ECSS-E-ST-80C
1 July 2024

Space engineering

Security in space systems lifecycles

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Section
Noordwijk, The Netherlands

Foreword

ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards. Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

This Standard has been prepared by the ECSS-E-ST-80C Working Group, reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

Disclaimer

Published by: ESA Requirements and Standards Section
ESTEC, P.O. Box 299,
2200 AG Noordwijk
The Netherlands

Change log

ECSS-E-ST-80C 1 July 2024	First issue

Table of contents

Figures

Tables

Introduction

Security is a broad domain, affecting people, processes, and technologies. Application of security within all parts of an organisation and its activities are necessary for a coherent and structured approach to security. Security needs to apply to the system(s) to be operated, the systems used to enable security, the facilities to host and provide the global context, and the processes and methods used. Security must evolve and vary depending upon the threats and security risks, phase of the activity, regulations, the resources, and mechanisms selected to host and share the assets. On top of this, security is needed to be addressed when choosing the design, implementation aspects, mitigations to vulnerabilities, and the resources used to develop, operate, maintain, and dispose of the system.

The objective of this standard is to ensure a systematic and consistent consideration and implementation of a secure lifecycle for space systems.

As mentioned at the beginning, security is a broad domain covering many different aspects, technological, engineering or process related, etc. Therefore, this standard is intended to be accompanied by a set of handbooks or even additional security standards focused on specific security aspects.

1
Scope

This standard provides requirements on the implementation of security in space systems, and requirements on the processes implemented during their lifecycle. This means ensuring the correct implementation of required security functionality in the system (e.g., implementation of an Information Security Management System in the ground segment); and also ensuring reasonable security of the lifecycle itself (e.g., ensuring reasonable management of design information). Space systems include manned and unmanned spacecraft, launchers, payloads, experiments and their associated ground equipment and facilities. Specifically, in the scope of this document are the Space Segment, Ground Segment, Launch Segment, and Support Segment, as defined in ECSS-S-ST-00-01, during their whole lifecycle (from definition, design, development, to operation and decommission).

This standard considers the wide variety of security aspects that must be examined during the lifetime of a space system, including potential certification needs, allowing a tailoring to adapt to specific missions and services. It also considers the interaction between security of the system and its lifecycle, and the corporate security of the organisations involved. This standard is applicable to unclassified missions and projects, and used or tailored, as needed, abiding by national and inter-governmental rules for classified governmental security projects that often require additional processes and controls (such as formal System Security Accreditation); however, System Security Accreditation process is out of scope of this standard. Corporate security is usually specific to each organisation and may be constrained by national regulations or standards. Therefore, this standard avoids imposing unnecessary constraints that conflict with corporate security of the organisations involved in the lifecycle.

A security risk assessment should support the identification of sensitive information as well as the corresponding required protective security marking and measures.

This standard interfaces with space engineering and management, which are addressed in the Engineering (-E) and Management (-M) branches of the ECSS System.

This standard may be tailored for the specific characteristics and constraints of a space project in conformance with ECSS-S-ST-00.

2
Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revision of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the more recent editions of the normative documents indicated below. For undated references, the latest edition of the publication referred to applies.

ECSS-S-ST-00-01	ECSS system — Glossary of terms
ECSS-E-ST-40	Space engineering – Software
ECSS-Q-ST-10	Space product assurance – Product assurance management
ECSS-Q-ST-80	Space product assurance – Software product assurance

3
Terms, definitions and abbreviated terms

3.1 Terms from other standards

a. For the purpose of this Standard, the terms and definitions from ECSS-S-ST-00-01 apply, in particular for the following terms:

NOTE The terms defined in ECSS-S-ST-00-01 have preference over the terms defined in CCSDS 350.8-M-3.

1. acceptance
2. analysis
3. assurance
4. audit
5. availability
6. component
7. conformance
8. contract
9. COTS
10. customer
11. design
12. dependability
13. development
14. element
15. fail safe
16. ground segment
17. incident
18. launch segment
19. lifecycle
20. lifetime
21. maintenance
22. mission

23. process
24. product
25. product assurance
26. project
27. redundancy
28. reliability
29. requirements
30. space missions
31. space segment
32. space system
33. spacecraft
34. subsystem
35. supplier
36. support segment
37. support system
38. system
39. tailoring
40. validation
41. verification
42. waiver

b. For the purpose of this Standard, the terms and definitions from ECSS-E-ST-40 apply, in particular for the following terms:

1. software

3.2 Terms specific to the present standard

In this clause the terms specific to this standard are defined. As potential sources, various creditable ones have been considered (ISO, CCSDS, NIST, IETF, ESA Security Directives). The ones used were chosen on their suitability for the intended purpose of this document (and if needed modified) and not following any specific "hierarchy" in the adoption.

3.2.1 access control

prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

[CCSDS 350.8-M-3]

3.2.2 accountability

assignment of responsibility for actions and decisions to an entity

NOTE Adapted from ISO/IEC 27000

3.2.3 asset

anything that has value to a person or organization

NOTE There are many types of assets, including:

1. information;
2. software, such as a computer program;
3. hardware, such as computer;
4. services;
5. people, and their qualifications, skills, and experience; and intangibles, such as reputation and image.

[NIST SP 800-160v1r1, ISO/IEC/IEEE 24765:2017]

3.2.4 attack

attempt to destroy, expose, alter, disable, steal, make unavailable, deceive, disrupt, or gain unauthorized access to or make unauthorized use of an asset

NOTE Adapted from ISO/IEC 27000

3.2.5 attack vector

the context by which vulnerability exploitation is possible

[Common Vulnerability Scoring System version 4.0: Specification Document]

3.2.6 authentication

process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data

[CCSDS 350.8-M-3]

NOTE An authentication process consists of two basic steps: 1) Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem. 2) Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed (see IETF RFC 4949).

3.2.7 authenticity

property of being genuine and able to be verified and trusted

[IETF RFC 4949]

3.2.8 authorisation

the right or a permission that is granted to a system entity to access a system resource

[IETF RFC 4949]

3.2.9 certification

formal statement issued by an appropriate authority, supported by an independent review of the conduct and the results of an evaluation, of the extent to which a system meets the security requirements, or a communications or computer security product meets predefined security claims

NOTE 1 Certification is performed by independent technical personnel to an acceptable standard of proof such that the level of security protection is identified with regard to procedure, programme, system component or system.

NOTE 2 A security claim is a statement to meet a number of agreed security requirements.

[CCSDS 350.8-G-1]

3.2.10 compromise

situation when some protected information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability

NOTE 1 Compromise arises due to a breach of security or adverse activity.

NOTE 2 A breach of security can refer to espionage, acts of terrorism, sabotage or theft. Compromise includes loss, disclosure to unauthorized individuals (e.g., through espionage or to the media) unauthorized modification, destruction in an unauthorized manner, or denial of service.

[ESA Security Directives]

3.2.11 confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[CCSDS 350.8-M-3] [ECSS-E-ST-70-11]

3.2.12 cyber

related to cyber space

3.2.13 cyber disaster

cyber incident that results in an extended cyber damage, making the eradication of the artefacts that lead to the cyber incident and the recovery of the affected system extremely difficult by the typical incident handling means and procedures

3.2.14 cyber incident

see definition of "**incident**"

3.2.15 cyber space

global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

[NIST SP 800-30 Rev. 1, NIST SP 800-39]

3.2.16 cyber security

ability to protect or defend the use of cyberspace from cyber attacks

[CNSSI_4009]

3.2.17 data integrity

property that data has not been changed, destroyed, or lost in an unauthorized manner

[CCSDS 350.8-M-3]

NOTE The term “integrity” is synonymous.

3.2.18 encryption

cryptographic transformation of data to produce cipher text

[CCSDS 350.8-G-1]

3.2.19 fuzzing

test or automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities

3.2.20 incident

occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

[NIST SP 800-53 Rev. 5]

3.2.21 incident handling

mitigation of violations of security policies and recommended practices

[NIST SP 800-61 Rev. 2]

NOTE The term incident response is synonymous.

3.2.22 information security

measures that implement and assure security services in information systems, including in computer systems (COMPUSEC) and in communication systems (COMSEC)

[IETF RFC 4949]

3.2.23 information security management system

a framework of policies, procedures, guidelines, and associated resources to establish, implement, operate, monitor, review, maintain and improve information security and achieve the objectives of an organisation based on a business risk approach.

NOTE Adapted from ISO/IEC 27000.

3.2.24 information system

set of applications, services, information technology assets, or other information-handling components

[ISO/IEC 27000]

3.2.25 integrity

see "data integrity"

3.2.26 malware

software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an Information System

[CCSDS 350.8-G-1]

3.2.27 penetration testing

test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system

[NIST SP 800-53, NIST SP 800-95]

3.2.28 protective marking

means used to associate a set of security attributes with objects in a human-readable form to enable organizational, process-based enforcement of information security policies, national laws and regulations

NOTE 1 The terms security marking and protective security marking are synonymous.

NOTE 2 Adapted from NIST SP 800-53.

3.2.29 residual risk

risk remaining after risk treatment

[CCSDS 350.8-G-1]

3.2.30 risk treatment

process of selection and implementation of measures to modify risk

[CCSDS 350.8-M-3]

3.2.31 security audit

independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established

security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures

[NIST SP 800-82]

3.2.32 security controls

management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[CCSDS 350.8-M-3]

3.2.33 security incident

see definition of "**incident**"

3.2.34 security maintenance

consolidated release of a software product that can include different features and bug corrections

NOTE In the context of this standard the term "security maintenance" has a different meaning than "security patch".

3.2.35 security monitoring

the process (often automated) of collecting and analysing indicators of potential security threats, then triaging these threats with appropriate action

3.2.36 security patch

"repair job" for a piece of programming; also known as a "fix", often targeted at a specific vulnerability

NOTE 1 A patch is the immediate solution to an identified problem that is provided to users A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.

NOTE 2 Adapted from NIST SP 800-45.

3.2.37 security policy

set of criteria for the provision of security services

[CCSDS 350.8-M-3 (mod.)]

3.2.38 security posture

the security status of an organization's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the organization and to react as the situation changes

[NIST SP 800-137]

3.2.39 security risk

function of the impact of an occurrence of a security incident and the likelihood of that impact's occurrence

NOTE 1 Security risk can be considered qualitatively (e.g., low/medium/high) or quantitatively according to organizational needs:
Security Risk = Likelihood × Impact.

NOTE 2 Adapted from CCSDS 350.7-G-2.

3.2.40 security risk analysis

systematic use of information to identify item or activity having a potential (likelihood) for a consequence (impact) and to estimate the security risk

NOTE 1 Adapted from ENISA and ISO/IEC Guide 73.

NOTE 2 The terms 'potential' and 'likelihood' are interchangeable.

NOTE 3 The terms 'consequence' and 'impact' are interchangeable.

3.2.41 security risk appetite

pre-defined type and level of security risk that, on a broad level, the organisation, program and project are willing to accept in order to meet its objectives

3.2.42 security risk assessment

process of comparing the estimated security risk against given security risk criteria to determine the significance of risk

[ISO/IEC Guide 73]

3.2.43 security risk management

the process, distinct from security risk assessment, of weighing policy alternatives in consultation with interested parties, considering security risk assessment and other legitimate factors, and selecting appropriate prevention and control options

[ENISA Glossary]

NOTE Security risk management is implemented at each level of the customer-supplier network.

3.2.44 security risk owner

person or entity with the accountability and authority to set the security risk appetite, accepting security risk treatment plans and residual security risks for an activity

NOTE 1 The security risk owner is defined by the customer or mission owner and agreed with the project. Security risks are formally accepted by the next higher-level responsibility within the customer/supplier chain.

NOTE 2 The term risk owner is used as the short form of security risk owner.

NOTE 3 Adapted from ISO/IEC 27005:2022.

3.2.45 security sensitivity

measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection

[NIST SP 800-12, NIST SP 800-30]

NOTE Sensitivity is used as the short form of security sensitivity.

3.2.46 source code review

examination of source code to discover hidden vulnerabilities, design flaws, and verify if key security controls are implemented

3.2.47 threat

circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

NOTE 1 Adapted from NIST SP 800-30, NIST SP 800-53, and NIST SP 800-128.

NOTE 2 A summary of security threats for space missions can be found in Annex B.

NOTE 3 An alternative definition is: potential cause of an unwanted incident, which can result in harm to a system or organization [adapted from ISO/IEC 27000:2018].

3.2.48 threat source

the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability

[CCSDS 350.8-G-1]

3.2.49 vulnerability

flaw or weakness in a system's design, implementation, or operation and management that could be exploited by a threat source to violate the system's security policy

NOTE Adapted from IETF RFC 4949

3.2.50 vulnerability assessment

systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation

[CCSDS 350.8-M-3]

3.3 Abbreviated terms

For the purpose of this Standard, the abbreviated terms and symbols from ECSS-S-ST-00-01 and the following apply:

Abbreviation	Meaning
AR	Acceptance Review
CDR	Critical Design Review
COTS	Commercial Off the Shelf
DRD	Documents Requirements Definition
FOSS	Free and Open Source Software
FPGA	Field Programmable Gate Arrays
INFOSEC	Information Security
ISMS	Information Security Management System
KOM	Kick-Off Meeting
MGT	Management file
NTK	Need-to-Know
ORR	Operational Readiness Review
OSS	Open Source Software
PDR	Preliminary Design Review
QR	Qualification Review
SF	Security File
SOC	Security Operations Centre
SRR	System Requirements Review
TS	Technical Specification

3.4 Nomenclature

The following nomenclature applies throughout this document:

a. The word “shall” is used in this Standard to express requirements. All the requirements are expressed with the word “shall”.

b. The word “should” is used in this Standard to express recommendations. All the recommendations are expressed with the word “should”.

NOTE It is expected that, during tailoring, recommendations in this document are either converted into requirements or tailored out.

c. The words “may” and “need not” are used in this Standard to express positive and negative permissions, respectively. All the positive permissions are expressed with the word “may”. All the negative permissions are expressed with the words “need not”.

d. The word "can" is used in this Standard to express capabilities or possibilities, and therefore, if not accompanied by one of the previous words, it implies descriptive text.

NOTE In ECSS "may" and "can" have completely different meanings: "may" is normative (permission), and "can" is descriptive.

e. The present and past tenses are used in this Standard to express statements of fact, and therefore they imply descriptive text.

4
Security in Space Systems Lifecycles Principles

4.1 Security Design and Operations Principles

4.1.1 Overview

Design and operations principles are presented together because most of them affect both the design of the system and how its maintenance and operations can be organised.

During design and operation of any system, the following principles (listed in alphabetical order) apply.

4.1.2 Attack Surface Reduction

This principle refers to the reduction of the total reachable and (potentially) exploitable services, applications, assets, resources, etc. to the bare minimum required for the function of the system, subsystem, or component. Attack surface reduction refers to all the measures that can be taken so as to achieve the final objective, from applying appropriate boundary controls (e.g. network and host firewalls by minimising access to the bare minimum ports), to completely removing services, applications, any kind of software and functionalities that are not strictly needed for fulfilling the mission requirements.

This principle is also known as the principle of minimalism.

4.1.3 Conflicts with Design Principles

The application of one principle can partially conflict with another. In such cases, conflicts are covered and reviewed during the whole lifecycle of the system, and one can be emphasised more than the other, depending on the objectives of the system.

4.1.4 Defence-in-Depth

Defence-in-depth is an information security strategy integrating people, technology, and operations capabilities to establish multiple countermeasures in a layered or stepwise manner to achieve the security objectives. The

application of this principle involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another.

[Source: NISTIR 8183 (mod.)].

These layers can include:

- Prevention: security measures aimed at impeding or blocking an attack on the system.
- Detection: security measures aimed at discovering the occurrence of an attack on the system.
- Resilience: security measures aimed at limiting impact of an attack to a minimum set of information or assets and preventing further damage, and
- Recovery: security measures aimed at regaining a secure situation for the System if it is compromised.

This principle focuses on maximising the complexity of an attack for the adversary and encourages the use of redundancy in defences, where security is not dependent on only one security feature working.

4.1.5 Domain Separation

Domains with distinctly different protection needs are physically or logically separated.

Note: The separation of domains enables enhanced control and, therefore, protection of system function and the flow of data. Control relative to separated domains limits the extent to which an entity or domain is influenced by or is able to influence some other entity or domain, thereby enhancing the protection of a domain. This is achieved through the control of information flow and data between domains as well as control over the use of a system capability between domains.

[Source: NIST SP 800-160v1r1, Appendix E.12 (mod.)].

4.1.6 Fail Secure

Fail secure is a principle that refers to a mode of termination of system functions that prevents loss of secure state when a failure occurs or is detected in the system (but the failure still might cause damage to some system resource or system entity).

[Source: IETF RFC 4949].

NOTE Fail Secure is not the same with Fail Safe, which is a design feature or practice that, in the event of a specific type of failure, inherently responds in a way that can cause only minimal or no harm to other equipment, to the environment or to people.

4.1.7 Least Privilege

Least privilege is the principle that a security architecture is designed so that each entity is granted the minimum system resources and authorisations that the entity needs to perform its function.

[Source: NIST 800-53 Rev.5].

4.1.8 Need-to-Know

Need-to-Know (NTK) is the principle according to which a positive determination is made by the issuer of the information that a prospective recipient has a requirement for access to, knowledge of, or possession on information in order to perform tasks or services in the scope of the contract programme, project or activity.

4.1.9 Secure Evolvability / Agility

The principle of secure evolvability states that a system should be developed to facilitate the maintenance of its security properties when there are changes to its functionality structure, interfaces, and interconnections (i.e., system architecture) or its functionality configuration (i.e., security policy enforcement).

[Source: NIST SP 800-160v1, appendix F.1.8].

4.1.10 Separation of Duties

Separation of duties refers to the principle that no user should be given enough privileges to misuse the system on their own. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule.

[Source: NIST SP 800-192 (mod.)].

An example of application of this principle is to require two different physical persons to authorise an operation so as this to take place. Another example is to allocate critical but interdependent roles to different persons, e.g., a domain controller administrator to be a different person from a database administrator, or a crypto custodian to be a different person than a crypto operator.

4.1.11 Redundancy

The system design delivers the required capability by replication of system functions or elements.

Note: Redundancy employs multiples of the same system elements, data and control flows, or paths to avoid single points of failure. Redundancy requires a strategy for how multiple system elements are used individually or in combination (e.g., load-balancing, fail-over, concurrently, backup, etc.).

[Source: NIST SP 800-160v1r1, Appendix E.26 (mod.)].

4.2 Organisation of this Standard

This standard is organised in four main parts:

- Organisation (i.e. personnel, Security Management Plan, organisational structure of involved entities);
- Mission Security;
- System Security Engineering;
- Security Assessment during Space Systems Lifecycle.

The documentation collecting the expected output of the requirements of the current document is summarised in Annex A.

Each requirement of this Standard is identified by a hierarchical number, plus a letter if necessary (e.g. 5.3.1.5, bullet a). For each requirement, the associated output is given in the "Expected Output" section. With each output, the destination file of the output is indicated in brackets, together with the corresponding document DRD (after a comma) and review(s) (after a semicolon). When no DRD is defined for an Expected Output, and/or the Expected Output is not to be provided at any specific milestone review, then the corresponding sections of that Expected Output are replaced by dashes.

4.3 Tailoring of this Standard

The general information and requirements for the selection and tailoring of applicable standards are defined in ECSS-S-ST-00.

5
Requirements

5.1 Organisation

5.1.1 Organisational Structure

ECSS-E-ST-80_0600001

a. The supplier shall establish an organisational structure of personnel required to ensure security in space systems, projects and missions during their whole lifecycle.

ECSS-E-ST-80_0600002

b. In this organisational structure the responsibilities, the authority, the tasks and the interrelation of personnel who manage, perform and verify work affecting security in space systems lifecycle shall be defined.

ECSS-E-ST-80_0600003

c. This organisational structure shall include at a minimum a Security Manager and a Security Internal Auditor.

ECSS-E-ST-80_0600004

d. The Security Manager and the Security Internal Auditor shall perform their duties without prejudice due to their functional hierarchy in their entity.

ECSS-E-ST-80_0600005

e. The interfaces with any external or internal entity involved in a project or a mission and their responsibilities in respect to the project or mission shall be defined and documented.

ECSS-E-ST-80_0600006

f. The organisational structure shall be incorporated into the Security Management Plan.

EXPECTED OUTPUT: Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]

5.1.2 Security Management Plan

ECSS-E-ST-80_0600007

a. Each entity participating by any means to any space project, programme, or mission, shall develop, document, and implement an organization-wide plan to provide security for the information, information and communication systems and facilities that support the operations and assets of that organization.

EXPECTED OUTPUT: Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]

NOTE Example of facilities include factories, test centres, and other.

ECSS-E-ST-80_0600008

b. A Security Management Plan shall be part of entity's Information Security Management System (ISMS).

ECSS-E-ST-80_0600009

c. The process of uniquely assigning information resources to an information system shall define the security boundary for that system.

ECSS-E-ST-80_0600010

d. The security boundary shall take into account regulatory authority, trust relationships, and line management authority.

NOTE Source: CCSDS 350.7-G-2, para. 3.6.2 (mod).

ECSS-E-ST-80_0600011

e. A Security Management Plan shall describe resources under the same management control.

ECSS-E-ST-80_0600012

f. The Security Management Plan shall define the organizations protective marking and handling rules.

ECSS-E-ST-80_0600013

g. Processes as well as project/mission data and information shall be handled and protectively marked in compliance with the international or national applicable Security Controls Frameworks standards.

NOTE This includes project/mission data and information shared with subcontractors.

ECSS-E-ST-80_0600014

h. Access to assets and information shall be given, based on the "Need-To-Know (NTK)" principle and its related sensitivity.

EXPECTED OUTPUT: Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]

5.1.3 Personnel

5.1.3.1 Security Manager

ECSS-E-ST-80_0600015

a. The organisation or entity shall appoint a Security Manager responsible for managing the implementation of security requirements in the scope of the activities under the responsibility of this organisation or entity.

NOTE Security requirements can be system security engineering requirements (security requirements imposed to apply a security by design approach), mission security requirements (security requirements applicable at mission level) or Information Security Management System (ISMS) related requirements. Each appointed Security Manager is responsible for the security requirements which fall in the scope of responsibilities.

ECSS-E-ST-80_0600016

b. The Security Manager shall be trained for the role.

ECSS-E-ST-80_0600017

c. The Security Manager shall be responsible for conducting at least the following tasks:

1. Establishment of implementation plans for security policies and security requirements.
2. Support to the implementation of the necessary security measures and of the security risk mitigations.
3. Supervision and monitoring of the performance of all security related planned tasks.
4. Reporting of the status of all security related tasks, as well as of the security posture of the system that falls under the responsibility of her/his entity.
5. Promotion of Information Security (INFOSEC) within her/his entity.

NOTE to item 3: Examples of such tasks are vulnerability assessments, security risk assessments, application of needed asset sensitivity, protective marking, security controls, and other.

ECSS-E-ST-80_0600018

d. The responsibilities of the Security Manager shall be defined in the Security Management Plan.

EXPECTED OUTPUT: Security Management Plan [MGT; KOM, SRR, and updated when needed]

5.1.3.2 Security Internal Auditor

ECSS-E-ST-80_0600019

a. The organisation or entity shall appoint a Security Internal Auditor responsible for conducting security audits in the perimeter of this organisation or entity.

ECSS-E-ST-80_0600020

b. The Security Internal Auditor shall be trained for the role.

ECSS-E-ST-80_0600021

c. The Security Internal Auditor shall carry out the security auditing activities impartially and independently from the execution of the Security Manager.

ECSS-E-ST-80_0600022

d. The Security Auditor shall be independent from the team implementing or controlling the security measures.

ECSS-E-ST-80_0600023

e. The Security Internal Auditor shall have direct reporting line to the high-level management of the project or mission.

ECSS-E-ST-80_0600024

f. The Security Internal Auditor shall not be part of the internal organisation that manages the execution of the project (operations or development) or mission.

ECSS-E-ST-80_0600025

g. The Security Internal Auditor shall be responsible for conducting at least the following tasks:

1. Planning and implementation of security audits in the perimeter of her/his area of responsibility.
2. Evaluation of the level of compliance of the Information Security Management System (ISMS) of her/his entity, of the implementation of the security requirements, and of the security measures that have been put in place.
3. Providing independent feedback and report on a regular basis (at least every six months) on the effectiveness of Security Management Plan, security measures, and their application.

ECSS-E-ST-80_0600026

h. The Security Internal Auditor shall always be granted access to the information required to perform her/his duties.

ECSS-E-ST-80_0600027

i. The responsibilities of the Security Internal Auditor shall be defined in the Security Management Plan.

EXPECTED OUTPUT: Security Management Plan [MGT; KOM, SRR, and updated when needed]

5.1.4 Personnel Authorisation and Training

ECSS-E-ST-80_0600028

a. All personnel shall be appropriately authorised, security trained & briefed based on their responsibilities, role and function.

ECSS-E-ST-80_0600029

b. Personnel authorisation and training shall be periodically refreshed also depending on role, and function and changes in threat and security risk.

ECSS-E-ST-80_0600030

c. Security awareness briefings shall be periodically organised for all personnel.

ECSS-E-ST-80_0600031

d. The personnel authorisation requirements and their training plan shall be included in the Security Management Plan.

EXPECTED OUTPUT: Security Management Plan [MGT; KOM, SRR, and updated when needed]

5.1.5 Accounting and Authorisation

ECSS-E-ST-80_0600032

a. Any equipment and resource shall be accounted and authorised prior to use within a space project or mission.

NOTE Equipment includes hardware all types of software, and their configuration.

ECSS-E-ST-80_0600033

b. The person(s) (in terms of functional roles) responsible for providing the authorisation shall be defined in the Security Management Plan.

ECSS-E-ST-80_0600034

c. Processes and tools shall be in place to detect and address unauthorized equipment, personnel use or access.

ECSS-E-ST-80_0600035

d. The processes and tools to be used to address accounting and authorisation requirements shall be defined at the beginning of the project or mission and checked throughout the complete lifecycle.

ECSS-E-ST-80_0600036

e. Access to assets and information shall be given, based on the “Need-To-Know (NTK)” principle and the sensitivity of the asset.

ECSS-E-ST-80_0600037

f. The processes and tools to be used for accounting and authorisation shall be included in the Security Management Plan.

EXPECTED OUTPUT: Security Management Plan [MGT; KOM, SRR, and updated when needed]

5.2 Mission Security

5.2.1 Mission Security Policy

ECSS-E-ST-80_0600038

a. Every mission shall define a Mission Security Policy as an element of its overall mission concept definition.

ECSS-E-ST-80_0600039

b. The Mission Security Policy shall outline how the space system is intended to operate, and what action are taken when it operates outside its intended parameters.

ECSS-E-ST-80_0600040

c. The Mission Security Policy shall be observant of any higher-level organization.

ECSS-E-ST-80_0600041

d. The Mission Security Policy shall clearly state:

1. The sensitivity and therefore the required level of protection of all the information associated with the mission, both live and archived, during the whole lifecycle of the mission;
2. the protective marking to be applied to mission information and assets;
3. how mission information and assets will be protected when generated and received, including when it is exchanged;
4. the roles of those who have access to the system(s) operating the mission;
5. the confidentiality requirements of the mission;
6. the integrity requirements of the mission; and
7. the availability requirements of the mission.

NOTE 1 Source: CCSDS 350.7-G-2, para. 3.2 (mod.).

NOTE 2 Information associated with the mission includes, but is not limited to, telemetry, telecommand structure and their contents, software, and ground systems data, and personal data.

NOTE 3 a common mission protective marking for the mission needs to be defined. However, it may not be possible that all information and assets have the marking applied by all parties supporting the mission, especially if they use pre-existing organizational developed materials. In such cases, a mission level equivalence matrix shall be defined and approved.

ECSS-E-ST-80_0600042

e. Where a complex system includes interacting elements under different management control, those elements shall be described separately.

NOTE Elements under different management control can be spacecrafts, ground segment, or other.

ECSS-E-ST-80_0600043

f. Interactions between elements under different management control shall be documented.

ECSS-E-ST-80_0600044

g. Any shared resources shall be approved by the relevant authorities for the highest sensitivity level of the resources and information managed.

EXPECTED OUTPUT: Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

NOTE 1 Source: CCSDS 350.7-G-2, para. 3.6.2 (mod).

NOTE 2 Shared resources can be organizational processes, networks, physical facilities, and other.

5.2.2 Mission Security Requirements

ECSS-E-ST-80_0600045

a. All communication links, space (telemetry, telecommand, mission specific) and terrestrial (ground segment and other) shall, at a minimum, be protected with cryptographic authentication and integrity mechanisms sufficient for the sensitivity of the information and asset and accompanied by the required documented procedures.

NOTE The outcome of a security risk analysis can be used to support non-cryptographic alternative controls on the telemetry link where a mission risk owner has a high security risk appetite and low levels of residual risk.

ECSS-E-ST-80_0600046

b. A mission level security risk analysis shall be used to assess the need of encryption of the various communication links.

EXPECTED OUTPUT: Mission Security Policy; [TS; KOM, SRR, PDR, CDR; updated when needed]; Security Risk Analysis [SF; SRR, PDR, CDR, QR, AR, ORR]

NOTE See 5.4.1 for more information on security risk management process.

ECSS-E-ST-80_0600047

c. A mission level security risk analysis shall be used to assess the need of putting in place measures to support detection of physical layer interference.

ECSS-E-ST-80_0600048

d. A mission level security risk analysis shall assess the need and feasibility of encryption, authentication, integrity protection and detection controls regarding systems and information in transport, at rest and in-use with assessment of physically separated entities, dataflows and third-party access.

ECSS-E-ST-80_0600049

e. The operator shall ensure that technical and organizational measures that prevent unauthorized persons access to the installations and operating rooms for the commanding of the spacecraft as well as to the equipment and services for receiving, processing and storing the data appropriate to the sensitivity of the asset and information.

ECSS-E-ST-80_0600050

f. Measures shall be put in place to address retirement and disposal of hardware and software.

ECSS-E-ST-80_0600051

g. The operator shall ensure adequate security screening and (where appropriate) clearance of persons who have access to the facilities for commanding a spacecraft or to the facilities for receiving, processing and storing the data of a spacecraft, or access to any other relevant information or physical assets based on the assets' security sensitivity.

ECSS-E-ST-80_0600052

h. The measures and procedures ensuring the implementation of these requirements shall be part of the Mission Security Policy.

ECSS-E-ST-80_0600053

i. Mission security requirements shall be captured in the Mission Security Policy and be flown down to System and sub-system like any other functional and non-functional requirement.

EXPECTED OUTPUT: Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

5.2.3 Security Monitoring and Incident Handling

ECSS-E-ST-80_0600054

a. Each mission and each of its systems shall be continuously monitored in terms of security for intrusion detection purposes from a Security Operations Centre (SOC).

ECSS-E-ST-80_0600055

b. Security monitoring capability shall cover the whole perimeter of a mission or a system.

ECSS-E-ST-80_0600056

c. Security monitoring shall be able to detect all possible types of attacks with support of cyber threat intelligence, with a special focus with the

ones related with security risks identified during the security risk assessment.

ECSS-E-ST-80_0600057

d. It shall be assessed the need to define different security monitoring and incident handling resources, plans and procedures during the Phases A .. C from those during the Phases D .. E ((pre) operations and disposal activities).

ECSS-E-ST-80_0600058

e. Incident handling capability shall be incorporated into the security monitoring capability of the mission.

ECSS-E-ST-80_0600059

f. Incident handling processes, procedures and response performances shall be agreed by the mission owner.

ECSS-E-ST-80_0600060

g. Incident handling capability shall include a Security Incident Response Team, capable of being developed rapidly to handle a cyber incident.

ECSS-E-ST-80_0600061

h. Measures and plans shall be put in place to respond and recover in case of major incidents.

ECSS-E-ST-80_0600062

i. The measures and plans to be put in place to respond and recover in case of major incidents shall be verified periodically.

ECSS-E-ST-80_0600063

j. Security monitoring and incident handling capability may be outsourced.

EXPECTED OUTPUT: Security Monitoring and Incident Handling Plan [SF; SRR, PDR, CDR, QR, and updated when needed]

5.3 System Security Engineering

5.3.1 Introduction

Clause 5.3 provides high level requirements for system security engineering. System security engineering requirements define the requirements needed to engineer a system (flown down to subsystem, component, etc. as needed) following a security by-design approach. It is good practice that security engineering is not tackled in isolation, but rather as part of the whole engineering process and therefore, it can influence, and it can be influenced by the system engineering process, programmatic, technical documentation, and data packages.

5.3.2 System Security Engineering Requirements

ECSS-E-ST-80_0600064

a. System security engineering shall be incorporated from the very beginning of a project or mission as part of the whole system engineering for any kind of project or mission.

ECSS-E-ST-80_0600065

b. System security engineering requirements shall be derived from mission security policy and security risk treatment plan, as well as from functional system requirements with implications to security.

ECSS-E-ST-80_0600066

c. The system security engineering requirements shall be incrementally extended and derived based on the mission phase and level of the project customer-supplier.

ECSS-E-ST-80_0600067

d. In order to select appropriate security controls, organizations shall categorize the information to be handled by the system according to the criteria of Confidentiality, Availability, and Integrity.

EXPECTED OUTPUT: System Security Engineering Plan [TS; SRR, PDR, CDR, QR]

NOTE National security regulations as well as other laws (e.g., export, personal sensitive data and copyright restrictions) controlling the handling of specific information types override organizational discretion in categorizing information.

ECSS-E-ST-80_0600068

e. Security controls from the following categories shall be put in place:

1. Controls and measures designed to prevent a negative security event from occurring (preventive controls);
2. Controls and measures that aim to inform the organization about potential security events (detective controls);
3. Controls and measures in response to a potential security incidence to minimise impact, restore the system to nominal operation and/or collect forensic information about the nature and extent of the event (responsive controls).

ECSS-E-ST-80_0600069

f. The applicability and usefulness of the security controls originally implemented shall be periodically re-evaluated and adapted:

1. as threats and security risks to the system change over time;
2. when system components are replaced, upgraded or their sensitivity levels are changed;
3. as specific vulnerabilities are identified;
4. when the security risk appetite is modified;
5. periodically, even if there is no change, to confirm their applicability and effectiveness.

EXPECTED OUTPUT: Security Monitoring and Incident Handling Plan [SF; SRR, PDR, CDR, QR]

ECSS-E-ST-80_0600070

g. Together with the system architecture, a system security architecture shall be compiled, incorporating the security controls to be put in place.

ECSS-E-ST-80_0600071

h. The system security architecture shall be compiled adhering to the principles defined in Clause 4.1.

ECSS-E-ST-80_0600072

i. The system security architecture shall be driven by a mission/system security risk analysis including asset and information sensitivity.

ECSS-E-ST-80_0600073

j. The system security architecture shall incorporate the technical capabilities required to apply business continuity and disaster recovery plan including cyber disasters such as malware pandemic.

ECSS-E-ST-80_0600074

k. The system design shall address or mitigate the security risks identified in the security risk analysis performed at the beginning of the project or mission by proposing for implementation the required security controls and taking into account the available security risk treatment plans.

EXPECTED OUTPUT: System Security Architecture [TS; PDR, CDR, QR]

ECSS-E-ST-80_0600075

l. For each system, a security obsolescence plan shall be defined specifying the requirements for support by the vendors of each component for security maintenance and patches, fixes and security certifications (if applicable).

EXPECTED OUTPUT: Security Obsolescence Plan [SF; PDR, CDR, QR]

ECSS-E-ST-80_0600076

m. The security obsolescence plan shall be agreed with the security risk owner and maintained during the system lifetime.

ECSS-E-ST-80_0600077

n. For each system a security maintenance and patching policy for all types of software and hardware (including FPGAs) shall be defined and be applicable during the whole lifecycle of the mission.

ECSS-E-ST-80_0600078

o. Each system shall be designed and developed in a way to be capable of applying the defined security maintenance and patching policy.

ECSS-E-ST-80_0600079

p. The security maintenance and patching policy shall include as a minimum:

1. the security patches to be applied;
2. how frequently to apply security patches and security maintenance updates.

NOTE To decide which security patches to be prioritised for application, several criteria can be used, like the severity of a vulnerability, its impact on a mission, etc.

ECSS-E-ST-80_0600080

q. All security patches and in general all updates to be applied shall be tested and verified in terms of their authenticity.

ECSS-E-ST-80_0600081

r. For secure software development, ECSS-Q-ST-80 and ECSS-E-ST-40 shall be followed.

ECSS-E-ST-80_0600082

s. The supplier shall define and apply guidelines for secure configuration of all the services, sub-systems and components in a system.

ECSS-E-ST-80_0600083

t. System security engineering requirements shall be included in the system security engineering plan.

EXPECTED OUTPUT: System Security Engineering Plan [TS; SRR, PDR, CDR, QR]

5.3.3 Supply Chain requirements

ECSS-E-ST-80_0600084

a. The supplier shall define and implement processes and technical measures to ensure and verify at any phase of the project the authenticity of a service, component or a subsystem across the whole supply chain.

NOTE 1 Supply chain also includes services provided by third parties such as contractors and sub-contractors.

NOTE 2 In Figure 5-1 an example of a supply chain and of corresponding potential security issues is given.

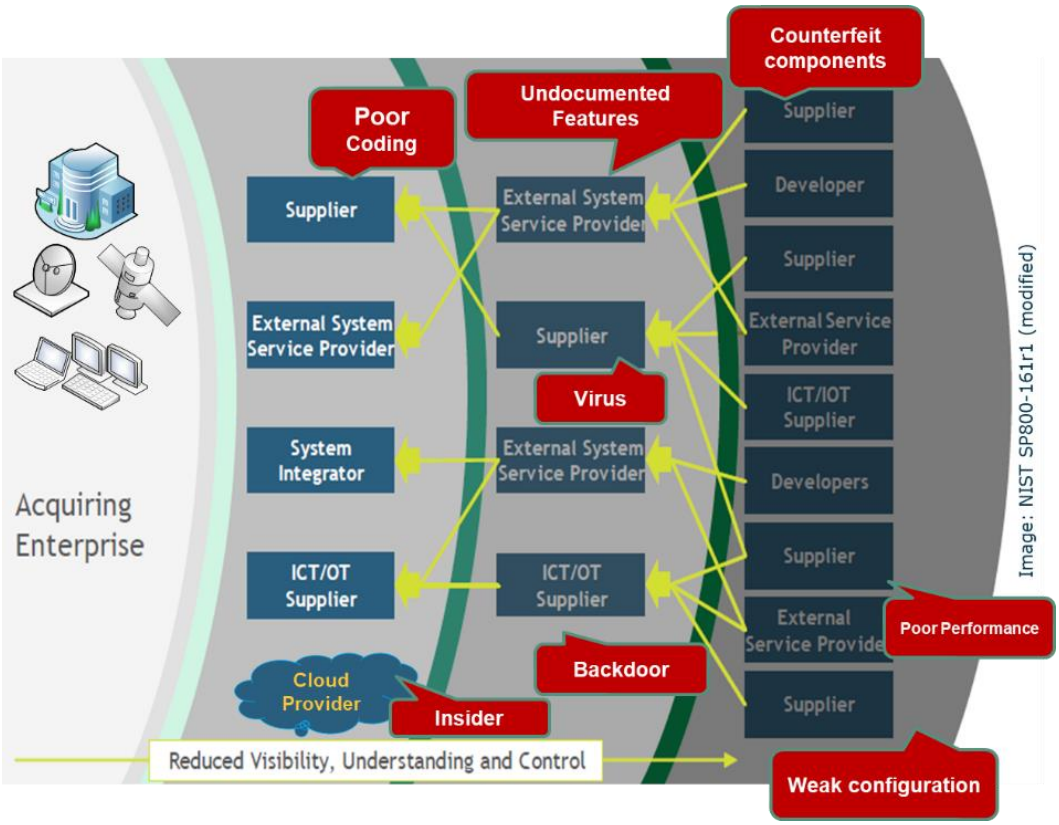


Figure 5-1: Indicative Supply chain challenges

ECSS-E-ST-80_0600085

b. Supplier shall implement product assurance requirements considering ECSS-Q-ST-10.

ECSS-E-ST-80_0600086

c. The system security engineering requirements which have been derived in the frame of the project shall be flown-down to the relevant suppliers of security sensitive products and considering also ECSS-Q-ST-80 and ECSS-E-ST-40 if the supplies contain software modules.

ECSS-E-ST-80_0600087

d. The supplier shall assess potential vendors, taking into account the criticality and sensitivity of the product or service to determine if they:

1. Provide products and components, or sub-components, sourced through original equipment manufacturers or authorized resellers with clear and traceable bill of materials with appropriate integrity and authenticity measures.
2. Have previously incurred significant malicious network intrusions, data breaches, loss of client data, or intellectual property.
3. Have an adequately mature cyber security organisation, appropriate certifications and qualifications.
4. Provide services and products compliant to national regulations.

NOTE 1 to item 3: Example for an organization include ISO/IEC 27001 ISMS certification and for a product Common Criteria Product evaluation. This standard does not mandate a specific one, since the exact certificate requirements can also be mission/project specific.

NOTE 2 to item 4: Examples include Export Control, Personal Information and the location of the organisation/service.

ECSS-E-ST-80_0600088

e. The customer shall define the supplier privacy and system security engineering requirements based on the criticality and sensitivity of the asset, resource or services to be provided by the supplier.

ECSS-E-ST-80_0600089

f. The supplier shall provide a statement of compliance against the requirement set identified in accordance with 5.3.3b and 5.3.3c with supporting credible evidence.

ECSS-E-ST-80_0600090

g. Supply chain management and requirements shall be defined and implemented at each level of the customer-supplier network.

ECSS-E-ST-80_0600091

h. Supply chain management and requirements shall be defined in Supply Chain Management Plan.

EXPECTED OUTPUT: Supply Chain Management Plan [MGT; Proposal/KOM, SRR, PDR, CDR, QR, AR]

5.3.4 System Security Engineering Plan

ECSS-E-ST-80_0600092

a. Each supplier shall develop a System Security Engineering Plan that references or provides:

1. A summary of the system security engineering requirements;
2. The system security controls in place and how it is planned for meeting the system security engineering requirements;

3. A complete list of the inventory up to component level including each COTS and OSS with a detail versioning;
4. A cyber disaster recovery plan; and
5. A plan for source code analysis, security audits, vulnerability assessments and penetration tests to ensure that products are delivered to meet specified system security engineering requirements.

NOTE A Business Continuity Plan can also contribute to manage a cyber disaster.

ECSS-E-ST-80_0600093

b. The scope of the system security engineering plan shall include all its subsystems or subordinate systems.

ECSS-E-ST-80_0600094

c. The system security engineering plan shall include in its scope everything that falls in the responsibility of the specific mission, project, or contract.

ECSS-E-ST-80_0600095

d. Organizational policy shall clearly define who is responsible for approving the system security engineering plan.

NOTE Source: CCSDS 350.7-G-2, para. 3.6.4 (mod).

ECSS-E-ST-80_0600096

e. The system security engineering plan shall be subject to review during the major project review milestones.

EXPECTED OUTPUT: System Security Engineering Plan [TS; SRR, PDR, CDR, QR]

NOTE Source: CCSDS 350.7-G-2, para. 3.6.4 (mod).

5.4 Security Assessment During Space Systems Lifecycle

5.4.1 Security Risk Management

ECSS-E-ST-80_0600097

a. A security risk owner shall be defined by the customer or the mission owner who is the responsible party to accept and agree on security risks and treatments.

EXPECTED OUTPUT: Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

ECSS-E-ST-80_0600098

b. The pre-defined acceptable security risk level shall be agreed by the security risk owner.

EXPECTED OUTPUT: Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

NOTE The pre-defined acceptable security risk is called "risk appetite".

ECSS-E-ST-80_0600099

c. At the beginning of each project or mission a security risk management process shall be defined and agreed with the risk owner and the customer.

EXPECTED OUTPUT: Organization process - Security Management Plan [MGT; KOM, SRR]
Mission process – Mission Security Policy [TS; KOM, SRR, PDR]

NOTE An indicative Security risk management process is given in Figure 5-2 and an example of its application along a project's lifecycle in Figure 5-3.

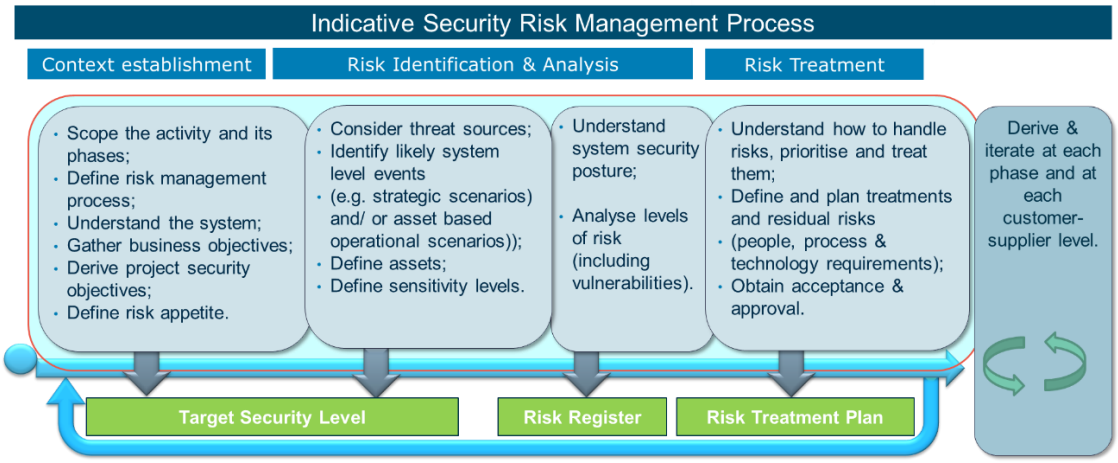
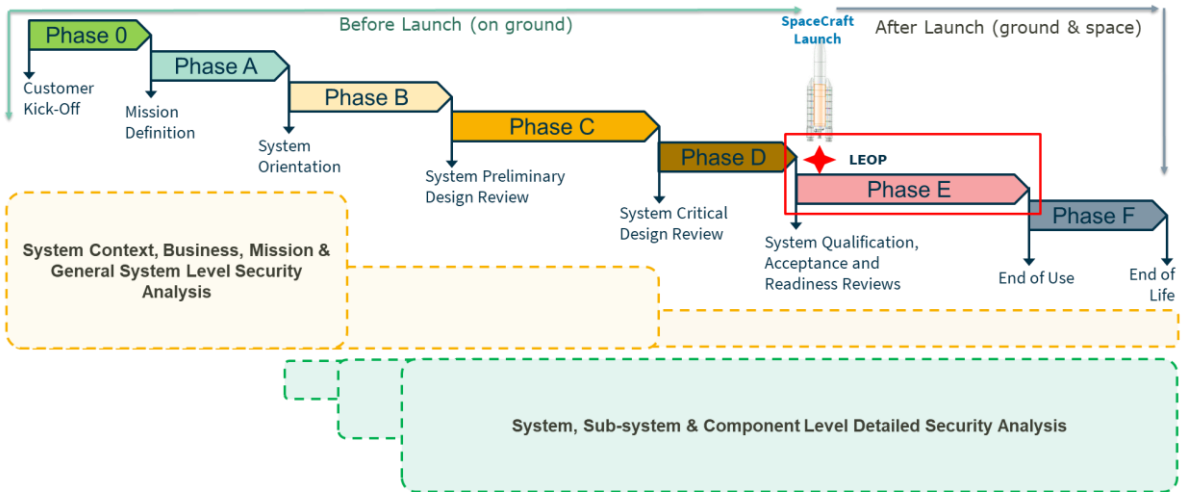


Figure 5-2: Indicative Security Risk Management Process



* In this example, the higher-level context and low-level assessments are shown as parallel activities present in later phases to support different stakeholder and reporting needs, but this is not always necessary.

Figure 5-3: Example of an Incremental Security Analysis to be Iteratively Derived at each Project Lifecycle Phase

ECSS-E-ST-80_0600100

d. At the beginning of each project or mission a preliminary security risk assessment shall be performed.

ECSS-E-ST-80_0600101

e. The preliminary security risk assessment shall consider at least the following:

1. The type of the mission and the information security threats to that mission.
2. All parts of the mission and system architecture during all phases of the mission/project, as the relevant threats can change during their lifecycle.

ECSS-E-ST-80_0600102

f. The preliminary security risk assessment shall use the outputs of the Mission Security Policy and system interconnections as identified in the system architecture and mission requirements to help identify attack vectors, sensitivity, and the value of the information and assets to be protected.

ECSS-E-ST-80_0600103

g. The security risk assessment shall be performed at each level in the customer-supplier network.

ECSS-E-ST-80_0600104

h. The security risk assessment shall be refined and updated at least at each major milestone and when there is a major design change, or new vulnerabilities are identified.

NOTE New vulnerabilities can be identified during development, operations, and in general during the mission or system lifecycle via penetration tests, security risks assessments, security audits, etc.

ECSS-E-ST-80_0600105

i. The security risk assessment shall incorporate all known vulnerabilities existing along all stages of the components (hardware, software) supply chain and/or development.

NOTE 1 source: CCSDS 350.7-G-2, para. 3.6.3 (mod).

NOTE 2 In the early stages of development, vulnerabilities can be theoretical in nature; in later stages, they can be highly dependent upon implementation details.

NOTE 3 Vulnerability along the component supply chain can enable gateways for future threats or they can cause "residuals" that can develop under certain circumstances into threats.

ECSS-E-ST-80_0600106

j. Security risk assessment of a mission shall include as a minimum the following:

1. Launch site and facilities;
2. Manufacturing, Assembly, Integration and Test facilities;
3. Ground Segment;
4. Space Segment;
5. User Segment.

ECSS-E-ST-80_0600107

k. Security risk assessment of a system/subsystem shall cover all its perimeter, including its interfaces with external systems/subsystems in line with the security scope agreed with the security risk owner.

ECSS-E-ST-80_0600108

l. For each security risk found, the security risk assessment shall also identify and propose a mitigation strategy, including a security risk treatment plan (to be prioritized and scheduled).

ECSS-E-ST-80_0600109

m. Where identified security risk mitigation strategies conflict with other types of risk, most notably safety, environmental risk and dependability they shall be agreed with the risk owner(s).

ECSS-E-ST-80_0600110

n. The proposed security risk treatment plan shall include the risk treatments and measures to address, at least, the identified security risks above the security risk appetite.

EXPECTED OUTPUT: Security risk analysis SRR, PDR, CDR, QR, AR, ORR]; Security risk treatment plan [SF; PDR, CDR, QR, AR, ORR]

ECSS-E-ST-80_0600111

o. The security risk treatment plan shall define the security risk treatment(s) and plan for implementation that includes as a minimum:

1. The security risks with their associated criticality;
2. Proposed treatments for the security risk with rationale for selection;
3. Plan for implementation of the treatments;
4. Residual security risk assessment after treatment, defined in line with the implementation plan.

NOTE Security Risk Treatments include: Accept/Retain, Avoid, Transfer, Share, Mitigate/Modify.

ECSS-E-ST-80_0600112

p. Where a residual security risk is present that is above the security risk appetite for a release of the product/system, the security risk shall be supported by a security waiver that presents a risk balance case justifying why the residual risk and risk treatment plan can be acceptable to the risk owner.

NOTE Project constraints such as cost, schedule, safety, operability can be valid justification for the risk owner, often as temporary treatments.

ECSS-E-ST-80_0600113

q. The security risk treatment plan and security waivers shall be presented and approved by the risk owner.

ECSS-E-ST-80_0600114

r. The communication and ranking of security risks and treatments for incorporation into the overall project security risk management process shall be agreed by the risk owner.

NOTE The principles and requirements for integrated risk management on a space project are defined in ECSS-M-ST-80.

ECSS-E-ST-80_0600115

s. At each major milestone, the acceptance of the associated security risks, security waivers and related security risk treatment plans shall be considered to decide whether to authorise the completion for that phase.

NOTE Temporary authorisation can be permitted based on the completion of security risk treatment plans as authorised by the risk owner.

ECSS-E-ST-80_0600116

t. The applicable security handling and processing constraints shall be respected during the whole security risk management process (including the communication and processing of security risk assessments, security risk treatment plans and security waivers).

EXPECTED OUTPUT: Security Management Plan [MGT; Proposal, KOM, SRR, and updated when needed]; Mission Security Policy [TS; KOM, SRR, PDR, CDR; updated when needed]

ECSS-E-ST-80_0600117

u. The security analysis, associated security risks and security risk treatment plans shall be monitored, reviewed, updated systematically and periodically throughout the entire system lifecycle ensuring their continued consistency with each other and their validity.

EXPECTED OUTPUT: Security risk analysis [SF; SRR, PDR, CDR, QR, AR, ORR]; Security risk treatment plan (updated) [SF; PDR, CDR, QR, AR, ORR]

ECSS-E-ST-80_0600118

v. The security risk analysis shall include supply chain risks.

5.4.2 Software Vulnerability Analysis

ECSS-E-ST-80_0600119

a. During software development, the software verification process defined in ECSS-E-ST-40 shall be followed.

ECSS-E-ST-80_0600120

b. At the end of each software development, a source code review and analysis shall be performed to ensure the product is in conformance to security coding policies and is free from known vulnerabilities and malicious code.

NOTE Source code review and analysis can include static, dynamic code analysis, runtime analysis, fuzzing, etc.

ECSS-E-ST-80_0600121

c. The vulnerabilities identified during the source code review shall be fixed before qualification.

ECSS-E-ST-80_0600122

d. An additional source code review shall be performed to confirm the fixes.

ECSS-E-ST-80_0600123

e. For vulnerabilities which are not fixed, a justification shall be provided, and the waiver process be followed.

ECSS-E-ST-80_0600124

f. The security risk analysis shall be updated based on the not fixed vulnerabilities and the security risk management process be followed.

EXPECTED OUTPUT: Vulnerability analysis report [SF; PDR, CDR, QR, AR, ORR].

5.4.3 Security Audits

ECSS-E-ST-80_0600125

a. The Security Internal Auditor shall perform internal security audits at intervals defined at the system security engineering plan.

ECSS-E-ST-80_0600126

b. The security audits shall cover the complete lifecycle of a mission, system or product development, including processes, personnel and site security.

ECSS-E-ST-80_0600127

c. The customer shall have the capability to request additional security audits on the organization and mission during the system lifecycle.

ECSS-E-ST-80_0600128

d. The security risk analysis shall be updated based on findings of the security audits.

EXPECTED OUTPUT: Security audits report [SF; QR, AR, ORR].

5.4.4 Vulnerability Management

ECSS-E-ST-80_0600129

a. For each system a vulnerability management policy shall be defined.

ECSS-E-ST-80_0600130

b. The vulnerability management policy shall include at least the following:

1. The vulnerability scoring methodology to be used to assess the severity of the identified vulnerabilities;
2. The sources (“feeds”) of known vulnerabilities applicable to the system;
3. A mechanism/methodology to automatically correlate the system inventory with known vulnerabilities on COTS and FOSS used in the system (passive vulnerability assessment);
4. The importance of the system and information assets in terms of Confidentiality, Integrity and Availability (known also as “Security Sensitivity” or “Security Profile” of the assets).

NOTE The importance of a system and information assets in terms of Confidentiality, Integrity and Availability can be assessed using a security risk assessment.

ECSS-E-ST-80_0600131

c. Passive and active vulnerability assessments shall be performed during development, as part of the qualification, before acceptance and during operation.

NOTE Active vulnerability assessment can be performed using a vulnerability assessment tool, ideally using authenticated scanning to the systems to be assessed.

ECSS-E-ST-80_0600132

d. The security risk analysis shall be updated based on the identified vulnerabilities.

EXPECTED OUTPUT: Vulnerability assessment report [SF; QR, AR, ORR].

ECSS-E-ST-80_0600133

e. The security risk management process shall be followed for the identified vulnerabilities.

5.4.5 Penetration Testing

ECSS-E-ST-80_0600134

a. Independent penetration tests shall be performed during development, as part of the qualification, before acceptance and during operation.

NOTE Independent means that the penetration testers have not been involved in the design, development or implementation of the system(s).

ECSS-E-ST-80_0600135

b. The level of independence of the penetration testing team shall be agreed with the customer.

NOTE Level of independence can depend on whether the penetration testing team comes from an external company or agency, or whether it is an internal team independent from the development team, etc.

ECSS-E-ST-80_0600136

c. The penetration testing team shall have appropriate skills and qualifications to undertake the activity in line with the sensitivity of the assets to be tested.

ECSS-E-ST-80_0600137

d. The penetration testing team (also known as red team) shall replicate the potential adversarial threat to a given mission to assess vulnerability and to detect weaknesses.

ECSS-E-ST-80_0600138

e. The penetration testing scope and scenarios shall be agreed in advance with the customer.

ECSS-E-ST-80_0600139

f. The security risk analysis shall be updated based on the vulnerabilities identified during the penetration test.

EXPECTED OUTPUT: Penetration testing report [SF; QR, AR, ORR].

ECSS-E-ST-80_0600140

g. The security risk management process shall be followed for the identified vulnerabilities.

Annex A (informative) Security Documents

This annex defines the structure of the security documents to be produced, as depicted in Figure A-1:

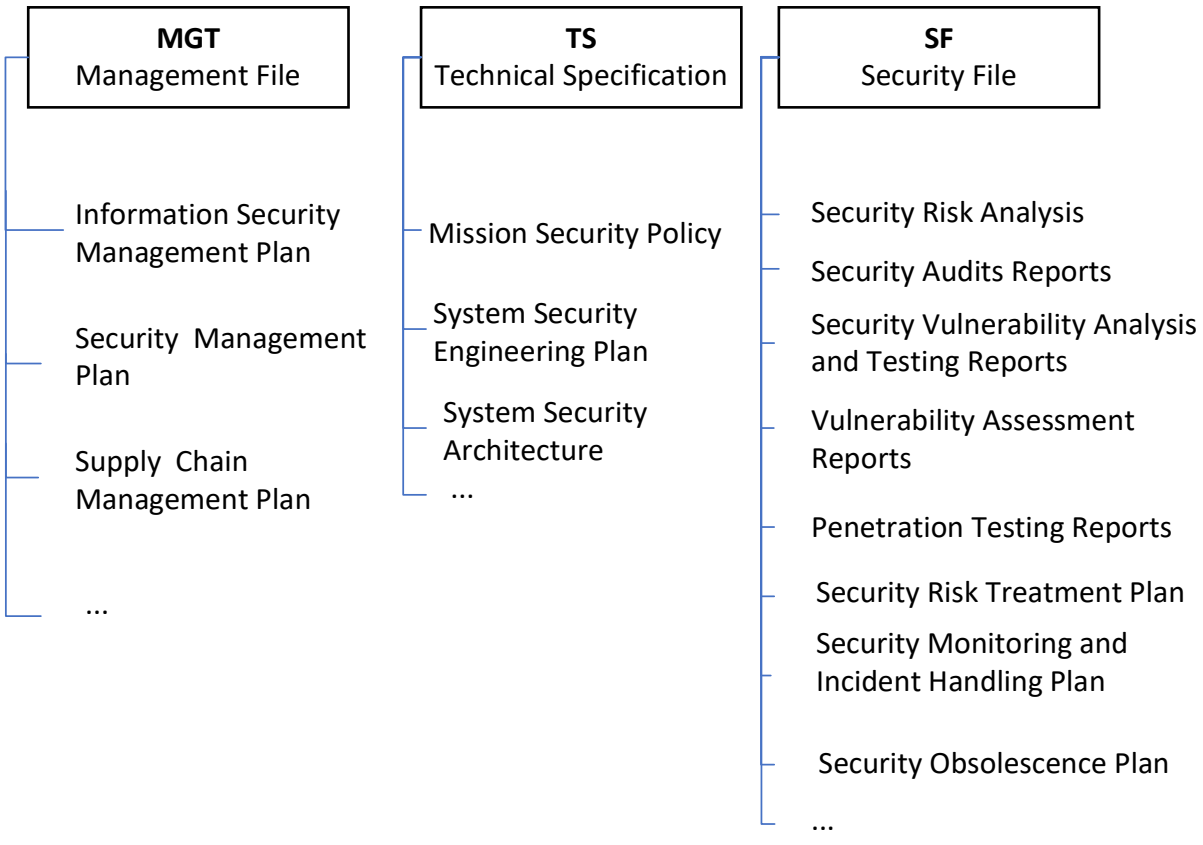


Figure A-1: Security Documents to be produced

In Figure A-2 the correspondence of the produced documents to the phases are depicted.

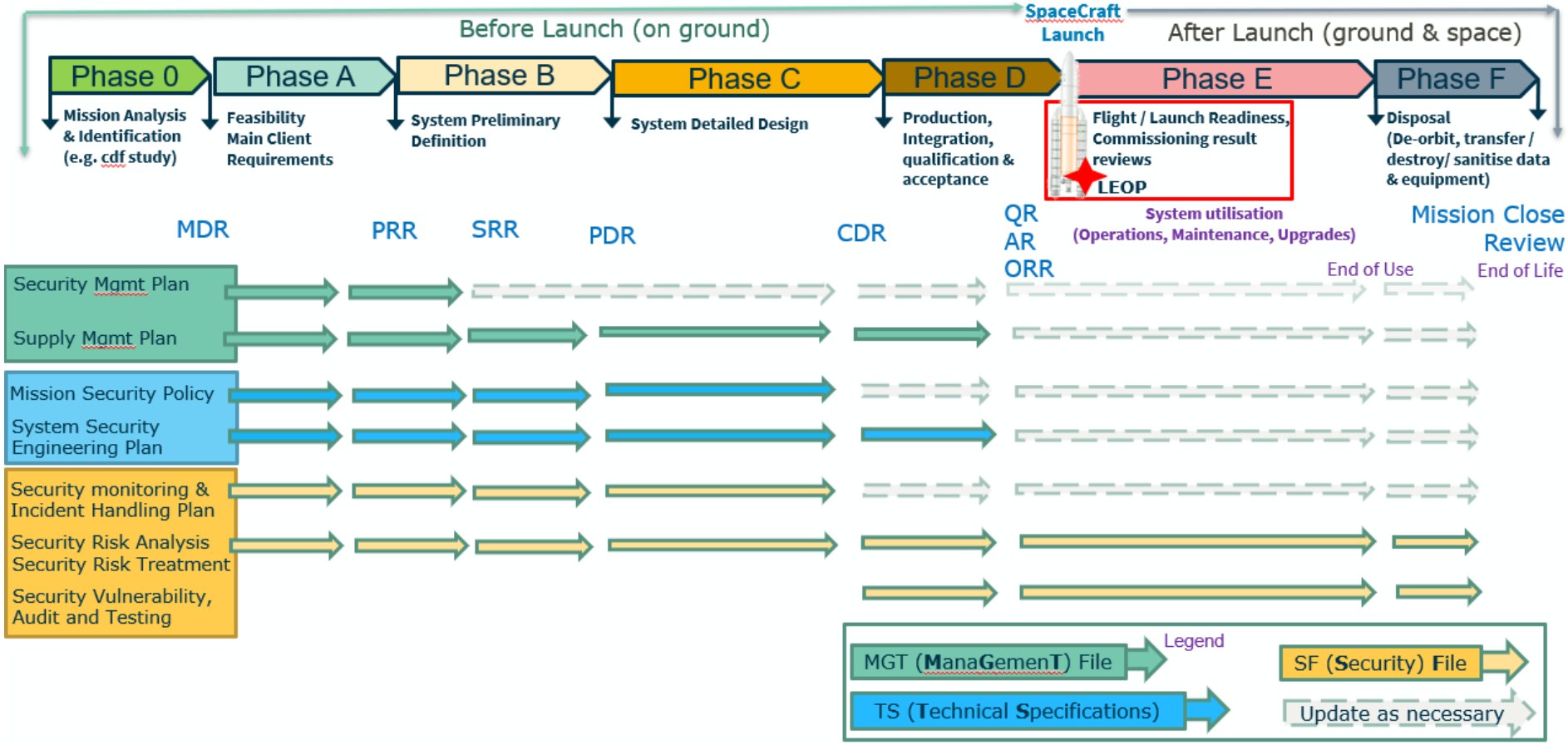


Figure A-2: Typical Security Documents to be produced per phase

Table A-1 represents the document requirements list, identifying the documentation to be produced per milestone for each related file in accordance with the requirements defined in this Standard.

Table A-1: Document requirements list (DRL)

Related file	DRL item (e.g. Plan, document, file, report, form, matrix)	KOM	SRR	PDR	CDR	QR	AR	ORR
MGT	Security Management Plan*	✔	✔					
	Supply Chain Management Plan*	✔	✔	✔	✔	✔	✔	
TS	Mission Security Policy*	✔	✔	✔	✔			
	System Security Engineering Plan		✔	✔	✔	✔		
	System Security Architecture			✔	✔	✔		
SF	Security Risk Analysis		✔	✔	✔	✔	✔	✔
	Security Audits Report					✔	✔	✔
	Vulnerability Analysis Report			✔	✔	✔	✔	✔
	Vulnerability Assessment Reports					✔	✔	✔
	Penetration Testing Reports					✔	✔	✔
	Security Obsolescence Plan*			✔	✔	✔		
	Security Risk Treatment Plan			✔	✔	✔	✔	✔
	Security Monitoring and Incident Handling Plan*		✔	✔	✔	✔		
* They can also be updated at later phase if/when needed.								

Annex B (informative) Common Threats Applicable to Space Missions Affecting Security

B.1 Data Corruption / Modification

Data Corruption/Modification refers to the intentional or non-intentional alteration of data, whether being communicated or at rest. Data corruption/modification always implies a breach of data integrity. Data can be corrupted at rest, in transit, or during processing, at its original source, final destination, or anywhere in between.

Possible Mission Impact: Corruption can be a result of software failures or bugs, hardware failures, use of unauthorized software, or active attempts to change/modify data to deny its use. A corrupted spacecraft command can result in catastrophic loss if either no action occurred (e.g., command is discarded) or the wrong action was taken onboard a spacecraft. For example, if a navigation manoeuvre burn command were corrupted, the spacecraft can end up in an unusable orbit, miss an encounter with a comet/planet/asteroid, or be destroyed.

Applicable to: Space Segment, Ground Segment, Space-Link Communication

Reference: CCSDS 350.1-G-3, para. 3.4.2 (mod.)

B.2 Denial-of-Service

Denial-of-service attacks can occur in several ways: consumption of resources (e.g., communication bandwidth, processor bandwidth, disk space, memory), disruption of system/network configurations (e.g., routing changes), disruption of state information (e.g., persistent network connection resets), disruption of network components (e.g., router or switch crashes), or obstruction/destruction of communications paths. High powered lasers can blind sensors or destroy solar cells. High powered microwaves can cause CPU restarts, disruption of electronics, or memory errors.

Possible Mission Impact: Denial-of-service attacks can prevent authorized access to resources, both in space and on the ground. Ground systems and their networks can be greatly affected by loss of system availability, which can result in an inability to control a mission or obtain data from a mission.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.6 (mod.)

B.3 Ground System Loss

A successful exploitation of a vulnerability through a physical/cyber-attack can disable the ground facility and directly affect the operation of the mission and the services provided. An attack can also take physical control of the facility to take control of the spacecraft without technically attacking the facility's systems. Environmental factors can also result in the loss of a ground facility. Tornados, hurricanes, tsunamis, flooding, or other weather-related factors can result in physical damage to the facilities or the loss of electrical power to the ground station.

Possible Mission Impact: The loss of a ground system can result in the loss of data, loss of access to data in a timely manner, degradation or loss of spacecraft commanding, or loss of the entire mission.

Applicable to: Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.3 (mod.)

B.4 Interception of Data

Possible Mission Impact: If the data is not encrypted, or is encrypted using weak algorithms or implementations, interception of data may result in the loss of data confidentiality and data privacy. In addition to those entities authorized for the data, non-authorized entities may also gain access. The interception of data can also result in masquerade or replay attacks.

Applicable to: Space Segment, Ground Segment, Space-Link Communication

Reference: CCSDS 350.1-G-3, para. 3.4.4 (mod.)

B.5 Jamming

An attack that attempts to interfere with the reception of broadcast communications. [IETF RFC 4949, Internet Security Glossary, Version 2].

Denial of communications to and from spacecraft can be accomplished by interfering with the RF signal. This can be achieved by injecting noise, by transmitting on the same frequency from another source, Electromagnetic Pulse (EMP), high powered microwave, or overpowering the original source. Optical sensors can be blinded, and solar arrays damaged by lasers.

[Source: CCSDS 350.1-G-3, para. 3.4.5]

Possible Mission Impact: The interference can result in link loss and loss of mission control. Spacecraft commanding as well as the ability to receive science or engineering data from the spacecraft can be blocked. In addition, authorized access to system resources can be blocked, possibly delaying time-critical operations on both the ground and in space.

Applicable to: Space Segment, Ground Segment, Space-Link Communications

Reference: CCSDS 350.1-G-3, para. 3.4.5 (mod.)

B.6 Masquerade

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. [IETF RFC 4949, Internet Security Glossary, Version 2] [also used in NIST standards].

Authentication of an entity's true identity is crucial for applying access control policies. When access control policies are being enforced, certain entities are allowed to perform specific actions while other entities may be denied. Access controls can be rendered useless if entities disguise their true identity or can masquerade as another entity. The lack of authentication can affect all space communications.

Possible Mission Impact: If an instrument operator masquerades as a spacecraft operator, incorrect spacecraft bus health and status actions can result in a loss of the mission. Likewise, if an external entity can masquerade as a spacecraft operator; unauthorized commands can be transmitted to the spacecraft resulting in damage, data loss, or loss of a mission.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.7 (mod.)

B.7 Replay Attack

An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack. [Source: IETF RFC 4949, Internet Security Glossary, Version 2]

For example, transmissions to or from a spacecraft or between ground system computers can be intercepted, recorded, and played back at a later time.

Possible Mission Impact: If the recorded data were a command set from the ground to the spacecraft and they are re-transmitted to their originally intended destination, they can be acted upon, potentially for a second time. If the replayed commands are not rejected, they can result in a duplicate spacecraft operation such as a manoeuvre burn or a spacecraft reorientation with the result that a spacecraft is in an unintended orientation (e.g., tumbling, antenna pointed in the wrong direction, solar arrays pointed away from the sun, or the reset of critical onboard parameters).

Applicable to: Space Segment, Ground Segment, Space-Link Communications

Reference: CCSDS 350.1-G-3, para. 3.4.8 (mod.)

B.8 Software Threats

Users, system operators, and programmers often make mistakes that can result in security problems. Users or administrators can install unauthorized or un-vetted software, which can contain bugs, viruses, spyware, or which can simply result in system instability. System operators can configure a system incorrectly resulting in security weaknesses. Programmers may introduce logic or

implementation errors which can result in system vulnerabilities or instability /unreliability. Weaknesses may be discovered after a mission is operational, which external threat agents can attempt to exploit to inject instructions, software, or configuration changes.

Possible Mission Impact: Software threats can result in loss of data, loss of spacecraft control, unauthorized spacecraft control, or loss of mission.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.9 (mod.)

B.9 Unauthorized Access

Access control policies based on strong authentication provide a means by which only authorized entities are allowed to perform system actions, while all others are prohibited.

"Weakness of an asset or control that can be exploited by one or more threats." Acc. To [ISO27K, (3.77)]

"Vulnerability weakness in the TOE that can be used to violate the SFRs in some environment." Acc. To [CC Part 1-17, Section 4.5 'Terms and definitions related to the AVA class'])

Possible Mission Impact: An access control breech would allow an unauthorized entity the ability to take control of a ground system or a ground system network, shut down a ground system, upload unauthorized commands to a spacecraft, obtain unauthorized data, contaminate archived data, or completely shut down a mission. If weak access controls are in place, unauthorized access can be obtained. Interception of data can result in unauthorized access because identities, identifiers, or passwords can be obtained. Social engineering can be employed to obtain identities, identifiers, passwords, or other technical details permitting unauthorized access.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.10 (mod.)

B.10 Supply Chain Threats

Software and hardware originate from various sources. Some of the sources are domestic, and some are not. Some are vetted, trusted sources, whereas some are not.

Chain-of-custody, even from vetted sources, is required to ensure that only genuine hardware and software, in full compliance with requirements and specifications, is delivered and integrated. Trust shall be validated and re-validated as the supply chain may have access to sensitive materials that require protection.

Resources, services and facilities with their logistical elements contribute to the supply chain that are specific for each project with resulting security risks and threats that need to be considered and addressed. Resources such as cloud services utilise a shared responsibility model. Outsourced suppliers or

workforce providing services require strong contractual coverage minimising security risks associated with the loss of direct control by the project.

Transport of equipment and supplies can be affected and disrupted by threats such as access to parts, fuel, even labour shortages or access to rare raw materials. Considering may be necessary if the transport is being made on sensitive or critical assets and potential impacts in case of disruption, destruction, loss or access and leakage of sensitive information.

Finally, hardware and software can be tainted because it can contain hidden, malicious capabilities, since cannot be produced by the claimed manufacturer and be counterfeit.

Possible Mission Impact: Supply chain disruption can result in genuine parts being unavailable, thereby resulting in the potential use of counterfeit parts. If trust is not verified, counterfeit hardware or software can be delivered and used on a mission without anyone's knowledge. The hardware or software may contain malicious circuits or malicious code that can result in unintended mission consequences. The hardware or software can allow unauthorized access to the system, or it can prohibit authorized access. It can send telemetry or observation data to an unauthorized entity. It can ignore authentic commands. Some of these scenarios can result in mission loss. Partners in the supply chain may expose or provide access to sensitive materials, cause disruption or delays to the availability of schedule critical elements. Connected suppliers with security weaknesses can be compromised and used to impact the availability of support services or to launch attacks on Agencies, systems, and missions. In addition, the mission may be seriously impacted by hardware or software that do not have all of the specified capabilities of the genuine hardware or software. The tainted hardware or software may lead to premature failure. The mission may be impacted by additional, hidden capabilities contained in the counterfeit hardware/software such as transmitting data to unauthorized and unintended destinations, intermittent system instability, damage to other system components, or other undesirable system effects that can lead to mission loss.

Applicable to: Space Segment, Ground Segment

Reference: CCSDS 350.1-G-3, para. 3.4.11/3.4.12 (mod.)

B.11 Other Threats with an Impact to Security

Threats such as human accidental or intentional, Physical threats such as kinetic attacks on satellites (kinetic weapon such as a missile, or laser to blind or damage the vehicle or to manipulate a satellites orbit) or a space-based platform, perhaps a hijacked satellite.

For satellites or ground systems with high value information, they may be targeted by 'characterisation' missions to eavesdrop or monitor the capabilities of the assets (whether on-ground or in-space).

Environmental threats such as geomagnetic storms, solar radiation, radio blackouts, satellite or debris conjunction events. Earth based environmental threats may include weather events (storms, rain, snow, lightning) as well as facilities such as flooding, electrical power disruption.

Possible Mission Impact: These threats can range from mildly disruptive, temporary denial of a command link or service, through to the release of unauthorised information and potentially the destruction of a mission or the ground facilities.

Applicable to: Launch Segment, Space Segment, Ground Segment, Space-Link Communication, Supply Segment.

B.12 Summary

The following table summarises the recommended security measures to counter act the most relevant threats for space systems [source: CCSDS 350.1-G-3, para. 5.8]. An exhaustive list of threats (but not specific to space missions) can be found in NIST Special Publication 800-30, appendix E.

Table B-1: Security Mechanisms to Counter Threats, Mitigations and Contingencies [source: CCSDS 350.1-G-3, para. 5.8, mod.]

Threat	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
Data corruption	• Data integrity schemes (hashing, check values, digital signatures) • Resilient hardware	• Secure data backups	• Verify integrity of backups • Hold offsite copies of critical data for cyber disaster scenarios
Ground facility physical attack	• Guards • Gates • Access control	• Alternate ground facilities	• Failover or hot standby to alternate site
Interception (Eavesdropping)	• Protection of traffic via encryption, frequency hopping, spread spectrum • Protection of archive & distribution systems via encryption	• Use secure transmission	• Use hardened transmission facilities
Jamming	• Multiple uplink paths • Multiple access points • Frequency hopping, spread spectrum	• Legislation • Monitoring • Interdiction • Reporting	• Have alternate frequencies or transmission facilities available • Provide resilience for outages (e.g. PNT local clocks, alternate sources)
Denial-of-Service (DoS)	• Firewalls • Routers • Switches • Intrusion Prevention Systems • Private, segregated networks • Encryption & authentication • ISP 'edge' support	• Access control lists • Rate limiting • 'expect' scripting • Service screening	• Safe Mode • Fault detection and isolation
Masquerade / Spoofing	• Strong authentication • Access control scheme • Vetting of staff • No use of open networks	• Strong authentication • Session tokens • Behaviour • Timestamps	• Intrusion Detection Systems • Intrusion Prevention Systems
Replay	• Data integrity schemes (e.g., authenticated command counter, timestamps)	• Sequence numbers • One-time passwords • Session tokens (nonces) • Timestamps • Challenge-response	• Intrusion Detection Systems • Intrusion Prevention Systems

Threat	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
Software Threats	• Acceptance testing • System evaluation (e.g., IVV, code analysis) • COTS product use • Continuous threat monitoring, continuous security risk management • Run-time security monitoring • Auditing • Software partitioning (trusted computing base) • Supply chain confidence • Data Leak Protection	• Secure software development methodologies • Security monitoring	• Develop multiple, independent implementations from the same specification for higher assurance platforms
Unauthorized Access	• Encryption of TT&C and mission data • Authentication/authorization of commands • No use of open networks • Access control in control centre • Access control in cross support network • Access control in control and dissemination systems • Accountability of access • Multiple access paths • Auditing & accounting • Non-repudiation • Authentication tokens (e.g. smart cards) • Access controls; flight, flight-to-ground, on-ground. • Access controls using data and service segregation • Apply security hardening and least privilege principles • Vetting of staff	• Strong authentication – Session tokens (nonces) • One-time passwords • Multi-factor authentication • Security monitoring	• Intrusion Detection Systems • Intrusion Prevention Systems

Threat	Security Mechanisms to Counter Threat	Threat Mitigations	Threat Contingencies
Tainted Components (hardware/software)	• Supply chain confidence • Authenticity of components • Vetted component suppliers • Vetted component production • Analysis of component functionality • Multi-vendor component components	• Diverse hardware purchasing • Blind buy purchasing • Random IVV testing	• Resource utilization monitoring • Intrusion detection • Intrusion prevention • Vetted back-up hardware stocks

Supply Chain	• Supply chain confidence
	• Vetted/trusted sources
	• chain of custody evidence
	• contract and performance penalties
		• Multiple, vetted
		• sources (non-reliance on a single source)
		• Strong chain of custody documentation
			• Accumulation of:
			  ○ parts enabling
			  ○ emergency
			  ○ reaction

The reader, for further information on the topic, can also refer (without this constituting any endorsement) to:

- https://sparta.aerospace.org,
- https://spaceshield.esa.int/

Bibliography

ECSS-S-ST-00	ECSS system - Description, implementation and general requirement
ECSS-E-ST-70-11	Space engineering - Space segment operability
ECSS-M-ST-80	Space project management – Risk management
CCSDS 350.1-G-3	Security Threats against Space Missions
CCSDS 350.7-G-2	Security Guide for Mission Planners
CCSDS 350.8-M-3	Information Security Glossary of Terms
IETF RFC 4949	Internet Security Glossary, Version 2
ISO/IEC 27000	Information technology — Security techniques — Information security management systems - Overview and vocabulary
ISO/IEC 27001	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
ISO/IEC 27005:2022	Information security, cybersecurity and privacy protection — Guidance on managing information security risks
ISO/IEC/IEEE 24765:2017	Systems and software engineering vocabulary
NIST SP 800-12	An Introduction to Computer Security: The NIST Handbook
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-45	Guidelines on Electronic Mail Security
NIST SP 800-53 Rev. 5	Computer Security Incident Handling Guide
NIST SP 800-61 Rev. 2	Computer Security Incident Handling Guide
NIST SP 800-82	Guide to Operational Technology (OT) Security
NIST SP 800-95	Guide to Secure Web Services
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
NIST SP 800-160, Volume 1	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST SP 800-160, Volume 1 Rev.1	Engineering Trustworthy Secure Systems
NIST SP 800-160, Volume 2	Developing Cyber Resilient Systems – A Systems Security Engineering Approach
NIST SP 800-192	Verification and Test Methods for Access Control Policies/Models
NISTIR 8183	Cybersecurity Framework Manufacturing Profile