Critical Software
TN06: Proposals to Change/Improve/Integrate Specific Requirements into the ECSS E40 & Q80

CYBERSECURITY FOR SPACE

CONTRACT REFERENCE: NOT APPLICABLE.

DATE: 2024-09-16
PROJECT CODE: CSEC4SPACE
DOC. REF.: CSW-2024-TNR-04549
STATUS: APPROVED
PAGES: 16
INFORMATION CLASSIFICATION: PUBLIC
VERSION: 1.0

DISCLAIMER -

The work described in this report was performed under the Master’s degree research title “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		2024-09-16
1.0	João Carlos Cunha	Academic Supervisor		2024-09-16

AUTHORS AND CONTRIBUTORS

NAME	DESCRIPTION	DATE
Pedro Miguel Sousa	Author	2024-06-14
Nuno Silva	Reviewer	2024-09-13

COPYRIGHT

REVISION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR
0.1	2024-09-13	First revision of the technical note.	Pedro Sousa
1.0	2024-09-16	Document reviewed and modifications applied and approved for release.	Pedro Sousa

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

No table of figures entries found.

1. INTRODUCTION

1.1. OBJECTIVE

This technical note proposes improvements (suggestions for standard requirements) to the ECSS standards, specifically ECSS-E-ST-40C [RD-1] and ECSS-Q-ST-80C [RD-2], regarding cybersecurity topics. The aim is to strengthen these standards to ensure more secure space applications.

1.2. SCOPE

This document builds on the previous technical notes (namely TN04 [RD-3] and TN05 [RD-4]), where space systems threats, vulnerabilities and associated mitigations have been identified/proposed and promotes the exercise of mapping the proposed mitigation to the existing ECSS standards for space software engineering and space software quality assurance (ECSS-E-ST-40C [RD-1] and ECSS-Q-ST-80C [RD-2]). The scope of this document is the proposal of generic requirements of the two mentioned ECSS standards in complement to the current software engineering requirements already listed in those standards.

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, as well as the ECSS Working groups.

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.
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

NAME	DESCRIPTION
	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
AES	Advanced Encryption Standard
CMMC	Cybersecurity Maturity Model Certification
COTS	Commercial-off-the-shelf
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
ECC	Error-correcting Codes
ECSS	European Cooperation for Space Standardization
ESA	European Space Agency
FAA	Federal Aviation Administration
FDIR	Fault detection, isolation, and recovery
GSaaS	Ground Station-as-a-Service
IOM	Installation, Operation, and Maintenance
ISVV	Independent Software Verification and Validation
NIST	National Institute of Standards and Technology
OSS	Open-Source Software
OWASP	Open Worldwide Application Security Project
QKD	Quantum Key Distribution

ACRONYM	DESCRIPTION
RSA	Rivest-Shamir-Adleman
SBOM	Software Bill of Materials
SCRM	Supply Chain Risk Management
SDL	Security Development Lifecycle
SDR	Software-Defined Radio
SHA	Secure Hash Algorithm
SSDF	NIST Secure Software Development Framework
SSDLC	Secure software development lifecycles

Table 2: Acronyms

1.5. DOCUMENT STRUCTURE

Section 1 (Introduction) presents this document.

Section 2 (Threats, Vulnerabilities and Proposals of cybersecurity) presents the cybersecurity proposals to the ECSS standards.

Section 3 (Conclusions) summarizes the outcome of this technical note namely the proposed requirements for the ECSS standards.

1.6. REFERENCE DOCUMENTS

Table 3 presents the list of reference documents.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-1] ECSS-E-ST-40C - Software	https://ecss.nl/standard/ecss-e-st-40c-software-general-requirements/, visited on 2024-09-13.
[RD-2] 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 2024-09-13.
[RD-3] TN04: Space systems threats and vulnerabilities	CSW-2024-TNR-04549, v1.0
[RD-4] TN05: Proposals to Cope Threats and Vulnerabilities	CSW-2024-TNR-03939, v1.0
[RD-5] Report – Cybersecurity Survey	CSW-2024-TNR-03904, v. 1.1

Table 3: Reference documents

2. THREATS, VULNERABILITIES AND PROPOSALS OF CYBERSECURITY REQUIREMENTS

This technical note presents several proposals aimed at enhancing the cybersecurity standards of the European Cooperation for Space Standardization (ECSS), specifically focusing on the ECSS-E-ST-40 (6 March 2009) [RD-1] and ECSS-Q-ST-80 (15 February 2017) [RD-2]. These proposals seek to address critical gaps in the current standards and provide a more comprehensive framework for mitigating cybersecurity risks in space systems.

The proposals listed in column “Proposal” of Table 4 and Table 5 are based on the threats and vulnerabilities identified in the technical notes TN04 "Space Systems Threats and Vulnerabilities" [RD-3] and the respective mitigations documented in TN05 "Proposals to Cope with Threats and Vulnerabilities" [RD-4]. Additionally, the proposals incorporate insights from the cybersecurity survey responses [RD-5]. These proposals are categorized into three types:

- **E40-P-xx**: Proposals primarily related to the E40 standard, focusing on software development.
- **Q80-P-xx**: Proposals primarily related to the Q80 standard, focusing on software assurance.
- **OTH-P-xx**: Proposals that fall outside the scope of both E40 and Q80.

Table 4 presents the proposed generic requirements to cope with the identified threats, mainly based on their associated mitigations. It should be noted that these requirements should be applied **whenever necessary** (i.e., when cybersecurity is applicable, which is not the case for all types of space applications).

THREATS	Mitigation	Proposal
Data Corruption and Interception	• 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.	**E40-P-01**: A Requirement on data integrity protection, intrusion detection and prevention. **Q80-P-01**: A Requirement on V&V of data integrity protection, intrusion detection and prevention
Software Threats	• 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	**E40-P-02**: A Requirement on the toolset environment and its protection, namely, that tools are up to date, known security issues are analysed and documented. **E40-P-03**: A Requirement on supply chain protection (see **E40-P-10**, **Q80-P-14**).

THREATS	Mitigation	Proposal
	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.	**Q80-P-02**: A Requirement on V&V of the toolset environment and its protection, namely, that tools are up to date, known security issues are analysed and documented. **Q80-P-03**: A Requirement on V&V of the supply chain protection (see **E40-P-10**, **Q80-P-14**).
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	**Q80-P-04**: Verify that code smells and warnings are checked, fixed or justified. **Q80-P-05**: Check that specific security assessments are performed on design and code.
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.	**E40-P-04**: A Requirement on intrusion detection and prevention, data integrity and authentication, and access control and geographical restrictions. **Q80-P-06**: A Requirement on V&V of intrusion detection and prevention, data integrity and authentication, and access control and geographical restrictions. **Q80-P-07**: A requirement on V&V of FDIR configurations.
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)	**E40-P-05**: A Requirement on secure-by-design approach, lessons learned from other domains and development environment authentication and access control. **Q80-P-08**: A Requirement on V&V of secure-by-design approach, lessons learned from other domains and development

THREATS	Mitigation	Proposal
		environment authentication and access control.
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.	**OTH-P-01**: A Requirement on prioritize thoroughness in development processes and adherence to 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	**OTH-P-02**: Recommend an independent cybersecurity assessment perform by ESA or the prime contractors. **Q80-P-09**: Reinforce that ISVV shall perform an independent cybersecurity analysis.
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 • 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	**E40-P-06**: A Requirement on vulnerability management, security reviews, and reinforce awareness and training, all referent to vulnerability / threat analysis. **Q80-P-10**: A Requirement on V&V of vulnerability management, security reviews, and reinforce awareness and training, all referent to vulnerability / threat analysis. (See also **E40-P-09**, **Q80-P-13**)
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	**E40-P-07**: A Requirement on Security Reviews and Testing, and Comprehensive Analysis and Testing, referring to development tools (tools assessment or certified tools). **Q80-P-11**: A Requirement on V&V of Security Reviews and Testing, and Comprehensive Analysis and Testing, referring to development tools (tools assessment or certified tools).
Unmitigated errata	• UE-1 - Errata analysis • UE-2 - Security reviews	**E40-P-08**: A Requirement on Errata Analysis and Mitigation, referring to unmitigated errata. **Q80-P-12**: A Requirement on V&V of Errata Analysis and Mitigation, referring to unmitigated errata.

Table 4: Threats, mitigations and respective requirements proposals

Table 5 presents proposed generic requirements to cope with the identified vulnerabilities, mainly based on their associated mitigations. It should be noted that these requirements should be applied **whenever necessary** (i.e., when cybersecurity is applicable, which is not the case for all types of space applications).

VULNERABILITIES	Mitigation	Proposal
Development Life Cycle	• 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.	**E40-P-09**: A Requirement on Implementing Comprehensive SDLC Frameworks, referring to development life cycle. **Q80-P-13**: A Requirement on V&V of Implementing Comprehensive SDLC Frameworks, referring to development life cycle.

VULNERABILITIES	Mitigation	Proposal
	• 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.	
Supply Chain	• 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. • 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.	**E40-P-10**: A Requirement on Enforcing Cybersecurity Requirements, Supply Chain Risk Management, Component Maintenance and Security, Regulatory Framework and Industry-Wide Improvements and Leveraging Advanced Technologies, referring to supply chain. **Q80-P-14**: A Requirement on V&V of Enforcing Cybersecurity Requirements, Supply Chain Risk Management, Component Maintenance and Security, Regulatory Framework and Industry-Wide Improvements and Leveraging Advanced Technologies, referring to supply chain.
Commercial-off-the-Shelf	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	**E40-P-11**: A Requirement on Security Analysis and Testing, referring to COTS. **E40-P-12**: A Requirement requesting

VULNERABILITIES	Mitigation	Proposal
	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	security analysis and assessments for all types of reused software. **Q80-P-15**: A Requirement on V&V of Security Analysis and Testing, referring to COTS. **Q80-P-16**: A Requirement on V&V of security analysis and assessments for all types of reused software.
Technological Evolution	• 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. • 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.	**OTH-P-03**: New technologies need to be fully assessed from security perspectives (threats and vulnerabilities analysis, interface impact with other technologies, risk analysis)
Security Analysis	• 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:	**E40-P-13**: A Requirement on Threat Modelling and Risk Assessment, Network Security Monitoring and Input Validation, referring to security analysis. **Q80-P-17**: A Requirement on V&V of Threat Modelling and Risk Assessment, Network Security Monitoring, Vulnerability Scanning and Testing, Input Validation, referring to security analysis. (See also **E40-P-16**, **E40-P-17**, for code analysis and **Q80-P-20**, **Q80-P-21**, for additional security testing techniques)

VULNERABILITIES	Mitigation	Proposal
	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.	
Security Requirements	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.	**E40-P-14**: A Requirement on security requirements analysis, referring to security requirements. **Q80-P-18**: A Requirement on V&V of security requirements analysis, referring to security requirements.
Security Design	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. Defence 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.	**E40-P-15**: A Requirement to reinforce the 10 principles of a secure design. **Q80-P-19**: A Requirement on V&V of the 10 principles of a secure design.
Security Implementation	• 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 Modelling: 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.	**E40-P-16**: A Requirement on Threat Modelling to be performed on development process to mitigate security risks. **E40-P-17**: A Requirement on Code Reviews focused on security topics. **Q80-P-20**: A Requirement on V&V of Threat Modelling to be performed on development process to mitigate security risks.

VULNERABILITIES	Mitigation	Proposal
		Q80-P-21: A Requirement on V&V of Code Reviews focused on security topics.
Security Testing	• SecT-1 - Security Requirements Testing • SecT-2 - Threat Mitigation Testing • SecT-3 - Vulnerability Testing • SecT-4 - Penetration Testing • SecT-5 - Independence of Testers	**E40-P-18**: A Requirement on a Comprehensive Security Testing that shall be included in the test plan. **Q80-P-22**: A Requirement on V&V of the Comprehensive Security Testing that shall be included in the test plan.
Installation/Operation/Maintenance	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.	**E40-P-19**: A Requirement on security checks before installation, secure configuration and integration with the existing infrastructure and access control and authentication mechanism during installation. **E40-P-20**: A Requirement on user training concerning security, monitoring the system for security concerns and regular security updates. **E40-P-21**: A Requirement for routine system maintenance, security patches, regular vulnerability assessments and incident response plans. **Q80-P-23**: A Requirement on V&V of security checks before installation, secure configuration and integration with the existing infrastructure and access control and authentication mechanism during installation. **Q80-P-24**: A Requirement on V&V of user training concerning security, monitoring the system for security concerns and regular security updates. **Q80-P-25**: A Requirement on V&V of routine system maintenance, security patches, regular vulnerability assessments and incident response plans.
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	**Q80-P-26**: A Requirement on analysing any software issue for potential security impacts (Data Integrity and Input Validation, Independent Security Audits, Reviews, Code Analysis and Security Testing).
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	**OTH-P-04**: A Requirement on Cautious Use of Agile Methodologies, to avoid a weak development process. (see also E40-P-09 and Q80-P-13)
Software update	• SU-1 - Authentication on software patch • SU-2 - Enforce patch management	**E40-P-22**: A Requirement on Authentication and Patch Management, referring to software update.

VULNERABILITIES	Mitigation	Proposal
		Q80-P-27: A Requirement on V&V of Authentication and Patch Management, referring to software update.
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)	(See **E40-P-05**, **Q80-P-08**, for authentication and **E40-P-02**, **E40-P-03**, **Q80-P-02**, **Q80-P-03** for software development environment protection.)
Debug ports not protected	• DP-1 - Access to target memories through unprotected debug ports.	**Q80-P-28**: A Requirement to ensure that debug ports are disabled for flight software.
Bad code practices	• BCP-1 - Extensive code analysis • BCP-2 - Zero code smells and zero warnings objective	**Q80-P-29**: A Requirement on verify that code smells and warnings are checked, fixed or justified.
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.	**Q80-P-30**: A Requirement to ensure that security and unusual are covered by the acceptance plan.
Weak secure information and deliverables flow	• WSI&DF-1 - More secure information and deliverables flow. • WSI&DF-2 - Use of certified tools	**E40-P-23**: One Requirement to ensure the secure delivery of all project information. (see also **E40-P-07**, **Q80-P-11**)
Weak password policies	• WPP-1 - Use cryptographic keys instead of passwords.	**E40-P-24**: A Requirement to ensure a strong password policy or cryptographic keys.
High turnover of contractors	• HTC-1 - Create a baseline workforce to be trained in cybersecurity.	**OTH-P-05**: A Requirement on comprehensive and documented cybersecurity training.
Deserialization of untrusted data	• DUD-1 - Security reviews	**E40-P-25**: A Requirement to ensure secure deserialization of untrusted data. **Q80-P-31**: A Requirement on V&V of the secure deserialization of untrusted data.
Improper monitoring in ground and space segment	• IM-1 - Intrusion detection mechanisms • IM-2 - Robust FDIR configuration • IM-3 - Firewall	**E40-P-26**: A Requirement to ensure intrusion detection in the flight software if needed. **OTH-P-06**: A Requirement to ensure intrusion detection and firewall protection to ground systems. (See **E40-P-04**, **Q80-P-06**, **Q80-P-07**)
Poor management of the exchange data	• PMED-1 - Advanced encryption • PMED-2 - Proper authentication methods and access control	(see **E40-P-01**, **Q80-P-01**)

Table 5: Vulnerabilities, mitigations and respective requirements proposals

3. CONCLUSIONS

This technical note has presented a comprehensive set of proposals aimed at enhancing the cybersecurity of space systems. The proposed generic requirements arise from the previous technical notes TN04 [RD-3], TN05 [RD-4] and also the cybersecurity survey on space systems [RD-5].

In total, 63 proposals have been presented, being:

- 26 requirements proposed for ECSS-E-ST-40C,
- 31 requirements proposed for ECSS-E-ST-Q-80C, and
- 6 requirements proposed other engineering/project/contract areas.

These proposals address key vulnerabilities and threats identified in previous research and analysis and intend to help the space industry in strengthening the security of space systems.

Lastly, these proposed requirements should be seen as such (proposals) to help the respective (E40 and Q80) ECSS Working Groups into improving the cybersecurity engineering of space systems.

Critical
software

We are CMMI Maturity Level 5 rated.

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

www.criticalsoftware.com