. The collected survey data intended to confirm and complement the literature review (Steps 1 and 2) but in a closer and more practical way to the space systems domain. The results have been reported on a dedicated technical note. (see [RD-27])

Step 4: Mitigation Techniques Identification

The fourth step involves identifying mitigation techniques and strategies to address the identified threats and vulnerabilities. This includes analysing the effectiveness of existing mitigation techniques and proposing innovative solutions to counter emerging threats (documented in this report).

Activities:

- Identify existing mitigation techniques and strategies.
- Consider also standards, processes, tools, best practices, lessons learned, etc.
- Analyse the effectiveness of existing mitigation techniques.
- Propose innovative solutions to counter emerging threats.

Step 5: Document Preparation

The fifth step involved compiling the identified threats, vulnerabilities, and mitigation techniques into a document. The document is divided into separate sections for threats and vulnerabilities, with each item referencing its corresponding mitigation technique or strategy. Identified threats and vulnerabilities without viable solutions are listed and justified at the end of each respective section.

Activities:

- Compile the identified threats, vulnerabilities, and mitigation techniques into a document.
- Divide the document into separate sections for threats and vulnerabilities.
- Reference each item to its corresponding mitigation technique or strategy.
- List and justify identified threats and vulnerabilities without viable solutions.

3. THREATS AND MITIGATIONS

This chapter categorizes threats based on the previous technical note, TN04 – Space System Threats and Vulnerabilities [RD-26]. The categorization divides threats into two primary groups: electromagnetic threats, encompassing issues like direct energy attacks or electromagnetic interference, and cyber threats targeting software, hardware, or communication infrastructure of space systems.

3.1. ELECTROMAGNETIC THREATS AND RESPECTIVE SOLUTIONS

This section focuses on electromagnetic threats, specifically those originating from both environmental and man-made sources.

3.1.1. Environmental

These threats arise from natural phenomena such as solar flares or geomagnetic storms. These events can induce electrical currents in spacecraft electronics, potentially causing disruptions to operations.

3.1.1.1. SOLAR RADIO BURSTS

Solar radio bursts originate from the Sun's activity, particularly during events like solar flares and coronal mass ejections (CMEs). These events release intense bursts of radio waves that can disrupt data transmission between satellites and ground stations/users, for example the usage of GPS.

The Global Positioning System (GPS) utilizes three primary L-band frequencies for civilian use, ranging from 1 to 2 GHz: L1, L2, and L5. Additionally, there's civilian codes, Course Acquisition (C/A) and military-exclusive P-Code and a more modern M code. These codes that are crucial for [RD-1]:

- Calculating distance: The codes help receivers determine the distance between themselves and the satellite.
- Identifying messages: Codes distinguish between different types of transmitted information.
- Security: Codes like the M code enhance transmission security through exclusivity, authentication, and confidentiality (along with streamlined key distribution).

With GPS modernization, new civilian signals have been introduced: L1C, L2C, and L5. Here's a breakdown of the frequencies and their purposes [RD-2]:

- L1 (1575.42 MHz): Primarily used for tracking GPS satellite location.
- L1C (similar frequency to L1): Designed for interoperability with Europe's Galileo system, it offers higher power and advanced security features.
- L2 (1227.60 MHz): Used to monitor the health of GPS satellites.
- L2C (similar frequency to L2): Designed to meet commercial needs for dual-frequency receivers, improving accuracy.
- L5 (1176.45 MHz): Improves accuracy for civilian applications like aircraft precision approach guidance.

Mitigation/Solution

SRD-1 – Increase Signal Power & New Civilian Codes: Solutions to mitigate the effects mentioned earlier are already in use. These include increasing the transmitted signal power at the L2 frequency and implementing new civilian codes, both of which enhance the stability and reliability of GNSS (Global Navigation Satellite System) operations during solar events [RD-3] .

3.1.1.2. SINGLE EVENT EFFECTS

The deposition of charged particles within a satellite, originating from cosmic events, direct ionization, and nuclear interactions, can cause significant damage to satellite hardware. Effects range from complete component destruction to more subtle errors like bit flips in memory cells or registers. [RD-4]

Catastrophic Single Events

- **Burnout:** High currents triggered by ionizing particles can overheat and permanently damage components.
    - **SEE-1 Mitigation:** Protect metal-oxide-semiconductor field-effect transistors (MOSFETs) with radiation-hardened designs to withstand larger linear energy transfer (LET).
- **Functional Interrupt:** This event causes unexpected loss of functionality or changes the state of a device, similar to a Single Event Upset (SEU).
    - **SEE-2 Mitigation:** Power-cycling the device typically restores functionality, though some damage may be permanent.
- **Gate Rupture:** The impact of ionizing particles damages the gate dielectric of a transistor, leading to insulator breakdown and increased temperature. Devices using non-volatile static random-access memories (SRAM) and electrically erasable programmable read-only memories (EEPROMs) are particularly vulnerable.
    - **SEE-3 Mitigation:** Avoid using SRAM and EEPROM technologies in radiation-sensitive environments.
- **Latchup:** This event creates a low-resistance path between power and ground due to ionizing particles, resulting in high currents, vaporized metals, and potentially permanent damage.
    - **SEE-4 Mitigation:** Rapidly disconnect power to prevent further damage from high currents.

Non-Catastrophic Single Events

- **Multiple Bit Upset (MBU):** This event primarily affects memory components. Ionizing particles flip multiple bits within the same data word.
    - **SEE-5 Mitigation:** Employ error-correcting codes (ECC) and distribute data bits non-contiguously in memory.
- **Multiple Cell Upset (MCU):** Ionizing particles cause multiple bits within an integrated circuit to flip state simultaneously.
    - **SEE-6 Mitigation:** Increase spacing between transistors in integrated circuit design.
- **Transient Errors:** Ionizing particles induce temporary errors in a circuit's combinational logic, with increased likelihood at faster operating speeds.
    - **SEE-7 Mitigation:** Employ techniques like circuit redundancy and voting to correct for transient errors.

3.1.2. Man-made

These threats can also be caused by human interference, potentially leading to disruptions of operations and alterations to data transmitted from the satellite.

3.1.2.1. JAMMING

Jamming interferes with RF communications by transmitting radio signals on the same frequency as legitimate communications, effectively overpowering them. This disruption interrupts transmissions between satellites, or between satellites and ground stations.

To mitigate this threat, various anti-jamming techniques can be employed [RD-7][RD-28]:

Signal Processing Techniques:

- **JAM-1 - Time-Frequency Filtering Mask**: This technique leverages the unique characteristics of jamming and GPS signals in both the time and frequency domains. The filter identifies and suppresses the jamming signal's energy while allowing the GPS signal to pass through.
- **JAM-2 - Adaptive Notch Filter**: This filter continuously detects, estimates the frequency of, and blocks single-tone continuous jamming signals. Its adaptability allows it to adjust to changes in the jamming signal's frequency.
- **JAM-3 - Short-Time Fourier Transform (STFT)**: By analysing signals in both time and frequency domains, STFT enhances the notch filter's ability to respond quickly to changes in jamming frequencies and handle wider jamming bandwidths.
- **JAM-4 - ACM and DWT Filtering**: This two-step process uses an Approximate Conditional Mean (ACM) filter to estimate the true GPS signal, followed by a Discrete Wavelet Transform (DWT) filter to further refine the signal and remove jamming components. This approach has demonstrated the ability to maintain a high signal-to-noise ratio (SNR), even under severe jamming conditions.

Antenna Array Techniques:

- **JAM-5 - Spatial Filtering, Polarization Diversity, and Adaptive Adjustment:** Antenna arrays utilize multiple antennas to pinpoint the desired GPS signal, suppress jamming signals from other directions, and adapt to changing jamming tactics.
- **JAM-6 - Spectral Self-Coherence Beamforming:** This technique amplifies the GPS signal based on its self-coherent properties while cancelling out the jamming signal, which typically lacks such patterns.
- **JAM-7 - Spatial-Temporal Interference Projection:** This method differentiates between the GPS and jamming signals based on their spatial and temporal characteristics, projecting the received signal onto a subspace orthogonal to the jamming signal to effectively eliminate it.
- **JAM-8 - Regret Minimization Framework & Game-Theoretical Approach:** This combines decision-making under uncertainty with game theory to develop a system where users can quickly adapt their strategies to maximize successful communication despite jamming.

3.1.2.2. SPOOFING

Spoofing involves transmitting counterfeit signals that mimic legitimate GPS signals to deceive receivers and gain unauthorized access.

To safeguard against this threat, various cryptographic techniques can be employed [RD-6][RD-8]:

- **SPOO-1 - Navigation Message Authentication (NMA):** This mechanism ensures the authenticity and integrity of navigation data using either symmetric or asymmetric key encryption.
- **SPOO-2 - Chips Message Robust Authentication (CHIMERA):** A hybrid of NMA and spreading code authentication, CHIMERA uses the P-224 elliptic curve digital signature algorithm for added security.
- **SPOO-3 - Timed Efficient Stream Loss-tolerant Authentication (TESLA):** Used in the Galileo GNSS system, TESLA, combined with Message Authentication Code (MAC), verifies the origin and identity of messages.
- **SPOO-4 – Cross sensor´s information:** sensors like inertial measurement units (IMUs) and vehicle odometers can help detect spoofing by cross-checking data against GNSS measurements. Discrepancies between sensor readings can indicate a potential spoofing attack.
- **SPOO-5 – Y-code:** Military GPS signals are further protected by an encrypted binary code known as the Y-code. This code significantly enhances security, making it extremely difficult to spoof these signals without access to the Y-code.
- **SPOO-6 - C/N0 monitoring:** C/N0, or Carrier-to-Noise density ratio, is a measure of the strength of a received GPS signal relative to background noise. C/N0 monitoring is a valuable tool in anti-spoofing techniques. By tracking the history and behaviour of C/N0, GPS receivers can detect

sudden anomalies that may indicate a spoofing attack, allowing for timely intervention and protection of GPS-based navigation systems.

- **SPOO-7 - Absolute Power Monitoring:** GPS signal strength decreases as it travels through the atmosphere and other obstacles (a phenomenon known as path loss). This decrease is highly variable and depends on factors like distance, terrain, and weather conditions. On Earth, the maximum power of a legitimate GPS signal at the L1 frequency (used by civilian GPS devices) is around -153 dBW (decibel-watts). If a receiver detects a signal significantly stronger than this, it strongly suggests a spoofing attack.

The authors of [RD-8] provide a comprehensive survey of over a dozen additional GPS defence techniques against spoofing. These include **analysing power variations relative to receiver movement**, **comparing L1/L2 power levels**, and **examining differences in signal direction of arrival**, among others.

3.1.2.3. EAVESDROPPING

Eavesdropping involves the interception of signals from satellites or other sources for monitoring purposes, often referred to as signals intelligence (SIGINT). SIGINT can be further divided into two categories:

- **Communications Intelligence (COMINT):** Focuses on intercepting and analysing voice communications.
- **Electronic Intelligence (ELINT):** Focuses on intercepting and analysing other types of radio signals, such as radar emissions or telemetry data.

To protect against eavesdropping, strong signal encryption is crucial. To mitigate such a threat there are various mitigation techniques [RD-9]:

- **EAV-1 - On-Board Encryption:** One traditional method involves employing on-board encryption capabilities with pre-shared secret keys between the ground station and satellite. This ensures only authorized parties can decrypt and understand the messages. However, this approach is vulnerable if the shared key is compromised.
- **EAV-2 – New Cryptographic techniques:** Newer approaches, such as public-key cryptography and quantum key distribution, can overcome the vulnerabilities of pre-shared keys.
    - **Public-Key Cryptography:** Utilizes a pair of keys – a public key for encryption (known to everyone) and a private key for decryption (known only to the recipient). This eliminates the need for pre-sharing secret keys.
    - **Quantum Key Distribution (QKD):** This cutting-edge technology leverages principles of quantum mechanics to securely distribute encryption keys between the satellite and ground systems, offering the potential for virtually unbreakable encryption.

3.2. CYBER THREATS AND RESPECTIVE SOLUTIONS

This section focuses on cyber threats, which can target both technical vulnerabilities and exploit social engineering tactics.

3.2.1. Technical

Cyber threats exploit technical vulnerabilities in software to gain unauthorized access to systems and data. This can potentially lead to disruptions of operations or even damage. The following sections will present solutions to mitigate these various technical threats.

3.2.1.1. SIGNAL HIJACKING

Signal hijacking consists of an unauthorized takeover of a transmission channel to cause disruption or spread malicious content. This can occur if the command and control (C2) link is poorly encrypted. Therefore, the first step in mitigation is to implement robust signal encryption. The solutions for this involve the same techniques already identified in section 3.1.2.3.

Additionally, **spread spectrum** can be implemented to further enhance security.

Mitigation/Solution
SH-1 - Spread Spectrum: Spread spectrum intentionally expands signal bandwidth by injecting a higher frequency signal, causing the transmitted signal to appear as noise. The process involves a spreading operation (injecting a spread-spectrum code) before transmission and a dispreading operation (removing the code) at the receiver. The same code, known at both ends of the channel, is essential for successful communication [RD-10].

3.2.1.2. DATA CORRUPTIONS AND INTERCEPTION

Data corruption and interception are critical security threats in the space sector, targeting communication channels between satellites and ground stations.

- **Data interception** refers to the unauthorized access and capture of data transmitted between a satellite and a ground station.
- **Data corruption** involves the unauthorized alteration or modification of data transmitted between a satellite and a ground station.

To mitigate these threats, it is essential to use robust cryptographic algorithms, such as those mentioned in section 3.1.2.3, to ensure data transmitted or stored remains secure and confidential. In addition to the encryption techniques already identified, several others can help protect data in transit and at rest, including [RD-11]:

- **DC&I-1 - Advanced Encryption Standard (AES):** A widely used symmetric encryption algorithm for securing sensitive data. In ground segment security, AES-counter mode is often employed to further enhance security and system performance. AES utilizes three key sizes (128, 192, and 256 bits), the selection of which should align with the required security standards.
- **DC&I-2 - Triple Data Encryption Standard (3DES):** A symmetric encryption algorithm that applies the Data Encryption Standard (DES) cipher three times to each data block using three different keys. However, 3DES performs poorly compared to AES, as it is considerably slower.
- **DC&I-3 - Rivest-Shamir-Adleman (RSA):** A widely used asymmetric encryption algorithm for secure data transmission. It employs a pair of keys: one public key for encryption and one private key for decryption. RSA is primarily used for digital signatures but is also valued for protecting sensitive data, including login credentials, in satellite communication systems.
- **DC&I-4 - Elliptic Curve Cryptography (ECC):** A public key encryption technique based on elliptic curve theory, offering strong security with relatively small key sizes. Compared to RSA, ECC provides equivalent security with smaller keys, making it a lightweight cryptographic technique ideal for satellites with resource constraints.
- **DC&I-5 - Secure Hash Algorithm (SHA):** A family of cryptographic hash functions used to generate unique, fixed-size message digests for data integrity verification. The resulting hash code is virtually impossible to reverse-engineer.
- **DC&I-6 - Intrusion Detection and Prevention Systems:** the use these systems onboard spacecraft, employing signatures and machine learning, can help detect and prevent cyber intrusions [RD-13].

3.2.1.3. DENIAL-OF-SERVICE

Denial-of-Service (DoS) attack aims to disrupt a system's operations by overloading it with data. Hackers often leverage botnets, networks of compromised computers infected with malware.

Mitigating denial-of-service (DoS) attacks on satellites is a significant challenge due to the unique constraints and vulnerabilities of space-based systems. However, several strategies can be employed to enhance resilience against such attacks [RD-12][RD-13][RD-27][RD-28]:

Network-Level and Satellite Mitigation:

- **DoS-1 - Traffic Filtering and Rate Limiting**: Implementing filtering mechanisms at ground stations or network gateways can help detect and block suspicious traffic patterns indicative of a DoS attack. Rate limiting can restrict the number of requests from a single source, preventing overwhelming legitimate traffic.
- **DoS-2 - Intrusion Detection and Prevention Systems (IDPS)**: IDPS can monitor network traffic for signs of malicious activity, such as sudden spikes in traffic or unusual packet patterns, and automatically trigger mitigation actions.
- **DoS-3 - Geolocation Filtering**: Filtering traffic based on geographic origin can help block attacks originating from known malicious sources or regions. (survey mitigations)
- **DoS-4 - Hardening Satellite Software and Firmware:** Regularly updating and patching satellite software and firmware can help address vulnerabilities that could be exploited in a DoS attack.
- **DoS-5 - Redundancy and Failover Mechanisms:** Building redundancy into critical satellite components and systems can ensure continued operation even if some components are overwhelmed or disabled by an attack.

Ground-Level Mitigation:

- **DoS-6 - Use DDoS-resistant services**: This ensures you have enough bandwidth to handle traffic spikes caused by malicious activity.
- **DoS-7 - Distribute servers geographically and topologically**: Distributing servers across different locations makes it harder for attackers to target and successfully attack your infrastructure.
- **DoS-8 - Configure firewalls and routers to drop Internet Control Message Protocol (ICMP) packets and block DNS**.
- **DoS-9 - Protect your DNS servers**: DNS servers are often targeted in DoS attacks. Using measures like DDoS-resistant DNS providers can help mitigate this risk.

3.2.1.4. WEB SPOOFING

In the network domain, spoofing is a deceptive tactic where cybercriminals gain unauthorized access to systems by impersonating trusted entities. Common types of spoofing include [RD-14]:

- **Email Spoofing:** Forging email headers to make messages appear as if they originated from a different sender.
- **IP Spoofing:** Masking the true source IP address of network traffic.
- **Website Spoofing:** Creating fake websites that mimic legitimate ones to steal information or distribute malware.

To mitigate the risks of spoofing attacks, several countermeasures can be taken [RD-14][RD-28]:

- **WS-1 - Use strong authentication:** Implement multi-factor authentication (MFA) and avoid relying solely on passwords.
- **WS-2 - Securely store secrets:** Avoid storing passwords or other sensitive data in plaintext. Use encryption or hashing techniques.
- **WS-3 - Protect credentials during transmission:** Encrypt credentials when sending them over networks.
- **WS-4 - Secure authentication cookies with SSL/TLS:** Use HTTPS to protect authentication cookies and ensure secure transmission of sensitive data.
- **WS-5 - Implement packet filtering:** Analyse and discard incoming/outgoing packets with suspicious source/sender IP addresses.
- **WS-6 - Avoid host-based authentication:** Use encrypted connections (e.g., SSH) for remote logins and authentication.

While detecting IP spoofing is difficult for end users, they can minimize their risk of other types of spoofing by taking the following precautions [RD-14][RD-28]:

- **WS-7 - Use HTTPS for secure browsing:** Ensure websites have valid SSL/TLS certificates to protect against eavesdropping and tampering.
- **WS-8 - Filter ICMP packets:** ICMP (Internet Control Message Protocol) can be used in some spoofing attacks, so filtering them can add a layer of protection.
- **WS-9 - Use random sequence numbers and reduce initial TTLs (Time-to-Live):** This can make it harder for attackers to guess sequence numbers and exploit vulnerabilities in network protocols.
- **WS-10 - Employ encryption:** Use encryption tools to protect sensitive data during transmission and storage.
- **WS-11 - Avoid authentication based solely on IP:** Rely on stronger authentication methods that are not easily spoofed.

3.2.1.5. SOFTWARE THREATS

Software threats, such as malware, are designed to infiltrate and control organizational information systems, identify sensitive data, exfiltrate that data back to adversaries, and conceal their activities. These threats pose a significant risk to space systems.

To mitigate the risks of software threats, adhere to the following best practices [RD-12][RD-28]:

- **ST-1 - Keep your software, internet browser, and operating system up to date**: Regularly apply security patches and updates to address vulnerabilities that could be exploited by malware.
- **ST-2 - Use safe search tools that warn you about malicious sites**: These tools can help you avoid clicking on links or visiting websites that may harbour malware.
- **ST-3 - Use security software and antivirus**: Install and regularly update reputable security software to detect and remove malware.
- **ST-4 - Install NoScript (or a similar extension) on your browser**: This extension can help prevent malicious scripts from running on websites.
- **ST-5 - Acceptance testing:** This involves thoroughly testing the software to ensure it meets all functional and non-functional requirements, including security requirements, before deployment. It helps identify any potential vulnerabilities or issues that might be exploited by malware.
- **ST-6 - System evaluation:** This involves independent verification and validation (IV&V) and code analysis to assess the system's security posture and identify any potential weaknesses or vulnerabilities.
- **ST-7 - Continuous threat monitoring, continuous risk management:** This involves continuously monitoring the system for potential threats and vulnerabilities, and proactively managing risks to mitigate the likelihood or impact of a security incident.
- **ST-8 - Run-time security monitoring:** Monitoring the system during operation to detect any suspicious activity or potential attacks in real time.
- **ST-9 - Auditing:** Periodically reviewing the system's security controls and processes to ensure they are effective and compliant with relevant regulations and standards.
- **ST-10 - Supply chain confidence:** Establishing trust and ensuring the security of the entire software supply chain, from development to deployment, to minimize the risk of introducing vulnerabilities through third-party components or services.

3.2.1.6. MAN-IN-THE-MIDDLE

A man-in-the-middle (MITM) attack is a cyberattack where a threat actor secretly positions themselves between two communicating parties. The attacker's goal is to eavesdrop on the communication, potentially intercepting or manipulating data without either party's knowledge.

To minimize the risk, users should [RD-12]:

- **MITM-1 - Avoid using Wi-Fi connections that are not password-protected**: Open Wi-Fi networks are more vulnerable to MITM attacks.
- **MITM-2 - Avoid using public networks for sensitive transactions**: Use a trusted and secure network (e.g., your home Wi-Fi) when conducting online banking or sharing sensitive information.
- **MITM-3 - Log out of applications immediately when not in use**: This prevents unauthorized access in case your session is hijacked.
- **MITM-4 - Use strong encryption, such as a VPN:** While an attacker can still intercept encrypted messages, they will be unable to read or alter the data without the encryption key.

3.2.1.7. ZERO-DAYS EXPLOITS

A zero-day exploit is a cyberattack that targets a software vulnerability unknown to the software vendor or security researchers. The term "zero-day" refers to the fact that developers have zero days to address the flaw before it's exploited.

While there is no immediate fix for a zero-day exploit, several proactive measures can mitigate the risk [RD-27]:

- **ZDE-1 - Vulnerability Databases:** Utilizing resources like the National Institute of Standards and Technology (NIST) National Vulnerability Database can expedite the identification and patching of known vulnerabilities, potentially preventing them from becoming zero-day exploits.
- **ZDE-2 - Machine Learning for Anomaly Detection:** Machine learning algorithms can analyse past exploit data to establish a baseline of normal system behaviour. Any deviations from this baseline might signal a potential zero-day attack.
- **ZDE-3 - Space System Information Sharing and Analysis Center (ISAC):** Establishing a Space System Information Sharing and Analysis Center (ISAC) would be a significant step in this direction [RD-16]. This will enable cooperation between the public and private space sectors, along with the academic community, is crucial for mitigating zero-day threats

The key functions of such an ISAC would include [RD-16]:

- **Information Sharing:** Encouraging participation from government agencies (e.g., the U.S. Department of Defence, NASA) and private sector space organizations to foster information sharing and collaboration on cybersecurity threats and best practices.
- **Timely Vulnerability Disclosure:** Requiring member entities to promptly disclose vulnerability and attack information within a predefined timeframe, similar to the European Union's General Data Protection Regulation's 72-hour breach notification requirement.
- **Curated Best Practices:** Developing and maintaining a central repository of cybersecurity standards and best practices specific to space systems, with input and contributions from ISAC members.
- **Cross-Sector Threat Sharing:** Sharing relevant threat information with other critical sectors that rely on space systems (e.g., telecommunications, finance) to ensure comprehensive preparedness and response.

3.2.1.8. PASSWORD ATTACKS

Passwords serve as the first line of defence, protecting data access from unauthorized individuals. Over time, password requirements have become more stringent.

Hackers employ various methods to crack passwords, including:

- **Phishing:** Deceptive emails or messages designed to trick users into revealing their passwords or clicking malicious links.
- **Man-in-the-middle (MitM) attacks:** Attackers intercept communications to steal data, including passwords.

- **Brute-force attacks:** Automated software rapidly tries numerous username and password combinations to gain access to an account.
- **Dictionary attacks:** Hackers use lists of common words and phrases to guess passwords.
- **Credential stuffing:** Hackers test stolen username and password combinations from other breaches, hoping they work on different platforms.
- **Keyloggers:** Malicious software that records keystrokes, including passwords.

While passwords are considered a primary defence, they are also a vulnerability. Complex password requirements often lead users to write down passwords, making them susceptible to discovery by malicious actors.

A potential solution is to move beyond passwords and adopt cryptographic keys, often called **passkeys**.

Mitigation/Solution
PA-1 – Passkeys: Passkeys leverage public key cryptography and biometrics (like fingerprints or facial recognition) for 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 [RD-27].

3.2.1.9. INJECTION ATTACKS

Injection attacks are a common and powerful threat, targeting vulnerabilities in web applications, databases, and other systems that rely on user input.

To withstand these attacks, the following measures are recommended [RD-12]:

- **IATT-1 - Apply the principle of least privilege:** Grant database users only the minimum permissions necessary to perform their tasks. This limits the potential damage if an attacker gains access.
- **IATT-2 - Avoid dynamic SQL:** If possible, use parameterized queries or prepared statements to prevent attackers from injecting malicious SQL code.
- **IATT-3 - Validate input data:** Implement rigorous input validation at the application level to ensure that user-supplied data conforms to expected formats and does not contain malicious code. Use a whitelist approach to allow only specific, safe input values.

3.2.2. Social Engineering

These threats exploit people's psychological vulnerabilities. Attackers manipulate and deceive victims into compromising systems, often by tricking them into installing malware or revealing login credentials.

Detecting social engineering attacks is increasingly difficult. The use of artificial intelligence (AI) in such attacks can make them harder to recognize, as attackers can craft sophisticated and personalized messages to deceive victims. Additionally, social engineering relies on manipulating human psychology, making it challenging to predict or prevent all potential scenarios.

To mitigate this threat, organizations can implement comprehensive cybersecurity strategies, as depicted in Figure 2:

- **SE-1 - Awareness and Training:** Educate employees and individuals about social engineering tactics, including common red flags and how to respond to suspicious requests.
- **SE-2 - Technical Controls:** Implement multi-factor authentication, email filtering, web filtering, and intrusion detection systems to bolster security and detect potential threats.
- **SE-3 - Policies, Procedures, and Governance:** Establish clear policies outlining acceptable use of systems and data, procedures for handling sensitive information, and a governance framework to oversee cybersecurity practices.

- **SE-4 - Incident Response and Reporting:** Develop a clear process for reporting and responding to suspected or confirmed social engineering incidents, including steps for containment, damage assessment, and recovery.

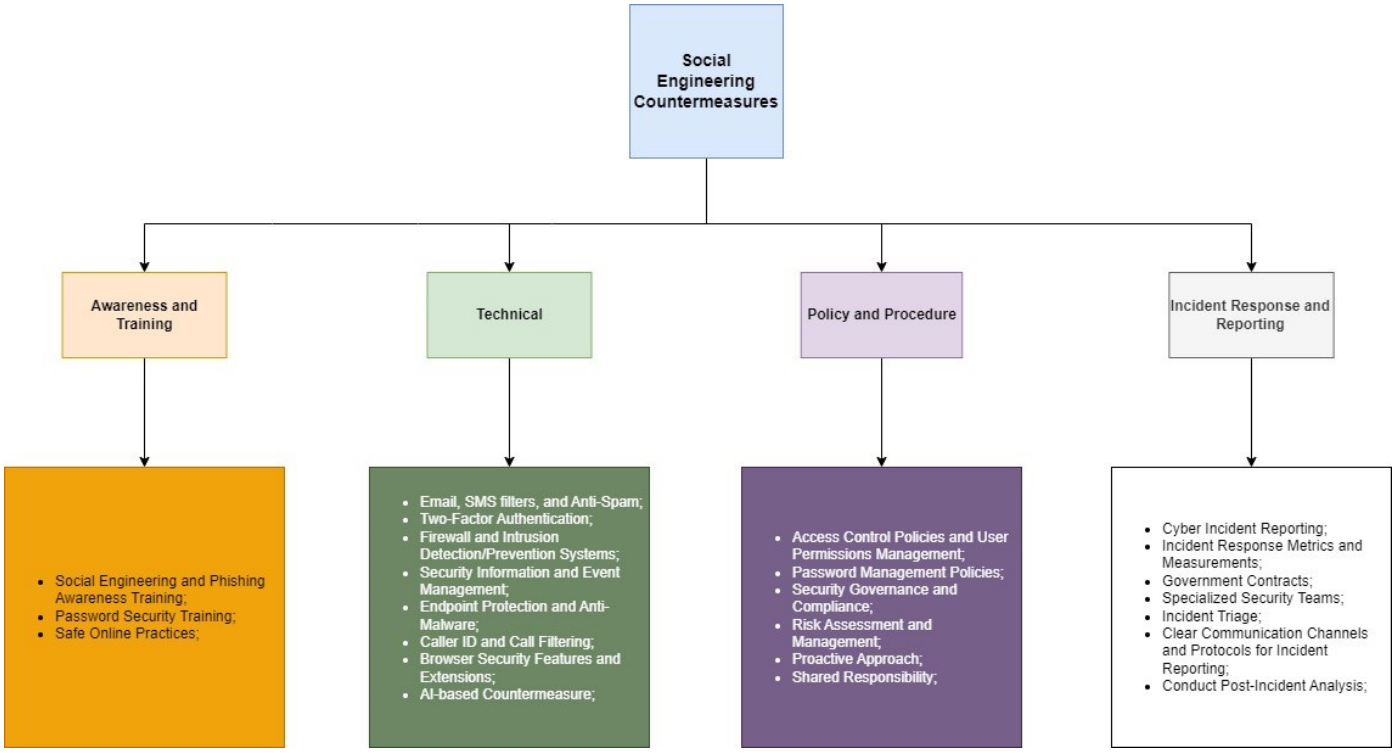

Figure 2: Mitigation Strategies for Social Engineering [RD-17]

The following sections will go more in detail about the cybersecurity.

3.2.2.1. AWARENESS AND TRAINING

Educating all personnel within an organization is crucial, as they are often the primary targets of social engineering attacks. Providing employees with the tools to protect themselves and the company is essential. To achieve this, comprehensive **social engineering and phishing awareness training** should be conducted.

This training should educate employees about the various types of social engineering techniques and keep them updated on the latest tactics and defense strategies. Simulated attacks, such as sending employees internal phishing emails, links, or attachments, or organizing a game that playfully "penalizes" those who leave their computers unlocked (for example, by requiring them to buy donuts for the team [RD-16]), can be used to assess their awareness and preparedness [RD-17].

Password security training is equally important. Employees should be taught best practices for creating strong passwords, the risks of reusing passwords, and the importance of avoiding password sharing [RD-17].

Additionally, **training on safe online practices** is vital. This includes raising awareness about the risks of opening unknown attachments, analyzing email headers for potential red flags, hovering over links to verify their legitimacy before clicking, and refraining from sharing personal information online [RD-12][RD-17].

To achieve advanced cybersecurity proficiency, organizations can leverage solutions like "cyber ranges," immersing employees in hyper-realistic simulated attacks to enhance awareness, skills, and teamwork. A prime example is the Cyberbit Cyber Range [RD-15], an on-demand platform offering a comprehensive catalogue of cyber-attacks, as shown in Figure 3.

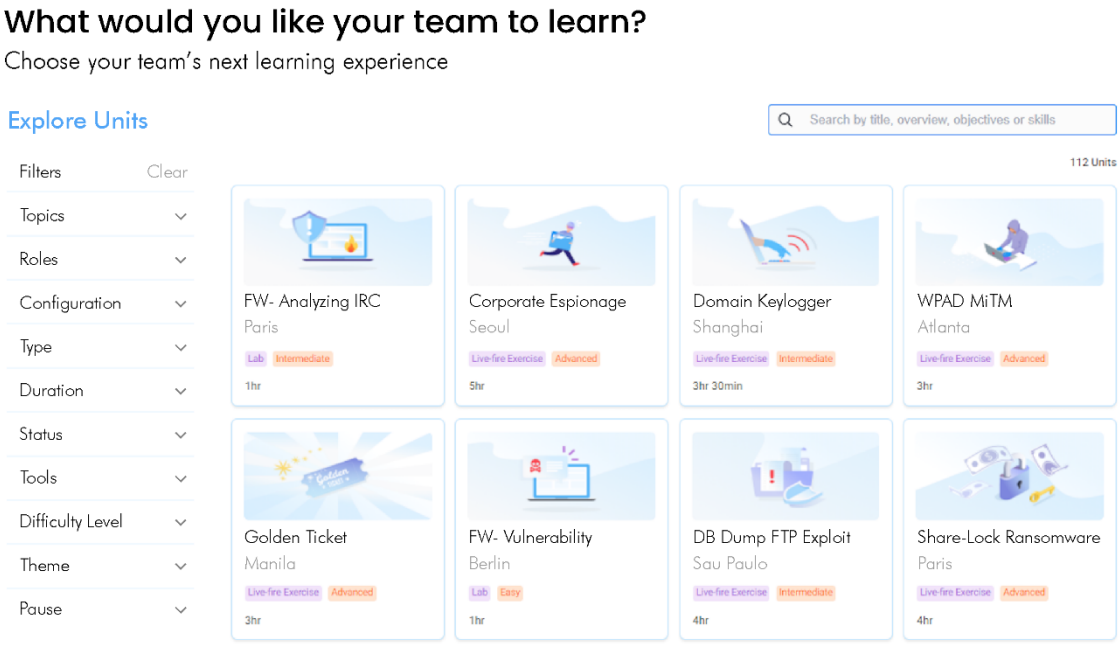

Figure 3: Catalogue of cyber-attacks [RD-15]

This enables teams to recognize and respond effectively to various threats while learning industry best practices through the integration of NIST, NICE, CREST, and MITRE ATT&CK frameworks. Suitable for Red, Blue, or Purple teams, it caters to all skill levels, from beginner to advanced.

The platform also supports attack simulations against cloud-native and hybrid environments, utilizing industry-standard tools like Wireshark, McAfee, Carbon Black, and others depicted in Figure 4.

Figure 4: Commercial tools used by Cyberbit Cyber Range [RD-15]

The exercises within this framework run on corporate-grade virtual networks, helping to identify challenges teams may face during incident detection, investigation, and response. To further strengthen this solution, it continuously assesses employees' real-time cyber performance during simulations.

The Cyberbit Cyber Range also offers a unique feature: simulated attacks on operational technology (OT). It provides a full-scale, emulated OT network and end-to-end simulations of IT-to-OT attacks, adding another layer of realism and complexity to the training environment, as depicted in Figure 5

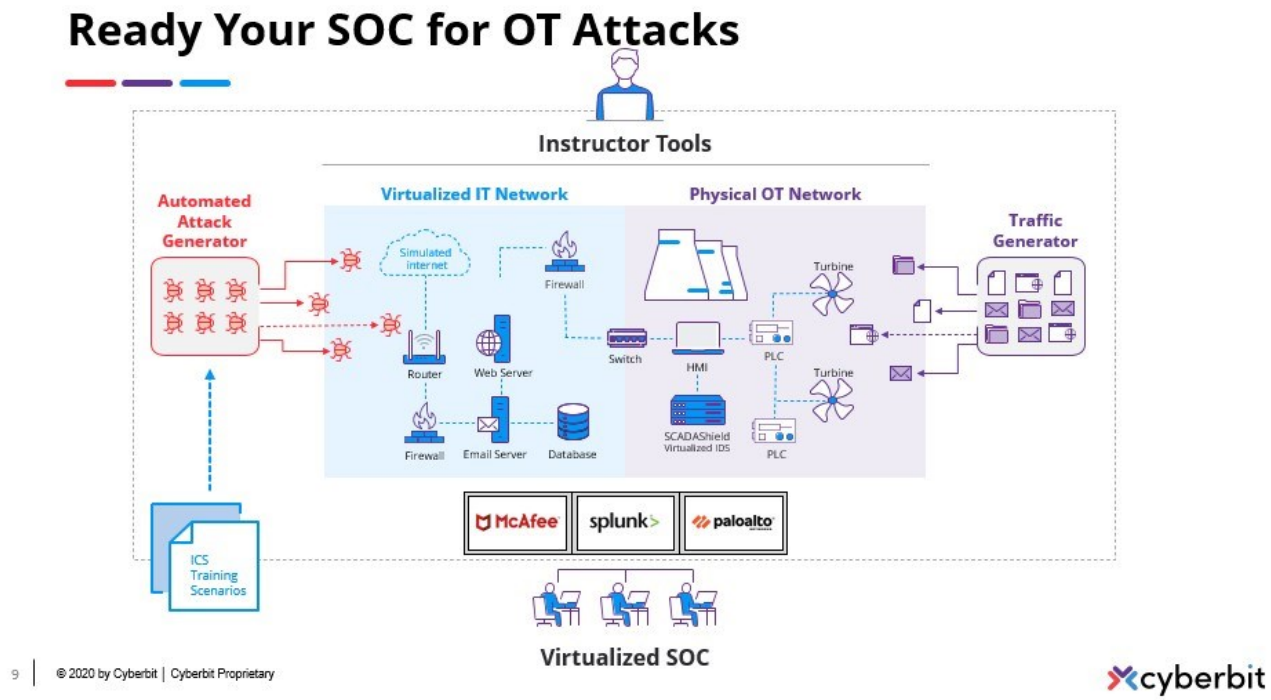

Figure 5: OT networks simulation attacks [RD-15]

By implementing comprehensive awareness training programs and promoting a culture of security, organizations can significantly reduce their vulnerability to social engineering attacks.

3.2.2.2. TECHNICAL CONTROLS

Once personnel are aware of the dangers, introducing software to enhance prevention further adds significant value. Examples of such technical controls include [RD-17]:

- **Email, SMS filters, and Anti-Spam Solutions:** These tools analyze incoming messages to identify and block phishing emails and spam containing malicious links or attachments.
- **Two-Factor Authentication (2FA):** Implementing 2FA strengthens access security by requiring an additional form of identification (such as a code from an authenticator app) beyond a password.
- **Firewall and Intrusion Detection/Prevention Systems (IDPS):** Employ a well-configured firewall to monitor and block unauthorized intrusions or malicious activities. IDPS actively scan network traffic for suspicious patterns and can take immediate action to protect systems.
- **Security Information and Event Management (SIEM) Solutions:** SIEM solutions aggregate and analyze security logs from various sources, enabling faster detection and response to suspicious activities.
- **Endpoint Protection and Anti-Malware Solutions:** Installing antivirus software, VPNs (Virtual Private Networks), and other endpoint protection tools safeguards user devices from malware and unauthorized access.
- **Caller ID and Call Filtering Solutions:** These solutions help identify and block fraudulent or spoofed calls, preventing social engineering attacks through phone communication.
- **Browser Security Features and Extensions:** Configure web browsers to enhance security by activating all available security features. Install extensions to block untrusted websites and restrict access to sites without valid certifications (e.g., those lacking HTTPS).
- **AI-based Countermeasures:** Leveraging AI can be a powerful defense against attacks that utilize AI. AI-powered tools can analyze communication patterns, identify anomalies, examine messages and links, flag potential threats, and scan data for breach indicators. Additionally, AI can

streamline incident response by automating tasks and learning from past incidents to improve future security measures.

3.2.2.3. POLICIES, PROCEDURES, AND GOVERNANCE

Regarding the establishment of policies, procedures, and governance mechanisms, the following should be considered [RD-16][RD-17]:

- **Access Control Policies and User Permissions Management:** Define and manage employee privileges and access to organizational resources. This minimizes the risk of unauthorized access and ensures appropriate access to systems, applications, and data.
- **Password Management Policies:** Establish clear guidelines and best practices for creating, storing, and changing passwords. Promote good password hygiene to ensure secure authentication.
- **Acceptable Use Policies:** Define acceptable behavior and actions when using organizational resources, systems, and networks. Emphasizing security responsibilities and potential liabilities for breaches is crucial. Legislation should incentivize responsible parties to take necessary measures to secure their systems.
- **Security Governance and Compliance:** Establish a robust framework for managing security risks, implementing controls, ensuring compliance with relevant regulations and standards, and overseeing the effectiveness of social engineering mitigation techniques.
- **Risk Assessment and Management:** Develop a process for identifying and assessing vulnerabilities and potential risks, prioritizing them based on their potential impact, and implementing appropriate controls and mitigation techniques.
- **Proactive Approach:** Policymakers must take a proactive stance on space cybersecurity, rather than waiting for major cyberattacks to occur before enacting relevant legislation.
- **Shared Responsibility:** Policies concerning critical infrastructure security should also encompass the third-party infrastructure upon which it relies. For example, space systems should be held to the same security standards as the critical infrastructure they support.

3.2.2.4. INCIDENT RESPONSE AND REPORTING

Responding to and reporting social engineering attacks in detail is crucial for organizations and the broader cyber community to evolve their mitigation strategies. To achieve this, the following activities should be undertaken:

- **Cyber Incident Reporting:** Similar to 32 Code of Federal Regulations Part 236, a rule should be established mandating that space asset organizations report all cyber incidents that have impacted or could potentially impact national security. This rule should include clear steps and instructions for timely reporting.
- **Incident Response Metrics and Measurements:** Utilize metrics to assess the effectiveness and efficiency of incident response efforts. This helps identify areas for improvement and optimize future responses.
- **Government Contracts:** Government contracts with space asset organizations should require contractors to comply with specific cybersecurity metrics, such as Key Performance Parameters (KPPs) and Key Performance Indicators (KPIs). These KPPs can specify the system's cybersecurity categorization for availability, integrity, and confidentiality, and should include appropriate cyber attributes within the system survivability KPPs based on applicable cybersecurity controls.
- **Specialized Security Teams:** Establish separate teams of cybersecurity specialists for mission systems and internal networks/server systems (operational technology vs. information technology). This is crucial due to the distinct operating environments, security skills, and expertise required for each. These teams would be responsible for effectively and promptly responding to any cyber threat, especially social engineering incidents.

- **Incident Triage:** Develop a process to analyze and categorize incidents based on impact, severity, and urgency. This prioritization facilitates the implementation of targeted response efforts and the allocation of necessary resources.
- **Clear Communication Channels and Protocols for Incident Reporting:** Establish secure and easily accessible communication channels through which employees can promptly report incidents.
- **Conduct Post-Incident Analysis:** Thoroughly reviewing and analyzing attacks helps identify weaknesses in current strategies and informs improvements for future defenses.

3.2.3. Other Technical Threats

The following technical threats were identified by the cybersecurity survey titled "Survey on Cybersecurity Challenges and Solutions for Space Systems" [RD-27], conducted among space sector specialists. A summary of these threats and respected mitigations is presented in Table 4.

Threat	Mitigation
Source Code Tampering	**SCT-1 - Extensive code analysis** (static analysis with cybersecurity rules) **SCT-2 - Zero code smells and zero warnings objective** (from static analysis tools) **SCT-3 - Protection of software development environments** **SCT-4 - Extensive V&V** of the embedded device against fuzz inputs **SCT-5 - Specific security assessment of the design/code** **SCT-6 - Integrity checks** for all data, configurations, inputs to the system
Spacecraft configuration modification	**SCM-1 - Intrusion detection mechanisms** **SCM-2 - Robust FDIR configuration** **SCM-3 - Proper authentication methods and access control** **SCM-4 - CRCs for all data transmission** **SCM-5 - Give an ID to every entity in the system** **SCM-6 - Telecommands acceptance is subject to validation** **SCM-7 - Periodically change the CRC/checksum/cryptography algorithms** **SCM-8 - Authentication on software patch** **SCM-9 - Accept telecommands and download telemetry only when flying above certain regions.**
Bad design	**BD-1 - Secure-by-design approach** (Zero trust solutions) **BD-2 - Take security lessons** learned from other projects/missions/domains into account. **BD-3 - Every user involved in activities related to the project shall be subjected to user authentication**. (Zero Trust model)
Speed up development / pressure	**SUD/P-1** - Prioritizing speed over thoroughness in design, code analysis, and testing can leave vulnerabilities in the final product. This must be tackled with the opposite, by following the good and secure development practices.
Lack of certification of space systems	**LCSS-1** - Unlike industries like aviation (FAA) and railways (TUV), space systems lack comprehensive certification processes that include cybersecurity aspects.
Lack of vulnerability / threat analysis	**LV&TA-1 - Awareness trainings** **LV&TA-2 - Security testing** **LV&TA-3 - Enforcing security standards** **LV&TA-4 - Conducting independent regular security audits**

Threat	Mitigation
	LV&TA-5 - Ensure a SDLC is integrated in the application development. **LV&TA-6 - Training on security aspects, V&V** **LV&TA-7 - Check of OSS libraries vulnerabilities.** **LV&TA-8 - Vulnerability / Threats Analysis done before requirements are closed.** **LV&TA-9 - Security reviews**
Exploit development tools	**EDT-1 - Security reviews** **EDT-2 - Check of OSS libraries vulnerabilities.** **EDT-3 - Robustness testing** **EDT-4 - Do a deep analysis and test all interfaces (Zero Trust model)** **EDT-5 - Conducting independent regular security audits** **EDT-6 - Security testing**
Unmitigated errata	**UE-1 - Errata analysis** **UE-2 - Security reviews**

Table 4: Threats identified by the specialists

4. VULNERABILITIES AND MITIGATIONS

Building upon the foundation laid in the previous technical note, TN04 – Space System Threats and Vulnerabilities [RD-26], this chapter delves into vulnerabilities. A vulnerability is a flaw or weakness within an asset's design, implementation, operation, or management. These weaknesses can be exploited by threats, potentially compromising the asset.

The subsequent sections will present mitigation techniques designed to address these vulnerabilities and enhance the overall security posture of space systems.

4.1. HUMAN FACTOR

The human factor represents a significant vulnerability in space systems and critical infrastructure across various industries. Humans design and build software and hardware, inevitably introducing vulnerabilities where human intervention occurs. Humans are also targets for cyberattacks, particularly social engineering. To mitigate these risks, organizations must invest heavily in building a strong cybersecurity culture and training their employees to be vigilant against the ever-present dangers, already discuss in section 3.2.2.

4.2. DEVELOPMENT LIFE CYCLE

The lifespan and security requirements of space missions vary widely. Some missions may last 5 years, while others may operate for 25 years or more. To address these diverse needs, it is essential to adopt distinct secure software development lifecycles (SSDLCs) to avoid long-term problems.

The Software Security Development Lifecycle (SSDLC) provides a framework that integrates security considerations throughout every stage of the software development process. This "security by design" approach ensures that developers prioritize security concerns from the project's inception.

Several examples of SSDLC frameworks exist, both in the space domain and other industries. The technical note on state-of-the-art cybersecurity for space and other domains identifies four prominent SSDLC frameworks [RD-18]:

- **SSDLC -1 - Microsoft Security Development Lifecycle (SDL):** A comprehensive process that covers security practices throughout the entire software development lifecycle, from planning to maintenance.
- **SSDLC -2 - Software Security Touchpoints:** A lightweight framework that focuses on key security activities at critical points in the development process.
- **SSDLC -3 - Software Assurance Forum for Excellence in Code (SAFECode):** A collaborative effort by leading software companies to develop and promote best practices for software assurance.
- **SSDLC -4 - NIST Secure Software Development Framework (SSDF):** A set of fundamental, sound, and secure software development practices based on established secure software development practice documents.

By tailoring the choice of SSDLC framework to the specific needs and constraints of each space mission, organizations can significantly improve the security and resilience of their software systems over the long term.

4.3. SUPPLY CHAIN

The supply chain is a significant vulnerability for space organizations. Space systems consist of numerous components often manufactured by diverse companies worldwide, which may operate under varying cybersecurity regulations and enforcement. This inconsistency introduces potential vulnerabilities that malicious actors could exploit.

To protect the supply chain, the sector could implement the following measures [RD-16][RD-19][RD-20][RD-21][RD-28]:

- **SC-1 - Enforce Cybersecurity Requirements:** Impose strict cybersecurity requirements for commercial technologies and off-the-shelf components used in both civilian and military space assets. Frameworks like the Cybersecurity Maturity Model Certification (CMMC) could be adopted.
- **SC-2 - Supply Chain Risk Management (SCRM):** Establish a robust SCRM program incorporating software assurance methods to minimize the likelihood of malware introduction into components and modules.
- **SC-3 - Obtain Products from Trusted Suppliers:** Prioritize suppliers with a proven track record of security and quality assurance. Verify their compliance with relevant cybersecurity standards and practices.
- **SC-4 - Component Maintenance:** Continuously monitor integrated components for any unauthorized modifications. Address known vulnerabilities identified by the team, community, or supplier through regular updates and patches. Maintain direct communication between the supplier and customer to ensure timely updates and support.
- **SC-5 - Software Bill of Materials (SBOM):** Maintain a detailed list of third-party components to facilitate validation and vulnerability identification. Examples of SBOM formats include:
  - The Linux Foundation's Software Package Data Exchange (SPDX)
  - OWASP CycloneDX
  - NIST Software Identification Tags
- **SC-6 - Harden the Build Environment:** Ensure that the environment used to build and assemble components is secure and free from potential vulnerabilities.
- **SC-7 - Promoting Security in Government Contracts:** Enforce strict cybersecurity standards in government contracts to incentivize commercial vendors to prioritize security in their products, potentially leading to industry-wide improvements.
- **SC-8 - Regulatory Framework for Private Sector Activities:** Create a regulatory framework to manage the growing private sector space activities, ensuring compliance with existing space treaties like the Outer Space Treaty while promoting industry efforts to strengthen cybersecurity and collaboration.
- **SC-9 - Use of Advanced Technology:** Leverage advanced technologies like blockchain to enhance the security, authenticity, and integrity of software and hardware throughout the supply chain. The decentralized and immutable nature of blockchain can bring transparency, security, and traceability to every component [RD-20].

4.4. COMMERCIAL-OFF-THE-SHELF

The rapid increase in the number of actors participating in the space sector is largely due to the availability of affordable commercial-off-the-shelf (COTS) software and hardware. Small companies can now easily enter the space domain by purchasing these products and assembling them without the need to develop software from scratch. However, COTS products are often highly complex, composed of millions of lines of code, with their inner workings not always clear to the user.

Therefore, thorough security analysis is crucial.

Mitigation/Solution

COTS-1 – Security Analysis: Black-box testing techniques such as fuzzing, boundary value analysis, and equivalence partitioning can be employed to assess the product's robustness. Additionally, ensuring compliance with established security guidelines, like Security Technical Implementation Guides (STIGs), and regularly checking for and addressing vulnerabilities listed in the OWASP Top Ten is essential for maintaining a secure system [RD-6].

4.5. TECHNOLOGICAL EVOLUTION

Since the space sector supports society and various industries, including critical ones, depend on it, any disruption to its operations can have worldwide repercussions, causing severe impacts on individuals and businesses alike. Therefore, it's imperative that the space sector remains at the forefront of technological evolution, particularly in the realm of cybersecurity.

Here are some examples of technological advancements that have enhanced cybersecurity in the space sector [RD-6]:

- **TE-1 - Software-Defined Radio (SDR):** SDRs offer software control over functions traditionally performed by hardware, such as filtering, modulation, and mixing. This reduces the reliance on hardware, freeing up space for other components, and enables low-cost signal authentication solutions like fingerprint embedding, which acts as an authentication tag over message waveforms.
- **TE-2 - Cloud Computing:** Shifting data processing and storage from personal computers to secure data centers, accessible via the internet, enhances flexibility, availability, and redundancy. This allows for better management of customer scheduling needs through browser applications and provides protection against cyberattacks.
- **TE-3 - Optical Communication:** Moving away from traditional radio frequency (RF) communication, optical communication uses visible light for satellite communication. This technology is less vulnerable to jamming and other RF-based electronic warfare tactics.
- **TE-4 - Quantum Key Distribution (QKD):** This emerging field of cryptography holds the key to future-proofing encryption. While traditional encryption algorithms could be compromised by powerful quantum computers in the future, QKD utilizes quantum mechanics to establish secret keys with unconditional post-quantum security [RD-20].
- **TE-5 - Ground Station as a Service (GSaaS):** This method aims to reduce the cost of acquiring infrastructure by enabling users to communicate with, process data from, control, and monitor satellites via the cloud using a simple laptop or desktop computer [RD-24].

4.6. STATIC CODE ANALYSIS TOOLS

Organizations heavily rely on information technology, necessitating proactive measures to safeguard their confidential data. Cybersecurity tools play a vital role by continuously monitoring computer systems and networks, helping companies and individuals maintain data privacy and security.

One such tool is Static Code Analysis (SCA), along with threat/vulnerability detection tools.

Mitigation/Solution

SCA-1 - Static Code Analysis: These tools play a crucial role in preventing vulnerabilities by analyzing source code to identify potential issues, bad practices, and vulnerabilities before they are exploited. A comprehensive list of tools with these characteristics can be found in technical note TN01 [RD-18].

4.7. SECURITY ANALYSIS (THREATS AND VULNERABILITIES)

This step focuses on identifying and understanding potential threats and vulnerabilities within a system. It is crucial for organizations, particularly those in the space sector, to conduct thorough security analyses **before finalizing requirements**. Several methods can be employed to perform this task effectively (from report of the survey) [RD-18]:

- **SA-1 - Threat Modelling:** This involves systematically identifying and assessing potential threats to a system, analysing their potential impact, and developing strategies to mitigate those risks.
- **SA-2 - Network Security Monitoring:** By analysing network traffic with tools like packet sniffers, security teams can extract data to be analysed, enabling the detection and prevention of attacks.
- **SA-3 - Vulnerability Scanning:** Automated tools scan the system for known vulnerabilities, such as outdated software or misconfigurations.
- **SA-4 - Penetration Testing:** This involves simulating real-world attacks to identify and exploit vulnerabilities in a system's defences, providing a more comprehensive assessment of the system's security posture.
- **SA-5 - Input Validation:** Rigorous validation of user input helps prevent injection attacks and other vulnerabilities arising from unexpected or malicious data.
- **SA-6 - Independent Regular Security Audits:** Periodically conducting independent security audits by external experts helps identify vulnerabilities and ensures compliance with industry best practices.
- **SA-7 - Fuzz Testing:** This software testing technique uncovers implementation bugs by injecting "random" or invalid input and analysing the system's behaviour.
- **SA-8 - Static Code Analysis:** This involves analysing the source code without executing it to identify potential issues, bad practices, and vulnerabilities.
- **SA-9 - Security Testing:** This encompasses various techniques like performance testing, simulated attacks (including buffer overflow and DoS testing), and equivalence class partitioning tests to assess a system's security posture under different conditions.

4.8. SECURITY REQUIREMENTS

Security requirements analysis is a critical process for protecting information and systems from cyber threats. To achieve this, it is essential to develop well-defined security requirements during the project design phase. This systematic process involves identifying, documenting, and refining the security needs of a system or organization.

Mitigation/Solution
SR-1 - Security Requirements Analysis: The first step is to identify and classify systems to assess their potential threats and vulnerabilities. After compiling a list of threats, a risk assessment is conducted to evaluate the likelihood and potential impact of each, allowing for the identification of the most significant risks. Based on these identified threats and risks, specific security requirements are established. Organizations can leverage commonly used cybersecurity standards, such as IEC 62443 [RD-25], to guide the development of these requirements.

4.9. SECURITY DESIGN

Based on the study and paper, titled "The Protection of Information in Computer Systems" done by Jerome H. Saltzer and Michael D. Schroeder in the 70s [RD-31], to have a good security design it must follow ten principles highlighted by the authors.

The main secure design principles are the following:

1. **Economy of Mechanism**: Design simplicity minimizes attack surfaces and aids code inspection.
2. **Fail-Safe Defaults**: Deny access by default, then grant permissions explicitly. Prioritize allowlists over denylists to prevent unauthorized access.
3. **Complete Mediation**: Check every access to every object, every time. Defense in depth is key.
4. **Open Design**: Security should rely on secret keys, not on obscurity. Embrace Kerckhoff's principle, which states that a cryptographic system's security depends solely on the secrecy of its keys.
5. **Separation of Privilege**: Multiple layers of protection, using different mechanisms, enhance security.
6. **Least Privilege**: Grant programs and users the minimum necessary rights (need-to-know basis).
7. **Least Common Mechanism**: Minimize shared components to limit the impact of a successful attack.
8. **Psychological Acceptability**: Balance security and usability to ensure user adoption.
9. **Work Factor**: Consider the attacker's resources when evaluating security measures.
10. **Compromise Recording**: Logging and evidence collection are vital for incident response.

These principles remain crucial guides in modern secure design. Following them can help avoid common vulnerabilities, but they must be complemented by secure implementation practices. The OWASP Top 10's inclusion of "Insecure Design" [RD-30] emphasizes the ongoing importance of design-level security.

4.10. SECURITY IMPLEMENTATION

In the security implementation phase of software development, the primary goal is to translate security requirements and design decisions into actual code. This critical stage demands meticulous attention to detail and a proactive approach to identify and mitigate potential vulnerabilities.

Adhering to secure coding guidelines and standards is paramount in this phase. These guidelines and standards, often established by industry organizations or internal teams, provide developers with a roadmap for writing code that is resistant to common security flaws.

Static Code Analysis tools are automated software solutions that analyse source code without executing it. They play a crucial role in the security implementation phase by acting as a vigilant second eye, scanning the code for potential security weaknesses and coding flaws that might have been missed during manual reviews [RD-26].

Besides secure coding practices and SCA tools, organizations should consider other security measures during the implementation phase, such as:

- **SI-1 - Code Reviews:** Conducting thorough code reviews by peers or security experts to identify potential issues that might have been missed by automated tools.
- **SI-2 - Threat Modeling:** Identifying potential threats and vulnerabilities early in the development process to proactively mitigate risks.
- **SI-3 - Security Testing:** Performing security testing, including penetration testing and fuzz testing, to simulate real-world attacks and assess the system's resilience.

4.11. SECURITY TESTING

Security validation and testing is a systematic process of evaluating the effectiveness of security controls in a system or organization. It serves as a form of proactive defence, testing the security of a system to identify weaknesses before attackers can exploit them.

The IEC 62443-4-1 standard [RD-25] includes a section that focuses on documenting the outcomes of all security testing. This documentation helps verify whether the security requirements are being met, ensuring the product is effectively maintained throughout its real-world use. Table 5 details tests that can be performed to assess if the applied security strategy is robust and well-established.

Security Verification and Validation Testing	Examples
SecT-1 - Security Requirements Testing	•Functional testing of security requirements •Performance and scalability testing •Boundary/edge condition, stress and malformed or unexpected input test
SecT-2 - Threat Mitigation Testing	•Create and execute mitigation plans •Create and execute plans for attempting to thwart each mitigation
SecT-3 - Vulnerability Testing	•Attack surface analysis •Black box known vulnerability scanning •Dynamic runtime resource management testing
SecT-4 - Penetration Testing	•Password cracking •Privilege escalation •Exploiting software vulnerabilities
SecT-5 - Independence of Testers	•Security consulting firms •Freelance security researchers •Internal audit teams with dedicated security expertise

Table 5: IEC 62443-4-1 Security Verification and Validation Testing [RD-18]

4.12. INSTALLATION/OPERATION/MAINTENANCE

Installation, Operation, and Maintenance (IOM) are three fundamental phases in the lifecycle of any system, from simple software applications to complex machinery or infrastructure. These phases ensure a system is set up properly, used effectively, and maintained for optimal performance throughout its lifespan.

Mitigating risks throughout the Installation, Operation, and Maintenance (IOM) phases is crucial for the security and longevity of any system. Key considerations include [RD-26]:

Installation:

- **IOM-1 - Security Checks:** Conduct thorough pre-installation security checks on all hardware and software components.
- **IOM-2 - Secure Configuration and Integration:** Ensure secure configuration and integration with existing infrastructure.
- **IOM-3 - Access Controls and Authentication Mechanisms:** Implement access controls and authentication mechanisms to restrict unauthorized access.

Operation:

- **IOM-4 - User Training:** Provide comprehensive user training to prevent accidental misconfigurations or misuse.
- **IOM-5 - Monitor System:** Monitor system logs for suspicious activity and potential security breaches.

- **IOM-6 - Regular Updates:** Regularly update software and firmware to address vulnerabilities.

Maintenance:

- **IOM-7 - Routine System Maintenance:** Perform routine system maintenance to prevent malfunctions and ensure optimal performance.
- **IOM-8 – Security Patches:** Apply security patches and updates promptly to protect against emerging threats.
- **IOM-9 - Regular Vulnerability Assessments:** Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses.
- **IOM-10 - Incident Response Plans:** Develop and test incident response plans to quickly address any security breaches.

4.13. OTHER VULNERABILITIES

The following vulnerabilities were identified through the cybersecurity survey titled "Survey on Cybersecurity Challenges and Solutions for Space Systems" [RD-27], conducted among space sector specialists. A summary of these vulnerabilities and respective mitigations is presented in Annex A.2.

Vulnerability	Mitigation
Software bugs with security impacts	•**SB-1 - Extensive code analysis** •**SB-2 - Security testing** •**SB-3 - Extensive V&V of the embedded device against fuzz inputs** •**SB-4 - Built-in or self-tests to ensure application and data integrity** •**SB-5 - Perform input validation** •**SB-6 - Integrity checks for all data, configurations, inputs to the system** •**SB-7 - Conducting independent regular security audits** •**SB-8 - Security reviews**
Weak development process	•**WDP-1 - Ensure a SDLC (Secure Development Life Cycle) is integrated in the application development.** •**WDP-2 - No agile methodology in security critical development**
Read and write operations in memory	•**R&W-1 - Robustness testing**
Software update	•**SU-1 - Authentication on software patch** •**SU-2 - Enforce patch management**
Weak software development protection	•**WSDP-1 - Protection of software development environments** •**WSDP-2 - Every user involved in activities related to the project shall be subjected to user authentication. (Zero Trust model)**
Debug ports not protected	•**DP-1 - Access to target memories through unprotected debug ports.**
Bad code practices	•**BCP-1 - Extensive code analysis** •**BCP-2 - Zero code smells and zero warnings objective**
Lack of security acceptance plan	•**LSAP-1 - Acceptance plans are often based on a subset of tests** that may not cover security or unusual situations. Contracts can also be a vulnerability, as subcontractors might prioritize scope over security, creating gaps.
Weak secure information and deliverables flow	•**WSI&DF-1 - More secure information and deliverables flow.** •**WSI&DF-2 - Use of certified tools**

Vulnerability	Mitigation
Weak secure boundary parameter	•**WSBP-1 - Robustness testing** •**WSBP-2 - Extensive code analysis**
Weak password policies	•**WPP-1 - Use cryptographic keys instead of passwords.**
High turnover of contractors	•**HTC-1 - Create a baseline workforce to be trained in cybersecurity.**
Use of dynamic memory	•**UDM-1 - Exclude dynamic memory in space systems.**
Deserialization of untrusted data	•**DUD-1 - Security reviews**
Integer overflow of wraparound	•**IOW-1 - Extensive code analysis**
Improper monitoring in ground and space segment	•**IM-1 - Intrusion detection mechanisms** •**IM-2 - Robust FDIR configuration** •**IM-3 - Firewall**
Poor management of the exchange data	•**PMED-1 - Advanced encryption** •**PMED-2 - Proper authentication methods and access control**.

Table 6:Vulnerabilities and respective mitigations identified by the experts[RD-27]

ANNEXES

ANNEX A. THREATS AND VULNERABILITIES MITIGATIONS SUMMARY

A.1 THREATS SOLUTIONS SUMMARY TABLE

The following Table 7 depicts the summary of proposed mitigations used against a specific number of threats relevant for space systems identified in the TN04 [RD-26] and described in the body of this document.

ID	Threat	Threat Source	Solutions / Mitigations	Solution / Mitigation Source
1	Solar Radio Burst	[RD-3], [RD-4], [RD-5]	•**SRB-1**	[RD-3]
2	SEE – Burnout	[RD-4]	•**SEE-1**	[RD-4]
3	SEE – Functional Interrupt	[RD-4]	•**SEE-2**	[RD-4]
4	SEE – Gate Rupture	[RD-4]	•**SEE-3**	[RD-4]
5	SEE – Latchup	[RD-4]	•**SEE-4**	[RD-4]
6	SEE – Multiple Bit Upset	[RD-4]	•**SEE-5**	[RD-4]
7	SEE – Multiple Cell Upset	[RD-4]	•**SEE-6**	[RD-4]
8	SEE – Transient Errors	[RD-4]	•**SEE-7**	[RD-4]
9	Jamming	[RD-4], [RD-6], [RD-9]	•**JAM-1** •**JAM-2** •**JAM-3** •**JAM-4** •**JAM-5** •**JAM-6** •**JAM-7** •**JAM-8**	[RD-7], [RD-28]
10	Spoofing	[RD-4], [RD-6], [RD-9]	•**SPOO-1** •**SPOO-2** •**SPOO-3** •**SPOO-4** •**SPOO-5** •**SPOO-6** •**SPOO-7**	[RD-6], [RD-8]
11	Eavesdropping	[RD-4], [RD-6], [RD-9]	•**EAV-1** •**EAV-2**	[RD-9]
12	Signal Hijacking	[RD-4], [RD-6], [RD-13]	• **SH-1** •**Section 3.1.2.3**	[RD-9], [RD-10]
13	Data Corruption and Interception	[RD-4], [RD-6], [RD-13]	•**DC&I-1** •**DC&I-2** •**DC&I-3** •**DC&I-4** •**DC&I-5** •**DC&I-6**	[RD-9], [RD-11], [RD-13]
14	Denial-of-Service	[RD-4], [RD-6], [RD-8] [RD-9], [RD-11], [RD-19]	•**DoS-1** •**DoS-2**	[RD-12], [RD-13], [RD-27], [RD-28]

ID	Threat	Threat Source	Solutions / Mitigations	Solution / Mitigation Source
			•DoS-3 **•DoS-4** **•DoS-5** **•DoS-6** **•DoS-7** **•DoS-8** **•DoS-9**	
15	Web Spoofing	[RD-12]	**•WS-1** **•WS-2** **•WS-3** **•WS-4** **•WS-5** **•WS-6** **•WS-7** **•WS-8** **•WS-9** **•WS-10** **•WS-11**	[RD-14], [RD-28]
16	Software Threats	[RD-9], [RD-19], [RD-20]	**•ST-1** **•ST-2** **•ST-3** **•ST-4** **•ST-5** **•ST-6** **•ST-7** **•ST-8** **•ST-9** **•ST-10**	[RD-12], [RD-28]
17	Man in the Middle	[RD-12]	**•MITM-1** **•MITM-2** **•MITM-3** **•MITM-4**	[RD-12]
18	Zero-days Exploits	[RD-27]	**•ZDE-1** **•ZDE-2** **•ZDE-3**	[RD-16], [RD-27]
19	Password Attacks	[RD-27]	**•PA-1**	[RD-27]
20	Injection Attacks	[RD-9], [RD-12], [RD-19]	**•IATT-1** **•IATT-2** **•IATT-3**	[RD-12]
21	Social Engineering	[RD-4], [RD-12], [RD-17]	**•SE-1** **•SE-2** **•SE-3** **•SE-4**	[RD-12], [RD-16], [RD-17]
22	Source Code Tampering	[RD-27]	**•SCT-1** **•SCT-2** **•SCT-3** **•SCT-4**	[RD-27]

ID	Threat	Threat Source	Solutions / Mitigations	Solution / Mitigation Source
			•**SCT-5** •**SCT-6**	
23	Spacecraft configuration modification	[RD-27]	•**SCM-1** •**SCM-2** •**SCM-3** •**SCM-4** •**SCM-5** •**SCM-6** •**SCM-7** •**SCM-8** •**SCM-9**	[RD-27]
24	Bad design	[RD-27]	•**BD-1** •**BD-2** •**BD-3**	[RD-27]
25	Speed up development / pressure	[RD-27]	•**SUD/P-1**	[RD-27]
26	Lack of certification of space systems	[RD-27]	•**LCSS-1**	[RD-27]
27	Lack of vulnerability / threat analysis	[RD-27]	•**LV&TA-1** •**LV&TA-2** •**LV&TA-3** •**LV&TA-4** •**LV&TA-5** •**LV&TA-6** •**LV&TA-7** •**LV&TA-8** •**LV&TA-9**	[RD-27]
28	Exploit development tools	[RD-27]	•**EDT-1** •**EDT-2** •**EDT-3** •**EDT-4** •**EDT-5** •**EDT-6**	[RD-27]
29	Unmitigated errata	[RD-27]	•**UE-1** •**UE-2**	[RD-27]

Table 7: Threat propose solutions

A.2 VULNERABILITIES SOLUTIONS SUMMARY TABLE

The following Table 8 depicts the summary of proposed mitigations used against a specific number of vulnerabilities relevant for space systems identified in the TN04 [RD-26].

ID	Vulnerability	Vulnerability Source	Solutions/Mitigations	Solutions/Mitigations Source
1	Human Factor	[RD-4], [RD-6], [RD-12]	•**Section** 3.2.2	[RD-12], [RD-16], [RD-17]
2	Development Life Cycle	[RD-27]	•**SSDLC -1** •**SSDLC -2**	[RD-18]

ID	Vulnerability	Vulnerability Source	Solutions/Mitigations	Solutions/Mitigations Source
			•**SSDLC -3** •**SSDLC -4**	
3	Supply Chain	[RD-4], [RD-6], [RD-9], [RD-16], [RD-19], [RD-22], [RD-27]	•**SC-1** •**SC-2** •**SC-3** •**SC-4** •**SC-5** •**SC-6** •**SC-7** •**SC-8** •**SC-9**	[RD-16], [RD-19], [RD-20], [RD-21], [RD-22]
4	Commercial-off-the-Shelf	[RD-5], [RD-6], [RD-9], [RD-16], [RD-19], [RD-22], [RD-27]	•**COTS-1**	[RD-6]
5	Technological Evolution	[RD-6], [RD-27]	•**TE-1** •**TE-2** •**TE-3** •**TE-4** •**TE-5**	[RD-6]
6	Static Code Analysis Tools	[RD-27]	•**SCA-1**	[RD-27]
7	Security Analysis	[RD-18], [RD-27]	•**SA-1** •**SA-2** •**SA-3** •**SA-4** •**SA-5** •**SA-6** •**SA-7** •**SA-8** •**SA-9**	[RD-18]
8	Security Requirements	[RD-27]	•**SR-1**	[RD-25]
9	Security Design	[RD-27]	•Ten secure design principles (section 4.9)	[RD-29]
10	Security Implementation	[RD-27]	•**SI-1** •**SI-2** •**SI-3**	[RD-26]
11	Security Testing	[RD-27]	•**SecT-1** •**SecT-2** •**SecT-3** •**SecT-4** •**SecT-5**	[RD-18]
12	Installation/Operation/Maintenance	[RD-27]	•**IOM-1** •**IOM-2** •**IOM-3** •**IOM-4** •**IOM-5** •**IOM-6**	[RD-26], [RD-27]

ID	Vulnerability	Vulnerability Source	Solutions/Mitigations	Solutions/Mitigations Source
			•**IOM-7** •**IOM-8** •**IOM-9** •**IOM-10**	
13	Software bugs with security impacts	[RD-27]	•**SB-1** •**SB-2** •**SB-3** •**SB-4** •**SB-5** •**SB-6** •**SB-7** •**SB-8**	[RD-27]
14	Weak development process	[RD-27]	•**WDP-1** •**WDP-2**	[RD-27]
15	Read and write operations in memory	[RD-27]	•**R&W-1**	[RD-27]
16	Software update	[RD-27]	•**SU-1** •**SU-2**	[RD-27]
17	Weak software development protection	[RD-27]	•**WSDP-1** •**WSDP-2**	[RD-27]
18	Debug ports not protected	[RD-27]	•**DP-1**	[RD-27]
19	Bad code practices	[RD-27]	•**BCP-1** •**BCP-2**	[RD-27]
20	Lack of security acceptance plan	[RD-27]	•**LSAP-1**	[RD-27]
21	Weak secure information and deliverables flow	[RD-27]	•**WSI&DF-1** •**WSI&DF-2**	[RD-27]
22	Weak secure boundary parameter	[RD-27]	•**WSBP-1** •**WSBP-2**	[RD-27]
23	Weak password policies	[RD-27]	•**WPP-1**	[RD-27]
24	High turnover of contractors	[RD-27]	•**HTC-1**	[RD-27]
25	Use of dynamic memory	[RD-27]	•**UDM-1**	[RD-27]
26	Deserialization of untrusted data	[RD-27]	•**DUD-1**	[RD-27]
27	Integer overflow of wraparound	[RD-27]	•**IOW-1**	[RD-27]
28	Improper monitoring in ground and space segment	[RD-27]	•**IM-1** •**IM-2** •**IM-3**	[RD-27]
29	Poor management of the exchange data	[RD-27]	•**PMED-1** •**PMED-2**	[RD-27]

Table 8: Vulnerability proposed mitigations

Critical software

We are CMMI Maturity Level 5 rated.

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

www.criticalsoftware.com