RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

cnes
CENTRE NATIONAL
D'ÉTUDES SPATIALES

ORBITAL SYSTEM
CYBERSECURITY HYGIENE GUIDE

Studio Graphique CNES, 2025- 265

Preface

Lionel Suchet

Interim CEO

The vital role that space plays in the day-to-day operation of individual, scientific, economic, and sovereign government activities is no longer disputed. In recent years, digitization and the arrival of many "new" players have greatly changed the ways an orbital system is designed, constructed, launched, operated, and used in a geopolitical context where there are all kinds of conflicts and tensions. It was, therefore, more recently that we were able to gauge the consequences of our dependence on space services, infrastructures, and systems, especially by observing the sharp increase in the volume and complexity of cyberattacks targeting them.

Therefore, space's strategic importance is no longer a secret, especially for those with ill intentions. Several recent cases in the news have demonstrated that orbital systems are exposed and that some ill-intentioned parties can exploit their vulnerabilities.

These new threats require us to adapt our response: we can no longer consider our space systems protected through their isolation or by a technology only available to a few organizations.

This is why CNES, in addition to the measures it has already taken for many years, has decided to take a number of proactive steps to head off this ill-defined and dissymmetric threat. This guide, prepared with our industrial, institutional, and academic partners, is the first step: the recommendations it makes stand alongside the new French Space Operations Act and, thanks to your contributions, will help prepare our future specific and sector-related activities. It is, therefore, vital to test the waters with this compilation of best practices so that it can evolve to meet the challenges we face.

We are certain that this is how we can improve our space cybersecurity practices, strengthen France's position in this field, guarantee that the support we lend to our institutional and industrial partners' space activities is effective and relevant, and take the space sector to the highest level.

TERMS DEFINITIONS ABREVIATIONS

Acronym/ Abbreviation	Definition
AIT	Assembly, Integration and Test
ANFR	French National Frequencies Agency
ANSSI	French National Cybersecurity Agency
BCP	Business Continuity Plan
BRP	Business Recovery Plan
CCSDS	Consultative Committee for Space Data Systems
CERT	Computer Emergency Response Team
CESTI	Information Technology Security Assessment Centres
CNES	French Space Agency (Centre National d'Etudes Spatiales)
COTS	Commercial Off The Shelf
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVE	Common Vulnerability Exposure
DAST	Dynamic Application Security Testing
EAR	Export Administration Regulations
EBIOS RM	Expression of Needs and Identification of Security Objectives Risk Manager
EOL	End Of Life
EOS	End Of Support
EUSL	European Space Law
FLSC	First Level Security Certification
FSOA	French Space Operations Act
HSM	Hardware Security Module
IDPS	Intrusion Detection and Prevention System
IGI	Interministerial General Instruction
II	Interministerial instruction
IoC	Indicator of Compromise
IS	Information System
ISAC	Information Sharing and Analysis Centre
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager
ISSP	Information Systems Security Policy
IT	Information Technology
ITAR	International Traffic in Arms Regulations

ITU	International Telecommunication Union
ITAR	International Traffic in Arms Regulations
KMI	Key Management Infrastructure
KMS	Key Management Service
FMPL	French Military Programming Law (Loi de Programmation Militaire)
MCO	Maintenance in Operational Condition
MCS	Maintenance in Secure Condition
MFA	Multifactor Authentication
MINARM	Ministry of the Armed Forces
NIS	Network and Information Security
OT	Operational Technology
OTAR	Over-the-air-rekeying
PGSC	General Security and Cybersecurity Policy
PKI	Public Key Infrastructure
PPST	Protection of Scientific and Technical Potential
PSI	Programme Security Instruction
PQC	Post-Quantum Cryptography
RETEX	Feedback (RETour d'EXpérience)
RF	Radio Frequency
ROOT CA	Certificate Authority Root
RRF	Rapid Response Force
RRZ	Restrictive Regime Zone (Zone à Régime Restrictif)
SAP	Security Assurance Plan
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SDR	Software-Defined Radio
SDS	Software-Defined Satellite
SIEM	Security Information and Event Management
SOC	Security Operation Centre
SSA	Space Situational Awareness
STIX	Structured Threat Information Expression
TAXII	Trusted Automated eXchange of Indicator Information
TC	Telecommand
TEE	Trusted Execution Environment
TEMPEST	Telecommunications Electronic Materials Protected from Emanating Spurious Transmissions
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
TM	Telemetry
TRANSEC	Transmission Security
VPN	Virtual Private Network

Sommaire

01 INTRODUCTION

1.1 I CONTEXT

Managing the level of cybersecurity of orbital systems is currently a hot topic and a major concern for governments. In recent years, the number of attacks targeting space infrastructures has risen. The war in Ukraine has confirmed this trend. This event, which started with an attack on a space operator, is proof that conflict is seeping into the space sector.

The first cyberattacks on orbital systems recorded in the public domain date back to the late 1970s. There was an estimated average of 5 known attacks per year up to 2020. Since 2020, publicly referenced cyberattacks have skyrocketed to more than 46 in 2022, around 80 in 2023, and more than 110 in 2024.

The complexity of these attacks has increased immensely in recent years, with attackers increasingly interested in disrupting space missions that are vital to the countries' critical infrastructures.

Geopolitical, economic, and technological issues linked to space security have led institutions to consolidate current regulations that can today be considered fragmented. Orbital systems stakeholders need guidelines and best practices that are both relevant and sufficiently specific to improve and harmonize the resilience of all the players making up the space ecosystem.

1.2 I OBJECTIVES & PRIORITIES OF THE GUIDE

CNES has created a cybersecurity hygiene guide for players involved directly or indirectly in the proper functioning of an orbital system. Applying these best practices will ensure minimum protection and reduce the risk of an attack or reduce the impact of an actual attack. This hygiene guide is based on the current state of the art in terms of best practices. It is inspired by existing literature and has been improved by the feedback provided by French space ecosystem players.

This guide is intended to suggest a set of best practices to the stakeholders of an orbital system and is not binding. It should be considered as a guide to help identify measures that could be implemented by an organization. Each player involved directly or indirectly in an orbital system should identify the best practices in this guide that are useful and applicable to them in order to improve its level of security. This is a general guide that does not claim to cover all of the players' security needs.

It can be applied to supplement or add to national regulations, such as the French Space Operations Act (FSOA), or European regulations, such as the forthcoming European Space Law (EUSL).

The first version of this guide is now available. It will be updated regularly to reflect the current state of the art in terms of best practices, and feedback from readers will be incorporated with each new version.

1.3 I SCOPE OF APPLICATION OF THE HYGIENE GUIDE

The cybersecurity hygiene guide for orbital systems is aimed at all the players in the ecosystem who are involved in operating or designing orbital systems. **In this guide, an "orbital system" is composed of segments (space segment, ground segment, signal segment), infrastructures, and all the players in the value and supply chains contributing directly or indirectly to the proper execution of the mission**. Although players involved in the user segment are concerned only indirectly, they will also find best practices applicable to them in this guide.

The players involved in this ecosystem have different roles, e.g., operator, manufacturer, and other system manufacturers or integrators. These players may also include New Space companies, VSBs/SMEs, or major industry players. The best practices identified in this guide are generic and applicable to all players.

The life cycle of an orbital system begins with a design phase and ends with a decommissioning phase. The life cycle duration leads the players involved at each phase to think about their level of security. This guide concerns the 6 different phases of a space program, i.e.: Phase A (Conception, Design), Phase B (Development, Integration, Verification, and Validation), Phase C (Detailed system design), Phase D (Testing, AIT), Phase E (Transportation, Launch preparation, Launch, Station acquisition, In-orbit validation, Operation), Phase F (Station keeping, Mission execution, End of life).

The guide applies to the information systems of players involved in the satellite's operational chain, from the preliminary design phases to operating and end-of-life.

This guide aims to be generalist and proposes best practices applicable to all information systems involved throughout the life cycle of an orbital system, whether this system is IT (information technology)-oriented or OT (operational technology)-oriented. This guide is intended for all players involved throughout the orbital system's life cycle.

FIGURE 1: **SCOPE OF THE HYGIENE GUIDE**

1.4 I READING GUIDE

This orbital system cybersecurity hygiene guide is based on a list of best practices to implement. The **best practices are grouped together into categories**, and a **set of themes** has been identified for each category.

Each theme is broken down as follows:

- **Description:** General description and contextualisation of the best practice.
- **Recommendation or best practice:** A measure to guarantee a minimum level of cybersecurity for the orbital system.
- **Support document** (excel file): spreadsheet listing all the best practices identified in this guide. It makes it possible to track the applicability and implementation of each best practice for each phase of the orbital system's life cycle.
- **Supplementary case study document** *(supporting document provided in the appendix as part of version 2 of the guide)*: The aim is to illustrate what happens when best practices are not implemented using examples or scenarios. This description is generally based on cases of cyberattacks on publicly known orbital systems.

In this guide, the **"organization" appoints the entity responsible for implementing the best practices identified**. An action can be carried out at different levels (manufacturer, operator, subcontractor, supplier). This level of detail will be considered in a later version of the guide.

02 HYGIENE GUIDE AND BEST PRACTICES

2.1 I HOW THE GUIDE WAS PREPARED

The **guide was prepared in 3 stages:**

1. **Understanding current regulations** by identifying all known national or international recommendations.
2. **Interviews with CNES** personnel involved in the various phases of an orbital system life cycle.
3. **Collective brainstorming workshop with players outside CNES** to consolidate the best practices identified, ensure that the approach is comprehensive and ensure that the needs of players with different opinions are properly understood.

2.2 I LIST OF BEST PRACTICE CATEGORIES

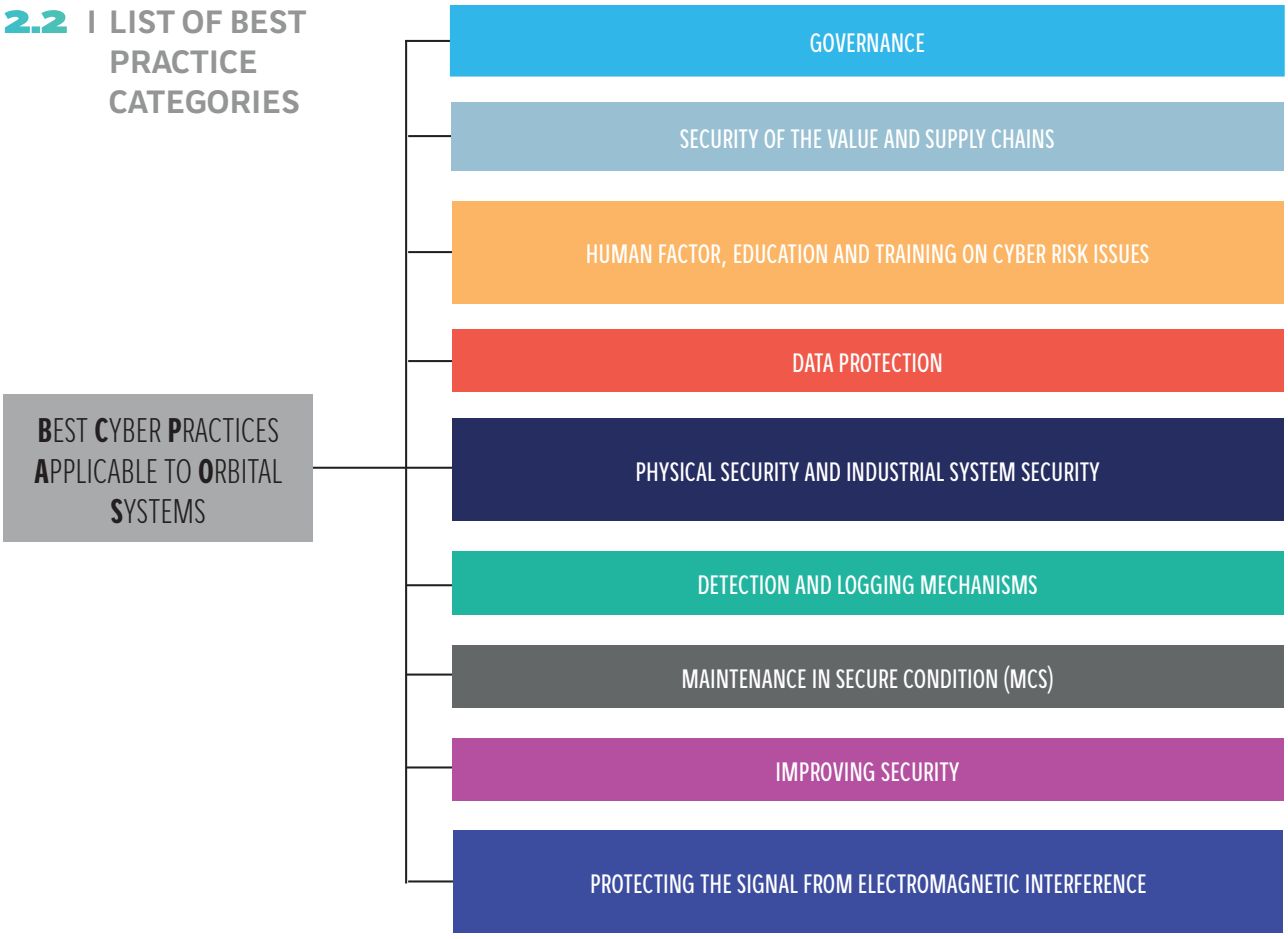


FIGURE 2: **BEST PRACTICE CATEGORIES**

2.3 | GOVERNANCE

ANSSI stresses that digital risks have become strategic risks for organizations. Governance aims to provide the strategic and organizational framework needed to anticipate, prevent, and respond to digital risks in the different phases of an orbital system, from design to operation and up to end-of-life.

Good governance of digital risks requires setting up an **organizational structure with clear responsibilities and a specific budget**. The aim is to define the organization's digital security strategy using a roadmap, ensure that an information system security policy is implemented, and manage its performance.

Risk analysis is a starting point for identifying a large number of security measures to implement. This can be based on a risk analysis method such as EBIOS Risk Manager.

Information systems can be **approved** to build confidence in the information systems before operating them. Approval is used to identify, achieve, and then maintain a level of risk acceptable for the information system in question. Approval is granted by a certification authority.

Regulatory compliance is a high priority and means mastering the requirements imposed by an ecosystem, a government, or a contract giver.

Controlling one's security means adapting on a daily basis through forward-thinking actions after **sharing with the ecosystem** through discussion groups such as CERT, CSIRT, or ISAC.

2.3.1 | ORGANIZATIONAL CYBERSECURITY STRUCTURE

SYS-ORBIT-GOUV_100: The organization **sets up an organizational structure to create cyber governance and ensures its proper implementation**. Cyber governance consists of all the decisions that the organization must make to guarantee the security of its information systems.

SYS-ORBIT-GOUV_101: The organization appoints individuals responsible for information security who will represent and express security needs in decision-making committees. The **related roles and responsibilities should be precisely defined** (information systems security manager, product security manager, strategic manager, operational manager, internal auditor, program information systems security architect, etc.). The organizational structure of cybersecurity may vary depending on the organization and the stage of the orbital system's life cycle.

SYS-ORBIT-GOUV_102: The organization allocates a dedicated cybersecurity budget to each project, the amount of which is commensurate with technical, operational, and organizational **recommendations or regulatory requirements applicable to the IS**. The budget foreseen by the organization must include financial, hardware, software, and human resources in line with the needs identified by the project.

2.3.2 | SECURITY POLICY

SYS-ORBIT-GOUV_103: As part of its cyber governance, **the organization implements an Information Systems Security Policy (ISSP) reflecting its strategic vision for cybersecurity**. This **ISSP can be adapted** to different levels of application: Global ISSP for the organization, ISSP applicable to partners or subcontractors, Operations ISSP applicable to the operational context of the orbital system, Project ISSP, etc.

In line with the organization's General Security and Cybersecurity Policy (GSCP), the ISSP will cover various subjects such as data protection, personnel training, access, and identity management, data encryption, incident response mechanisms, data backup, and export and supply, and value chain management.

SYS-ORBIT-GOUV_104: The **organization maps its information assets and regularly updates this mapping**. Depending on the need, different types of information asset mapping can be carried out: mapping the company's ecosystem under the responsibility of the ISSM, product-oriented mapping under the responsibility of the product security manager, orbital system-oriented mapping, support service-oriented mapping, etc.

SYS-ORBIT-GOUV_105: The organization **determines the classification level of its information assets according to the level of data sensitivity** and in accordance with the applicable guidelines and requirements (PPST, FMPL, IGI no. 1300, IGI no. 901).

SYS-ORBIT-GOUV_106: The organization sets up a Programme Security Instruction (PSI) to guarantee the security of the information exchanged. This instruction includes an appendix containing the information's classification level and serves as a contractual security plan covering the organization or orbital system's information system exchanges.

2.3.3 | RISK ANALYSIS APPROACH

SYS-ORBIT-GOUV_107: The organization implements a risk governance process based on a **risk analysis method compliant with international standards (ISO 27005 or EBIOS Risk Manager, for example)**, in accordance with the recommendations of national or international security agencies. The content of the risk analysis and, in particular, the identified attack scenarios or residual risks must be protected.

SYS-ORBIT-GOUV_108: The organization outlines and defines the technical and activity scope of the information system for the orbital system for which a risk analysis is conducted. It has a global vision of its information system and is capable of mapping it.

SYS-ORBIT-GOUV_109: The organization assesses the current threat level, the risks sources and the objectives for the orbital system to be protected.

SYS-ORBIT-GOUV_110: As part of this regular risk analysis approach, the organization **sets up a daily monitoring process** to monitor and identify new risks. This regular monitoring makes it possible to improve the measures implemented.

SYS-ORBIT-GOUV_111: The organization **identifies strategic or operational risk scenarios.**

SYS-ORBIT-GOUV_112: The organization puts in place a system to deal with the identified risks (prevention, reduction, transfer, acceptance).

2.3.4 | APPROVAL PROCEDURE

SYS-ORBIT-GOUV_113: When necessary, the organization sets up a **certification procedure** for its information systems. Certification must be tailored to the organization's system security priorities. The organization must contact the appropriate certification authority.

2.3.5 | REGULATORY COMPLIANCE

SYS-ORBIT-GOUV_114: The organization **identifies the mandatory regulatory requirements applicable** to cybersecurity. Particular attention should be paid to the FSOA (French Space Operations Act), the FMPL (French Military Programming Law), the NIS2 (Network and Information Security) directive, and the future EUSL (European Space Law).

SYS-ORBIT-GOUV_115: The organization **involves the various stakeholders in the security issues, in particular technical orbital system operators**, to ensure overall consistency and acceptance of the regulatory compliance issues.

SYS-ORBIT-GOUV_116: The organization **anticipates questions relating to export controls** on its data and documents, especially for dual-use cases (civil and military). Depending on **the orbital systems' uses, the extraterritorial scope** of foreign regulations (e.g., US ITAR or EAR) must also be taken into account.

2.3.6 | CRISIS MANAGEMENT AND RÉSILIENCE IN THE EVENT OF AN INCIDENT

SYS-ORBIT-GOUV_117: The organization **defines in advance the roles and responsibilities** within its team **to return to nominal functioning following a crisis.**

SYS-ORBIT-GOUV_118: Before a phase, the organization sets up a set of procedures to ensure **its resilience and return to nominal functioning following a crisis**, including a **BCP** (Business Continuity Plan) and a **BRP** (Business Recovery Plan).

SYS-ORBIT-GOUV_119:: The organization **foresees setting up a dedicated incident response team**, such as an **internal CERT** (Computer Emergency Response Team) or **RRF** (Rapid Response Force).

SYS-ORBIT-GOUV_120: The organization anticipates crisis communication and its public position in the event of a crisis in order to mitigate **or manage the potential effects on its reputation and public image.**

SYS-ORBIT-GOUV_121: In the event of an attack, the organization **informs the competent authorities** according to the sensitivity level of its activities (e.g., ANSSI, CNES, Ministry of the Armed Forces).

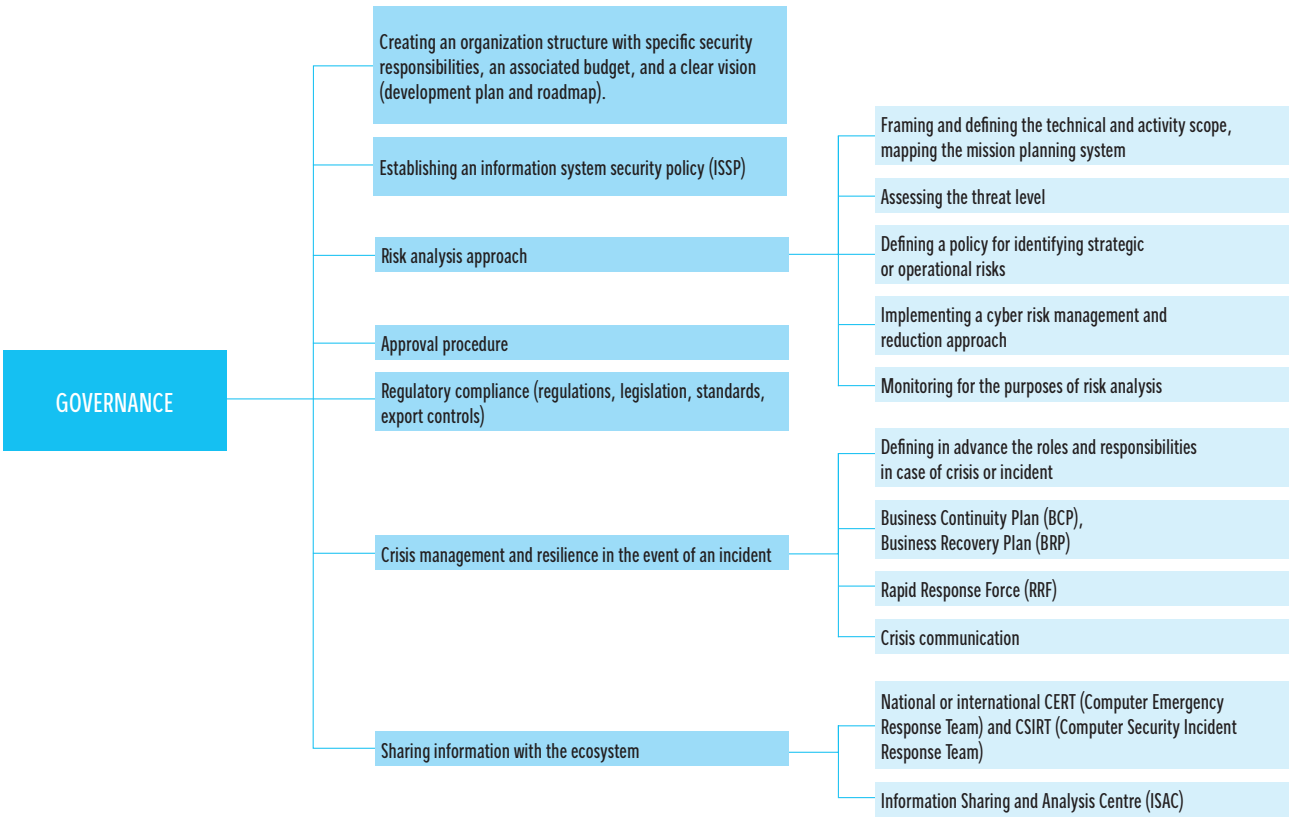
2.3.7 | SHARING INFORMATION WITH THE ECOSYSTEM

SYS-ORBIT-GOUV_122: The organization is invested and shares information, best practices and feedback with specific national or international entities such as CERT, CSIRT or ISAC. It can be useful to share information with other sectors (aviation, maritime, banking sectors, etc.).

KOUROU AS SEEN BY THE PLEIADES SATELLITE

FIGURE 3:

GOVERNANCE-RELATED THEMES



GUIANA SPACE CENTER AS SEEN FROM THE SPOT-6 SATELLITE

©Airbus/, 2015

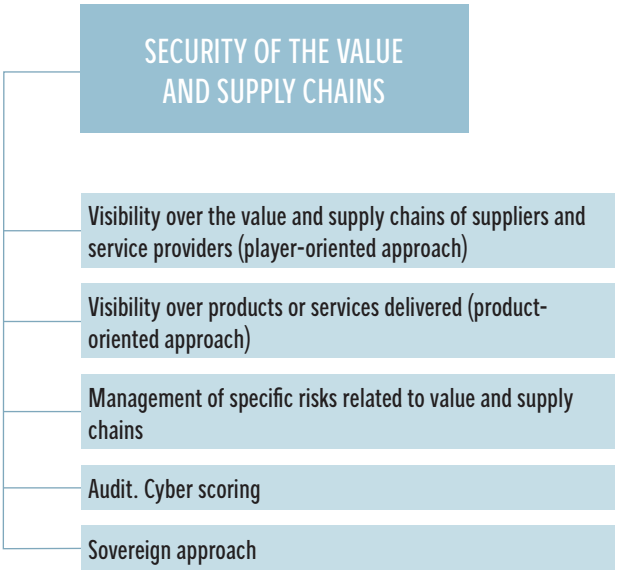
2.4 I SECURITY OF VALUE AND SUPPLY CHAINS

The value and supply chains associated with the development and operation of an orbital system involve a large number of players, often over a wide geographic area. The number of players involved increases the potential scope of attack and exposure to a cyber threat. New types of potential attacks that are increasingly common are espionage or a compromised component in the early phases of the life cycle.

Value and supply chains are increasingly complex due to the technology used by orbital systems opening up to the commercial sector and the integration of consumer technologies, in particular the use of COTS.

FIGURE 4:

THEMES RELATED TO VALUE AND SUPPLY CHAIN SECURITY



2.4.1 I VISIBILITY OVER SUPPLIER AND SERVICE PROVIDER CHAINS

SYS-ORBIT-CHAINE_200: The organization **maps its supply and value chains and identifies to what extent each participant is involved in the proper functioning of the orbital system**, including identification of tier-1 and tier-n suppliers, understanding each person's role, geographic location, type of interaction, level of dependence, etc.

SYS-ORBIT-CHAINE_201: The organization **determines extensive and achievable contractual obligations for its suppliers and service providers**. These may include, for example, the possibility of an audit, the obligation to notify the organization when a supplier or service provider changes, the right to communicate in the event of an attack, or notification in the event of obsolescence.

SYS-ORBIT-CHAINE_202: The organization **establishes a procedure to verify compliance with contractual obligations for each supplier and service provider.** This verification procedure may involve audits, investigations, and tests, such as a CESTI, to determine whether the security measures defined in the contract are followed

SYS-ORBIT-CHAINE_203: The organization **clearly communicates its expectations and the requirements and constraints applicable to its suppliers and service providers** by several means (contract, specifications, technical clauses, certification to uphold, etc.). The organization distinguishes between requirements relating to information management or security and technical requirements. The requirements may vary depending on the tier of the supplier or service provider.

In the case of a tier-1 supplier, for example, requirements may include the obligation to report information from their own suppliers.

2.4.2 I VISIBILITY OVER PRODUCTS OR SERVICES DELIVERED

SYS-ORBIT-CHAINE_204: The organization may choose to entrust any part or all of an activity that could be carried out internally to a third party through a **Security Assurance Plan (SAP)**. This document sets out the rules, guarantees, and security measures implemented by a service provider to protect its customer's data and IT systems.

SYS-ORBIT-CHAINE_205: The organization **investigates the origin of the components** of any product and service delivered by a supplier or service provider, and is able to guarantee its traceability.

SYS-ORBIT-CHAINE_206: The organization identifies **the services and products for which greater vigilance is needed due to their geographic origin**. In particular, the organization **identifies the different countries and regions** whose products and services could carry risks.

2.4.3 I MANAGEMENT OF RISKS RELATED TO VALUE AND SUPPLY CHAINS

Due to their scope and complexity, value and supply chains can carry risks for the organization. The organization must conduct a **specific risk analysis** to identify, assess, and manage cyber threats from this ecosystem.

SYS-ORBIT-CHAINE_207: The organization conducts a **risk analysis to identify specific threats related to the value and supply chain**. The organization takes into account information such as the geopolitical context or the threat level estimated by national security services.

SYS-ORBIT-CHAINE_208: **The organization pays particular attention to the risks associated with the use of COTS**. It maps its COTS in detail, determines the criteria for choosing them, such as the ability to patch or monitor vulnerabilities, and communicates them to its suppliers, making sure that these security requirements are maintained over time. Vulnerabilities associated with COTS include back doors, software or hardware, code obfuscation, dead code branches, integration of counterfeit or obsolete components or libraries, etc.

SYS-ORBIT-CHAINE_209: The organization **takes special care to protect its intellectual property, especially if its value chain includes foreign organizations.**

2.4.4 I CYBER AUDIT & SCORING

SYS-ORBIT-CHAINE_210: The organization **assesses the level of security of its suppliers and service providers.** The organization can set up a **system to assess its confidence level in its suppliers and service providers** by relying on a set of criteria and a **methodology, resulting in a final score**. The organization can define its own assessment system or delegate this task to a third party, for example, by setting up a certification program (e.g., FLSC, ISO27001, or another sector program) with a shared reference system. A high score is a sign of trustworthiness, which can help to reduce the number of controls carried out by the organization.

SYS-ORBIT-CHAINE_211: The organization **carries out regular audits of its suppliers and service providers**. The organization also encourages its tier-n suppliers and service providers to increase the accountability of their own tier-1 suppliers and service providers. To do this, the organization can inform its suppliers and service providers of the potential level of threat, the security issues, and the potential events identified in its risk analysis.

SYS-ORBIT-CHAINE_212: The organization considers **using products certified by security agencies**. It's necessary to discuss in advance with the supplier or service provider which labels the organization will accept and use.

SYS-ORBIT-CHAINE_213: The organization **devises a supplier development and security plan** to improve collaboration and increase the security measures that a supplier has implemented. To do this, the organization must understand the best practices that the supplier has implemented and can propose other best practices (based on this guide, for example).

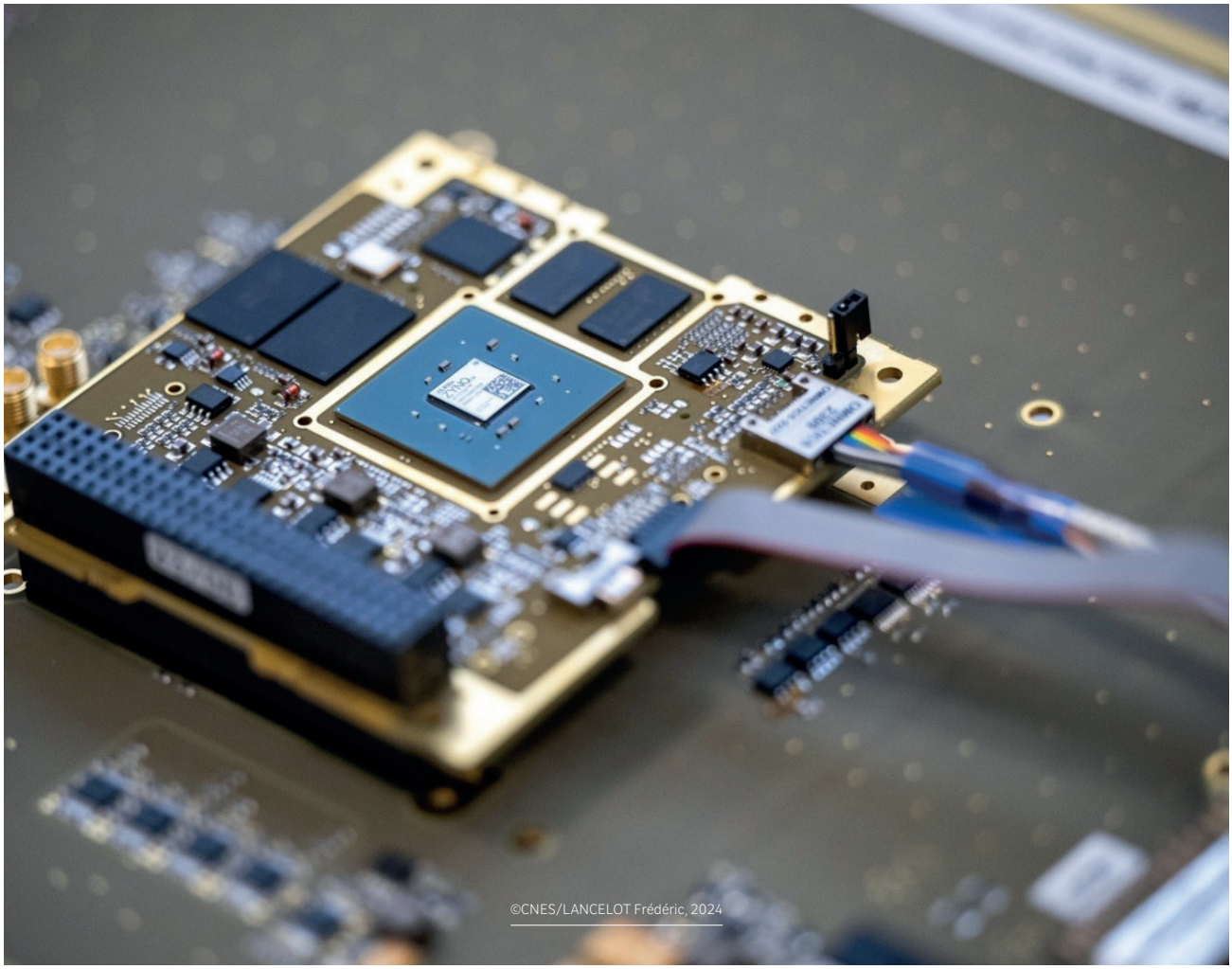
SYS-ORBIT-CHAINE_214: : The organization ensures that **each player in the value and supply chain conducts a risk assessment** of its information system and ecosystem

SYS-ORBIT-CHAINE_215: Depending on the need, the organization ensures that **certain suppliers or service providers have gone through a certification process.**

2.4.5 I SOVEREIGN APPROACH

SYS-ORBIT-CHAINE_216: Depending on the orbital system's mission and the associated risks, **the organization encourages a sovereign approach** to procurement and supplier selection.

SYS-ORBIT-CHAINE_217: Depending on the orbital system's mission and the associated risks, the organization ensures that it complies with the **restrictions or exclusions imposed by the national or international authorities on which it depends.** ▮



2.5 | HUMAN FACTOR TRAINING AND AWARENESS ON CYBER ISSUES

Human error is generally acknowledged as one of the main vulnerabilities when it comes to an information system attack scenario. A human error is exploited by indirect methods such as social engineering or email phishing. The risk associated with the human factor can be mitigated by an organization that trains and educates its employees on cybersecurity issues and risks..

2.5.1 | CYBER RISK AWARENESS

SYS-ORBIT-HUMAIN_300: The organization **creates a cybersecurity best practices awareness program.** This program focuses on creating and managing strong passwords, recognizing phishing attempts, and careful use of digital technologies in general. It is helpful to use real attack cases as examples.

SYS-ORBIT-HUMAIN_301: The organization **educates all its personnel on security issues, rules, and best practices to apply and the behavior** to adopt. The awareness sessions should be regularly updated. An independent provider can also carry out awareness sessions (e.g., using a MOOC).

SYS-ORBIT-HUMAIN_302: The organization implements measures **to assess its personnel's level of awareness, such as using phishing simulations.**

2.5.2 | CYBERSECURITY TRAINING

SYS-ORBIT-HUMAIN_303: The organization implements **training that allows the different members of the organization to improve their cybersecurity knowledge based on their position(s) and responsibilities**. This training process can be validated by awarding certifications.

SYS-ORBIT-HUMAIN_304: In accordance with **the corresponding ISSP, the organization encourages its personnel to report suspicious activities,** phishing attempts or any potential security problems. The mechanisms set up to report incidents must be simple and empowering..

SYS-ORBIT-HUMAIN_305: The organization arranges **cyber crisis management training**. Employees are trained to respond to different attacks and how to behave in the event of a cyber crisis.

SYS-ORBIT-HUMAIN_306: Depending on the needs, the organization plans **training activities based on practical cases using simulation platforms or test benches** (e.g. cyber ranges), enabling the security teams to practise on realistic cases and improve their expertise.

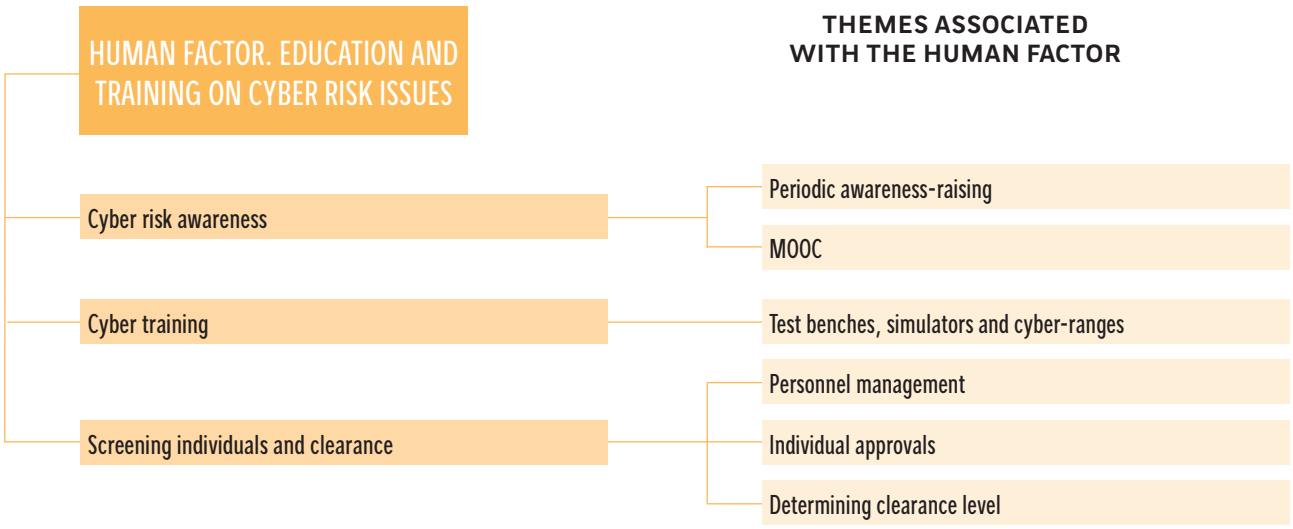
2.5.3 | SCREENING INDIVIDUALS AND CLEARANCE

SYS-ORBIT-HUMAIN_307: Depending on the needs associated with the orbital system information system, **the organization protects access to its strategic knowledge and know-how by screening people** based on right-to-know criteria, for example. It forms a responsible working team that is aware of the system's security issues.

SYS-ORBIT-HUMAIN_308: The organization determines the security notice of individuals involved in the information systems based on the sensitivity of the information they have access to and on a need-to-know basis (e.g., the French Interministerial General Instruction no. 1300).

FIGURE 5:

THEMES ASSOCIATED WITH THE HUMAN FACTOR



RTNC 2024 EVENT AT PIERRE BAUDIS CONGRESS CENTER IN TOULOUSE

2.6 | DATA PROTECTION

The increase in the number of orbital system attacks requires players to take appropriate security measures. Data protection mechanisms, such as encryption or signatures, guarantee confidentiality, integrity, and traceability.

2.6.1 | DATA MAPPING AND DEFINING PROTECTION NEEDS

SYS-ORBIT-PROTEC_400: The organization **maps its data**. It **differentiates between the different types of data** (activity data, system data, algorithms, images, onboard data, TM/TC, etc.) **and defines the protection needs for each type** (confidentiality, integrity, availability, authenticity, anti-replay) **based on their sensitivity** and the results of the risk analysis.

SYS-ORBIT-PROTEC_401: The organization implements **data protection processes according to the main security principles** such as confidentiality, accountability, traceability, integrity, authenticity or access management **according to the needs identified in the risk analysis.**

SYS-ORBIT-PROTEC_402: The organization takes special care to **protect its informational assets** and, when necessary, deploys this protection on an operational or project-by-project basis.

SYS-ORBIT-PROTEC_403: The organization implements a remote access management policy giving priority to secure connections, such as virtual private networks (VPN), and by implementing multifactor authentication-type strong authentication mechanisms (MFA).

2.6.2 | KEY MANAGEMENT AND SHARING

SYS-ORBIT-PROTEC_404: The organization **selects cryptographic algorithms adapted to the needs identified in the risk analysis**. It ensures compliance

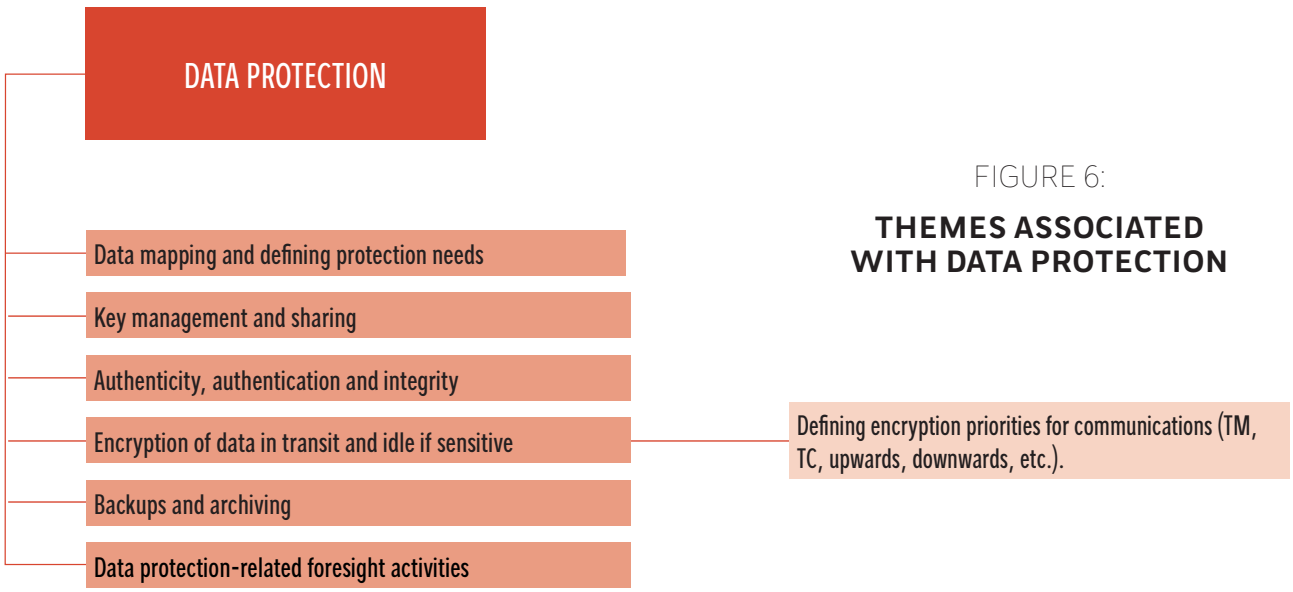


FIGURE 6:

THEMES ASSOCIATED WITH DATA PROTECTION

with the guidelines of security agencies (such as ANSSI or CCSDS). "Internal" measures must comply with current guidelines and standards.

SYS-ORBIT-PROTEC_405: The organization **ensures proper management of information system user privileges.**

SYS-ORBIT-PROTEC_406: To ensure the authenticity and encryption of the orbital system data, **the organization verifies that the initial sharing of encryption keys is secure.** In some cases, keys must be re-shared during the life cycle. The organization also ensures that the **root certificate** (also called "Root CA") of the chain of trust is exchanged securely and that certificates used downstream of the chain of trust are properly allocated.

SYS-ORBIT-PROTEC_407: A **trusted execution environment** (TEE) can be based on the use of a tamper-proof hardware security module (HSM) to be able to **generate and store cryptographic keys**.

SYS-ORBIT-PROTEC_408: The organization **sets up a Key Management Infrastructure** (KMS or PKI), covering the various types of symmetrical and asymmetrical keys, **ensuring that the keys are managed over time.** The general process may be something like production, sequestration, revocation, distribution, cryptoperiod, and key rotation.

SYS-ORBIT-PROTEC_409: In some specific cases identified, the organization can **follow the OTAR concept** (over-the-air-rekeying) to renew its encryption keys during the orbital system's operation phases.

SYS-ORBIT-PROTEC_410: **The organization anticipates the obsolescence of encryption algorithms and keys and ensures that they are replaced or updated based** on the current state of the art**.**

2.6.3 AUTHENTICATION AND INTEGRITY

SYS-ORBIT-PROTEC_411: If necessary, the organization ensures that entities connecting to the orbital system's information system are **authenticated** and that the messages exchanged are authentic through cryptographic mechanisms (e.g., public key, private key).

SYS-ORBIT-PROTEC_412: If necessary, **the organization verifies the integrity of the messages exchanged with or within the orbital system** through cryptographic primitives (e.g. hash function).

2.6.4 DATA ENCRYPTION

SYS-ORBIT-PROTEC_413: If necessary, the organization **chooses an end-to-end encryption system** to protect an entire communication chain..

SYS-ORBIT-PROTEC_414: In accordance with the risk analysis and depending on **the information's level of sensitivity, the organization encrypts the various orbital system links as required** (ground-onboard, onboard-ground, TM, TC, etc.).

2.6.5 BACKUPS AND ARCHIVING

SYS-ORBIT-PROTEC_415: **The organization defines a data backup policy** to schedule cold or hot backups to ensure data retention in the event of an attack or failure.

SYS-ORBIT-PROTEC_416: In accordance with the backup policy, the organization **makes regular backups, i.e., periodic copies of the information**, to be able to restore damaged data (e.g., using a cryptolocker). It also ensures that backups are tested regularly.

SYS-ORBIT-PROTEC_417: The organization **identifies the data it must keep over a long time and sets up an archiving system** for this purpose. Archiving must be carried out on media separate from those used for backups and must be subject to regular testing.

2.6.6 DATA PROTECTION-RELATED FORESIGHT ACTIVITIES

SYS-ORBIT-PROTEC_418: The organization **aims for state-of-the-art encryption and current best encryption practices.** The organization must be **able to adapt to technological changes in cryptography**. Depending on the orbital system's needs, it may be necessary to be able to adapt to future disruptive technologies such as quantum science and post-quantum cryptography (PQC) algorithms.

2.7 I PHYSICAL SECURITY

Physical security is generally accepted as all of the security measures designed to limit access to authorised persons and to protect against physical and material damage.

2.7.1 I IMPLEMENTING PHYSICAL OR REMOTE ACCESS CONTROL PROCEDURES

SYS-ORBIT-PHY_500: The organization identifies the physical access points of the orbital system installations and sites. This includes access to network sockets in places open to the public, such as meeting rooms, reception, corridors, etc..

SYS-ORBIT-PHY_501: The organization **defines and maps sensitive areas** to adapt physical and remote access controls according to the sensitivity of the activity carried out there. Premises where strategic research or production activities are carried out are given protected area status and are classified as an RRZ, to which access is controlled to protect the nation's scientific and technical potential (PPST) and counter capture or misappropriation attempts.

SYS-ORBIT-PHY_502: The organization stringently **monitors its sites' entrances and exits according to their sensitivity and keeps a register of persons accessing the site.**

SYS-ORBIT-PHY_503: The organization controls physical access to servers, technical rooms, and sensitive areas by **implementing accountability measures** (such as installing secure locks or badge readers). Access to the network sockets in areas with foot traffic must also be disabled or restricted. Controlling access also implies **managing physical keys and key cards**. Depending on the organization's needs, the measures to physically protect different zones can be adapted..

LAUNCH MONITORING OF ARIANE6'S FIRST FLIGHT VA262 FM1 FROM JUPITER 2 ROOM, CONTROL CENTER (CDC) OF THE FRENCH GUYANA SPACE CENTER (CSG), JULY 09, 2024

SYS-ORBIT-PHY_504: The organization regularly reviews the accounts and related rights, such as individuals' access rights, to avoid unauthorized access. In particular, the organization ensures that access rights have been deleted for personnel who have left the organization..

SYS-ORBIT-PHY_505: Depending on the level of risk, **the organization can foresee cases where its personnel is forced to work under duress** (hostage situation, terrorism). This can involve creating special passwords alerting to work under duress.

2.7.2 I TECHNICAL SITE MANAGEMENT

SYS-ORBIT-PHY_506: The organization takes a **global approach to security**, taking into account interactions with the elements so that **the site's technical constraints** (physical intrusion, fire, air conditioning, air filtration, humidity) **have a minimal direct or indirect effect** on the security of the orbital system's information system.

2.7.3 I SECURITY APPROACH DURING THE DIFFERENT PHASES OF THE ORBITAL SYSTEM

SYS-ORBIT-PHY_507: The organization ensures that the **orbital system's information system is secure**

during each life cycle phase, especially during the AIT, transportation, and launch phases, which can be considered high-risk phases.

SYS-ORBIT-PHY_508: The organization ensures that **sensitive components are physically stored securely** to prevent any intervention by unauthorized entities..

2.7.4 INDUSTRIAL SECURITY AND IT/OT INTERDEPENDENCY

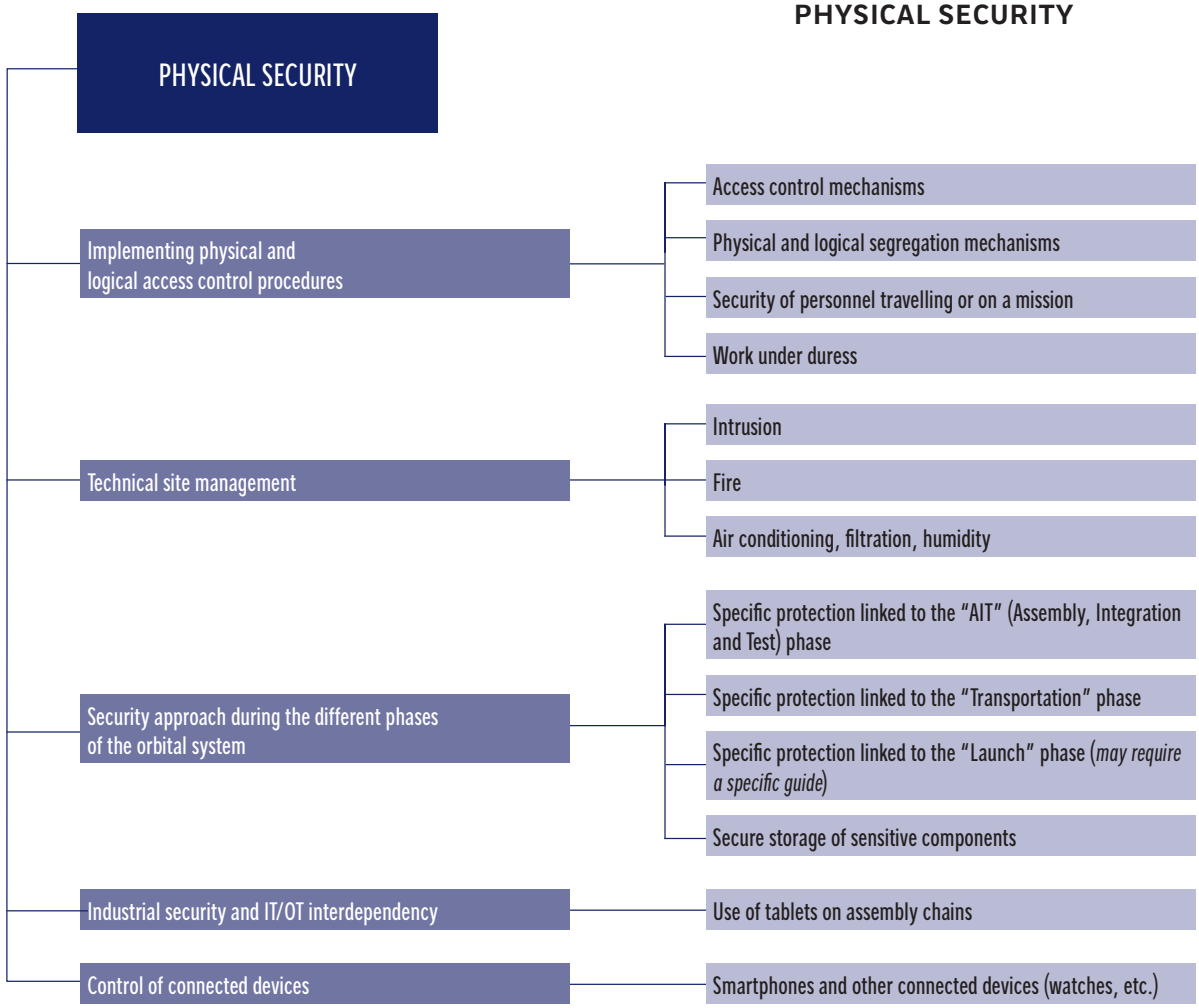
SYS-ORBIT-PHY_509: The organization **ensures that industrial systems (called OT and including tools to control and command technical installations, SCADA, etc.) are separated from conventional information systems (IT).** It ensures, in particular, that IT systems cannot impair the proper functioning of industrial systems.ment elle s'assure que les systèmes d'information IT ne puissent pas perturber le bon fonctionnement des systèmes industriels.

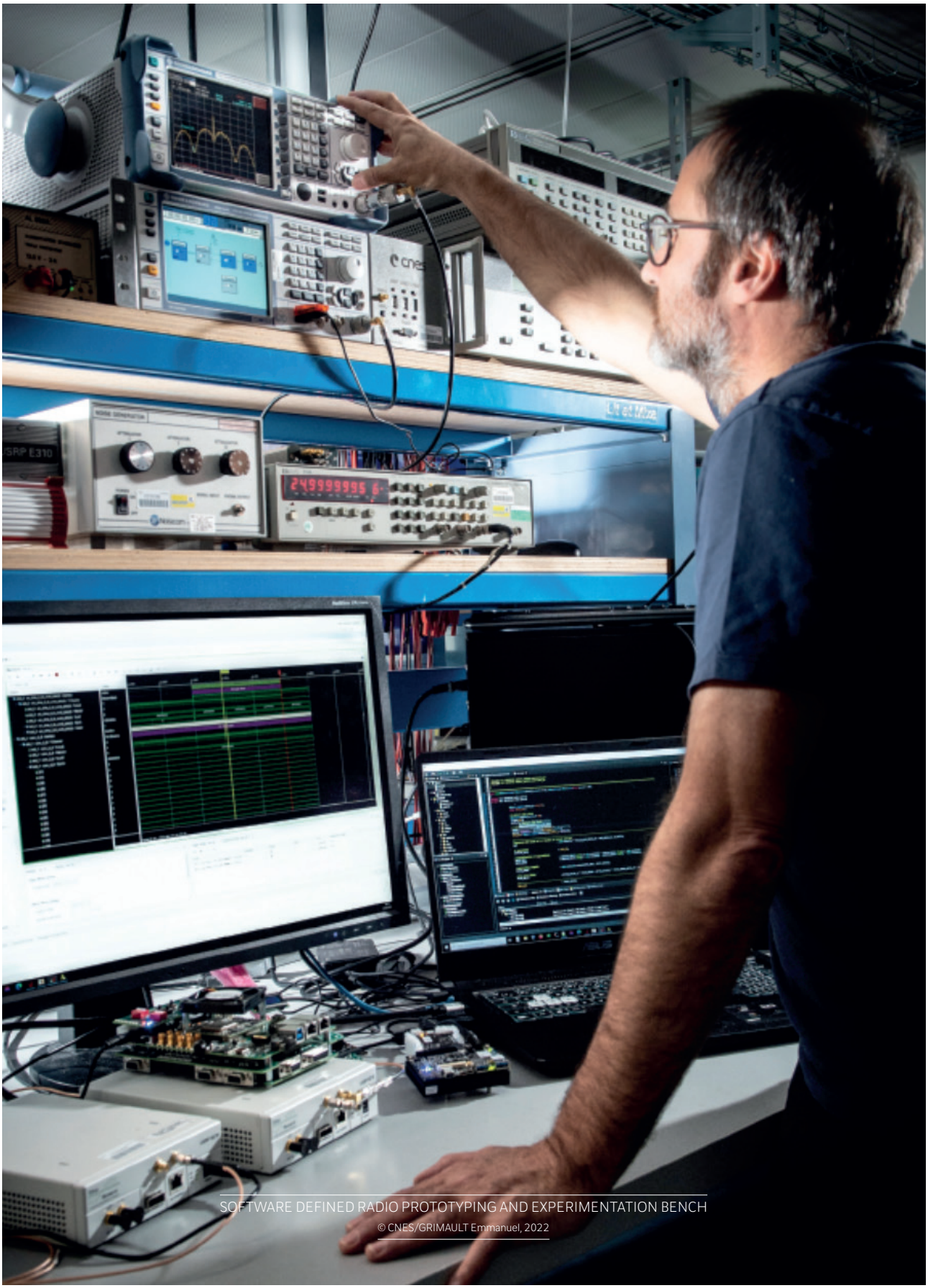
2.7.5 CONTROL OF CONNECTED DEVICES

SYS-ORBIT-PHY_510: The organization ensures that only duly authorized mobile devices can be connected to IT or OT systems and that **they cannot directly or indirectly interfere with or impair the industrial information systems or the orbital system's information systems** in general.

FIGURE 7:

THEMES ASSOCIATED WITH PHYSICAL SECURITY





SOFTWARE DEFINED RADIO PROTOTYPING AND EXPERIMENTATION BENCH

2.8 | DETECTION AND LOGGING MECHANISMS

Detection is used to identify, as soon as possible, behaviour resembling a cyberattack or an attempted attack and respond as quickly as possible. Logging is used to compile a set of information and record access and actions to be able to provide information if an incident is investigated.

2.8.1 | CHOOSING AND IMPLEMENTING DETECTION TOOLS

SYS-ORBIT-DETECT_600: The organization sets up an IDPS to detect cyber threats and prevent intrusions.

SYS-ORBIT-DETECT_601: The organization sets up a SIEM to collect, analyze, correlate, and respond to security events to identify threats as soon as possible and to minimize efforts to filter false positives.

2.8.2 | LOGGING, LOG MANAGEMENT AND CORRELATION

SYS-ORBIT-DETECT_602: The organization sets up mechanisms for logging events using log files. The logs recorded may be correlated with the use of different information bundles (e.g., physical security and digital security) to identify and understand potential security incidents.

2.8.3 | CYBER THREAT INTELLIGENCE (CTI) ACTIVITY AND ANTICIPATING THE TECHNICAL THREAT

SYS-ORBIT-DETECT_603: The organization considers CTI (Cyber Threat Intelligence) activities to acquire technical indicators of threat level changes and to be able to adapt its security based on the activities observed. This monitoring can be carried out by using a SOC (Security Operation Centre) or specific sensors. Depending on the risk analysis results, the organization launches an **adapted response and engages means to mitigate the risk**. In the future, artificial intelligence may be considered as a means of improving the quality of detection tools. CTI activities may require calling on threat specialists and threat indicators.

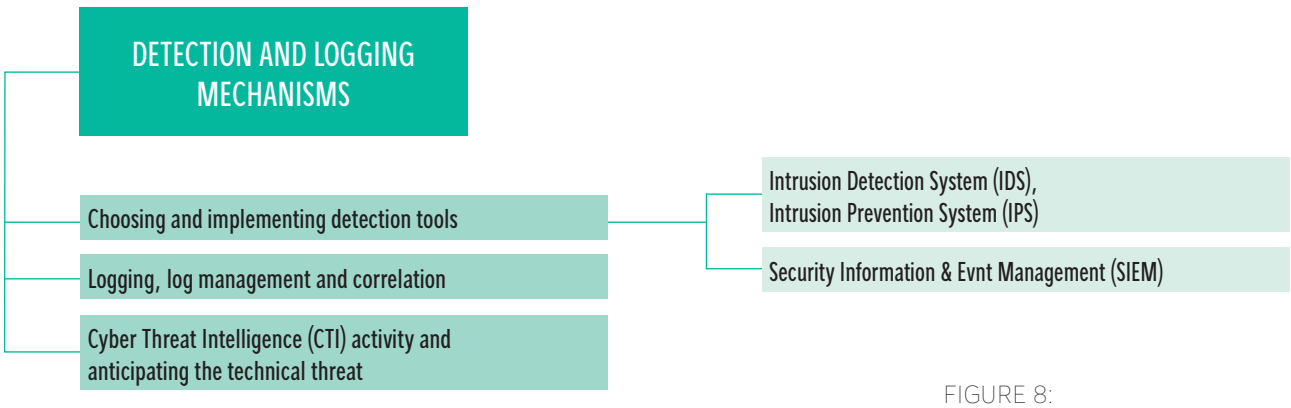


FIGURE 8:

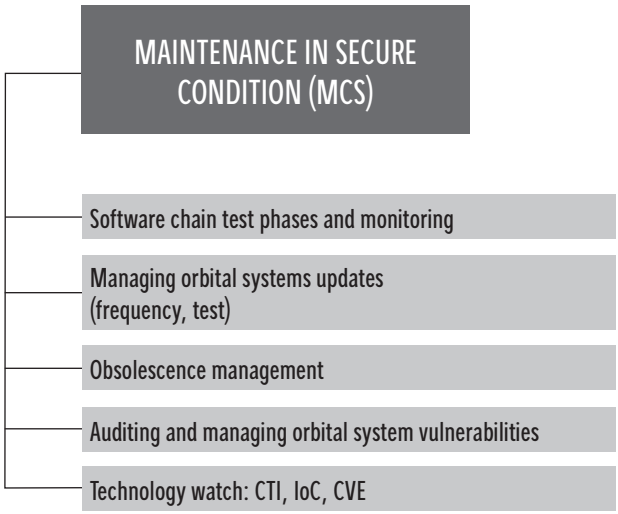
THEMES ASSOCIATED WITH DETECTION AND LOGGING MECHANISMS

2.9 | MAINTENANCE IN SECURE CONDITION (MCS)

The security of orbital systems is a process that must be maintained over time throughout the life cycle of the orbital system. Maintenance in Secure Condition, or MSC, enables the orbital system to be kept in an optimal state of security by taking into account threat developments and new vulnerabilities discovered on the orbital system.

FIGURE 9:

THEMES ASSOCIATED WITH MAINTENANCE IN SECURE CONDITION



2.9.1 | SOFTWARE CHAIN TEST PHASES AND MONITORING

SYS-ORBIT-MCS_700: The organization defines **its Maintenance in Secure Condition (MSC) and Maintenance in Operational Condition strategies.**

SYS-ORBIT-MCS_701: The organization pays **special attention to COTS-type software and implements processes to control the software chain through traceability mechanisms** (using a software nomenclature or an SBOM-type approach). The organization also pays particular attention to the possibility of trapping from open-access software.

SYS-ORBIT-MCS_702: When software is delivered from a supplier, the organization ensures that its supplier **signs its deliveries and provides mechanisms to check the integrity** of the code or software supplied.

2.9.2 | MANAGING ORBITAL SYSTEMS UPDATES

SYS-ORBIT-MCS_703: Depending on needs, the organization can develop and implement a **digital duplicate** of the orbital system **before updates are carried** out during the operation phase. The aim is to prevent technical contingencies that may occur after an update.

SYS-ORBIT-MCS_704: Based on the actions identified in the risk analysis, the organization **carries out non-regression tests** on functionalities that an update may impact. It **maintains restore states** in case the update causes a malfunction or regression.

2.9.3 | OBSOLESCENCE MANAGEMENT

SYS-ORBIT-MCS_ 705: The organization anticipates the hardware and software obsolescence of the orbital system's components. Regarding software, the organization can find out when a software's maintenance will end. Regarding hardware, the organization can anticipate obsolescence by providing spare parts. Spare parts can be used to anticipate when a piece of equipment's production is ended by a manufacturer or a main system manufacturer.

SYS-ORBIT-MCS_706: The organization **anticipates the end of life** (EOL) **or end of support** (EOS) phases of any part or all of the orbital system.

The EOL or EOS phases should be anticipated by, for example, considering deleting sensitive data, revoking certificates, or deleting flight keys before placement in the graveyard orbit. Depending on needs, it may be necessary to foresee launching a project to guarantee the continuity of the mission.

2.9.4 | AUDITING AND MANAGING VULNERABILITIES

SYS-ORBIT-MCS_707: The organization conducts intrusion tests and vulnerability scans, the type and frequency of which are determined by the risk analysis. Depending on needs, the organization makes corrections (configuration changes, **updates, patch applications, etc.).**

SYS-ORBIT-MCS_708: The organization **implements measures to protect the test results** to prevent them from being used by ill-intentioned parties.

SYS-ORBIT-MCS_709: The organization **produces an impact analysis of the vulnerabilities** detected, taking into account its level of exposure to the threats, to determine the appropriate action. Depending on the ISSP associated with the information system analyzed, **the organization applies the relevant fixes and patches** to stop these vulnerabilities from being exploited by ill-intentioned parties. Certain operational contexts of an orbital system are not conducive to fixes or patches.

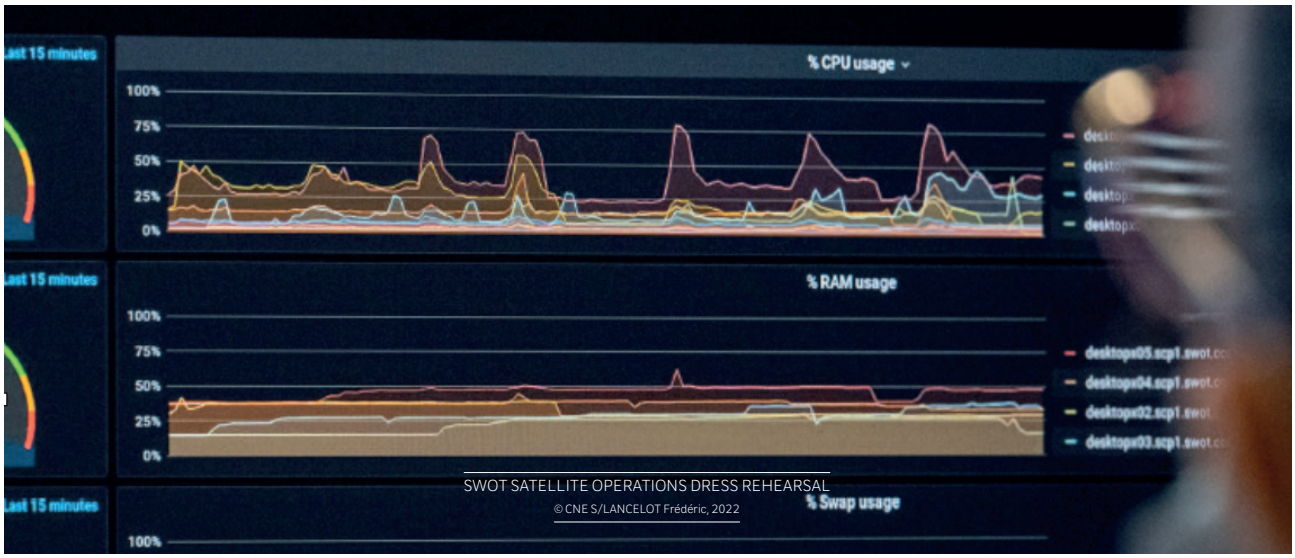
SYS-ORBIT-MCS_710: The organization protects the audit results and the vulnerabilities to prevent the information system from being compromised in the event of the data being stolen.

SYS-ORBIT-MCS_711: When applying fixes and patches, the organization ensures that it does not introduce any regression into the system by performing **non-regression tests.**

2.9.5 | TECHNOLOGY WATCH

SYS-ORBIT-MCS_712: The organization monitors vulnerabilities (IoC, CVE) to keep the various software or hardware components up to date, as well as the cyber detection sensors (in particular the antiviral database).

SYS-ORBIT-MCS_713: The organization adopts tools and frameworks helping it to share IoC-type technical indicators (using, for example, frameworks such as OpenCTI and protocols such as STIX/TAXII, etc.).



SWOT SATELLITE OPERATIONS DRESS REHEARSAL
© CNE S/LANCELOT Frédéric, 2022

2.10 | SECURITY IMPROVEMENTS

Securing orbital systems requires installing a proactive defense throughout their life cycle. Continuous security improvements are based on zero-trust approaches consisting of applying successive layers of security without implicitly trusting a service or component, even when internal to the system.

2.10.1 | IN-DEPTH KNOWLEDGE OF THE SYSTEM AND CREATION OF DIFFERENT LEVELS OF PROTECTION

SYS-ORBIT-AMELI_800: The **deep defense** approach allows the organization **to identify mechanisms to slow down any attack or deter attackers by making it harder to carry out an attack**. Inspired by military methods, this approach consists of slowing down an enemy by setting up successive obstacles to deter an attacker due to the efforts needed to carry out a cyberattack.

SYS-ORBIT-AMELI_801: The **zero-trust** approach allows the organization to apply several levels of protection to all segments of its orbital system **to avoid any implicit trust**. In other words, the trustworthiness of a person or component's identity must always be verified by performing regular, dynamic, granular checks. One example could be to set up mutual authentication between each system component.

SYS-ORBIT-AMELI_802: **Using a chain of trust** based on **a root of trust** (e.g., secure boot) allows the organization to secure the orbital system information systems as early as possible, from the initialization phase.

2.10.2 | SECURE DEVELOPMENT

SYS-ORBIT-AMELI_803: The organization **seeks to integrate security into its development process in an agile way** using the "devsecops" approach. .

SYS-ORBIT-AMELI_804: The organization **complies with and encourages the use of coding rules** to limit potential software failures and exploitation. It must be possible for the organization to regularly check that the coding rules are applied..

SYS-ORBIT-AMELI_805: **The organization ensures that its software forges are secured and that configuration is managed** to protect the confidentiality or integrity of its source code.

SYS-ORBIT-AMELI_806: During the design or maintenance phases, the organization carries out software tests or coordinates them with its suppliers as required. There may be different types of security tests, such as **Dynamic Application Security Testing** (DAST) or **Static Application Security Testing** (SAST).

2.10.3 | HARDENING AND REDUNDANCY

SYS-ORBIT-AMELI_807: In accordance with the risk analysis, **the organization guarantees the redundancy of the orbital system's critical systems or subsystems** to avoid single points of failure..

SYS-ORBIT-AMELI_808: In accordance with the risk analysis, **the organization partitions and creates a spatial and temporal separation** between the different parts of the orbital system's information system.

SYS-ORBIT-AMELI_809: **The organization applies filtering rules to the orbital system's information system** to ensure that only strictly necessary flows are authorized.

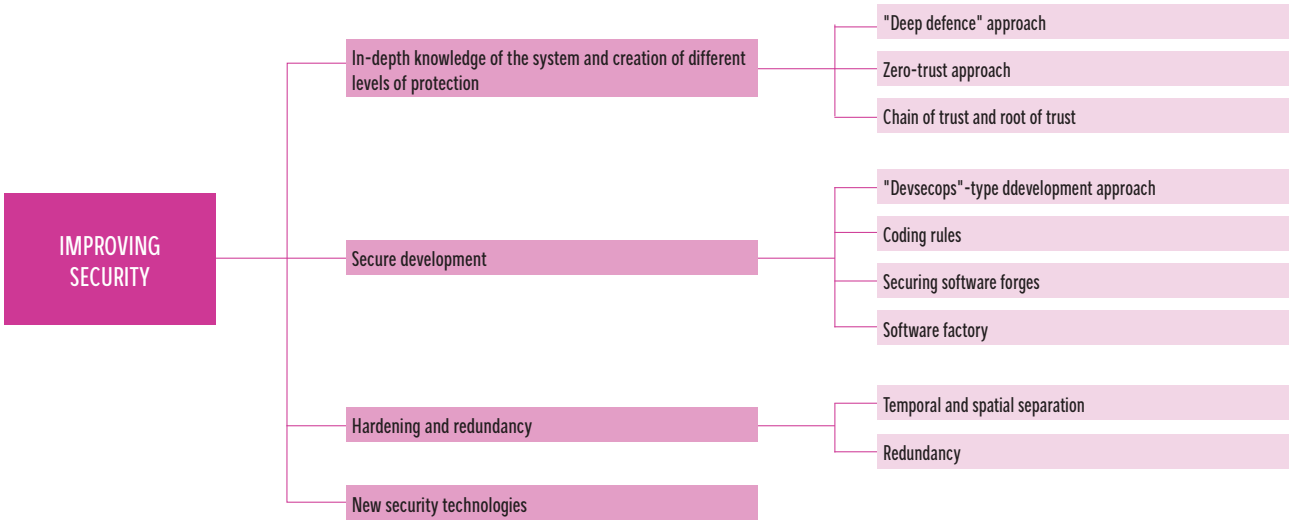
SYS-ORBIT-AMELI_810: In accordance with the risk analysis, **the organization considers implementing physical or logical hardening techniques to reduce the system's attack surface.**

2.10.4 I NEW SECURITY TECHNOLOGIES

SYS-ORBIT-AMELI_811: Whenever possible, **the organization considers new cybersecurity technologies** to protect its orbital system, particularly technologies based on the system's dynamics (reconfiguration in orbit, software-defined technologies like SDR or SDS). ▮

FIGURE 10:

THEMES ASSOCIATED WITH SECURITY IMPROVEMENTS



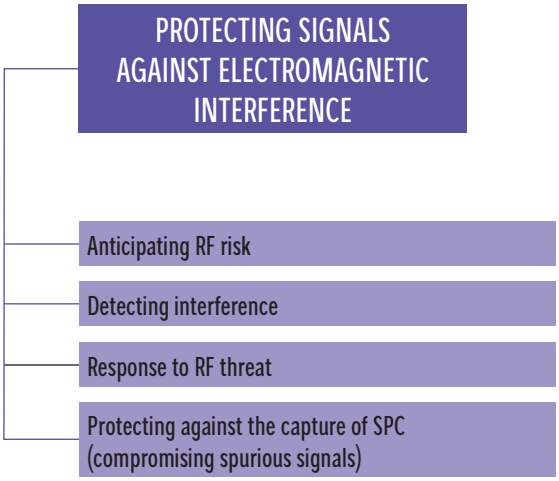
MICROCARB SATELLITE IN A CLEAN ROOM AT CNES' TOULOUSE SPACE CENTER
© CNES/GRIMAULT Emmanuel, 2024

2.11 | PROTECTING THE SIGNAL FROM ELECTROMAGNETIC INTERFERENCE

Electromagnetic interference means disturbances generated by an external source that can affect the communications and services provided by an electrical circuit, by degrading its performance or preventing its proper functioning. These attacks have been on the rise over the last few years and are accentuated by geopolitical tensions (many cases of jamming or spoofing). This type of threat can impact orbital systems.

FIGURE 11:

THEMES ASSOCIATED WITH PROTECTING SIGNALS AGAINST ELECTROMAGNETIC INTERFERENCE



Although it is often complicated and costly to take this threat into account, it is important to look at the system's ability to evolve in an environment increasingly subject to such attacks.

The radiofrequency risk on orbital system signals, whether onboard-ground, ground-onboard, or onboard-onboard, requires organizations to anticipate the related impacts and design mechanisms to improve robustness or resilience. Depending on the mission, the orbits used, and the specificities of the orbital system, the operator can choose the most applicable best practices..

The risk associated with compromising spurious signals is also referred to as a TEMPEST threat. A TEMPEST threat does not only concern radiofrequency (but can also target an acoustic, visual, or vibratory element, etc.). In this first issue, we will focus only on the radiofrequency aspect.

2.11.1 | ANTICIPATING RF RISK

SYS-ORBIT-SIGNAL_900: The organization carries out a **risk analysis** to identify the **security needs related** to the **risk of electromagnetic interference.** The organization identifies the different signals and data types according to the communication channels used and usage (nominal, backup, etc.). Depending on needs, the organization **implements a set of TRANSEC measures** (spectrum spreading, use of several frequencies, burst encoding, frequency hopping) for the signals concerned to respond to spoofing or jamming attacks in particular..

SYS-ORBIT-SIGNAL_901: Depending on the risk analysis results, **the organization may consider using backup systems and infrastructure, as well as alternative communication channels** (alternative antennas and frequencies, for example) to guarantee the continuity of communications in the event of interference.

2.11.2 I DETECTING INTERFERENCE

SYS-ORBIT-SIGNAL_902: Depending on the risk analysis results, t**he organization implements mechanisms to monitor the electromagnetic spectrum**, such as telemetry critical points, carrier lock status, or other RF parameters related to the signal.

SYS-ORBIT-SIGNAL_903: Depending on the risk analysis results and the resources available, the organization **can set up or use space situational awareness** (SSA) capabilities by identifying and tracking space objects to anticipate a threat in space.

2.11.3 I RESPONSE TO RF THREAT

SYS-ORBIT-SIGNAL_904: The organization **provides the frequencies or communications impacted by interference to the competent authorities** (CNES frequency bureau, MINARM, ANFR, ITU, etc.).

2.11.4 I PROTECTING AGAINST THE CAPTURE OF COMPROMISING SPURIOUS SIGNALS

SYS-ORBIT-SIGNAL_905: Depending on the results of the risk analysis, **the organization anticipates the risks of intercepting and exploiting Emanating Spurious Transmissions** on the orbital system information systems, such as those linked to the radiation from an electronic board or a screen, by, for example, taking TEMPEST measures (hardening the orbital system, auditing ground buildings, using a Faraday shield-protected enclosure on the ground for keying, etc.). These measures may be implemented when processing secrets in the ground or space segments and during keying. ▮

INAUGURATION OF A NEW STC TRACKING STATION AT ISSUS-AUSSAGUEL, FRANCE.
© CNES/GNAWAN, 2023


cnes

Version 1 **- Mars 2025**

DCS-2024.0004634

cyber4space@cnes.fr

https://cnes.fr/entreprises/centre-cyber-spatiale

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

SUIVI DU LANCEMENT DU PREMIER VOL VA262 FM1 ARIANE 6 EN SALLE JUPITER 2, CENTRE DE CONTRÔLE (CDC) DU CENTRE SPATIAL GUYANAIS (CSG), LE 09 JUILLET 2024