ESA Contract N° 4000121302/17/NL/FE

Innovative Security Concepts, Mechanisms and Architectures for Future Space Missions
-
ESA Study Executive Summary

Written by	***Responsibility***
THALES Study Team	TAS & TCS Teams
Verified by	
F. PERRIN	TAS Cyber Security Expert & Study Technical Manager
Approved by	
W. HALIMI	TAS Project Manager

Approval evidence is kept within the documentation management system.

CHANGE RECORDS

ISSUE	DATE	§ CHANGE RECORDS	AUTHOR
01	21/05/2019	First Issue	THALES Team
02	06/06/2019	New Issue taking into ESA review and comments.	THALES Team
03	21/06/2019	New Issue : update of document footer for OPEN distribution	THALES Team

1. INTRODUCTION

1.1. SCOPE AND PURPOSE

Present document is the Executive Summary of ESA R&T Study

- Innovative Security Concepts, Mechanisms and Architectures for Future Space Missions.
- ESA Contract N° 4000121302/17/NL/FE.

The main objective of this document is describe the main findings of ESA study.

1.2. STRUCTURE OF THE DOCUMENT

Present document is structured as follows:

- §2: Future Space Missions Architectures
- §3: Future Space Missions Risks Analysis
- §4: Review and Selection of Security Technics
- §5: Security Architecture Portfolio
- §6: Recommendations for future Activities
- §7 : Conclusion

1.3. REFERENCES

All references are defined in the study final Report

DR#	Title	Issue	Reference
DR01	ESA ITT 8751 ; Innovative Security Concepts, Mechanisms and Architectures for Future Space Missions Study Final Report	3.0	0003-0002457296

1.4. ACRONYMS

All acronyms are defined in the study Final Report addressed in previous section.

2. FUTURE SPACE MISSIONS ARCHITECTURES (WP1210)

2.1. OBSERVATION MISSION

The reference Observation mission scenario considered consisted in flying in tandem in Low Earth orbits two remote sensing satellites equipped with different sensors, able to download their acquisitions to the ground

- Through a geostationary relay satellite.
- Or directly by using proprietary ground stations or others belonging to the customers.

The space segment is composed of two satellites, one with a visible optical sensor on-board, the other with on-board a radar sensor and a low-resolution optical sensor for cloud detection.

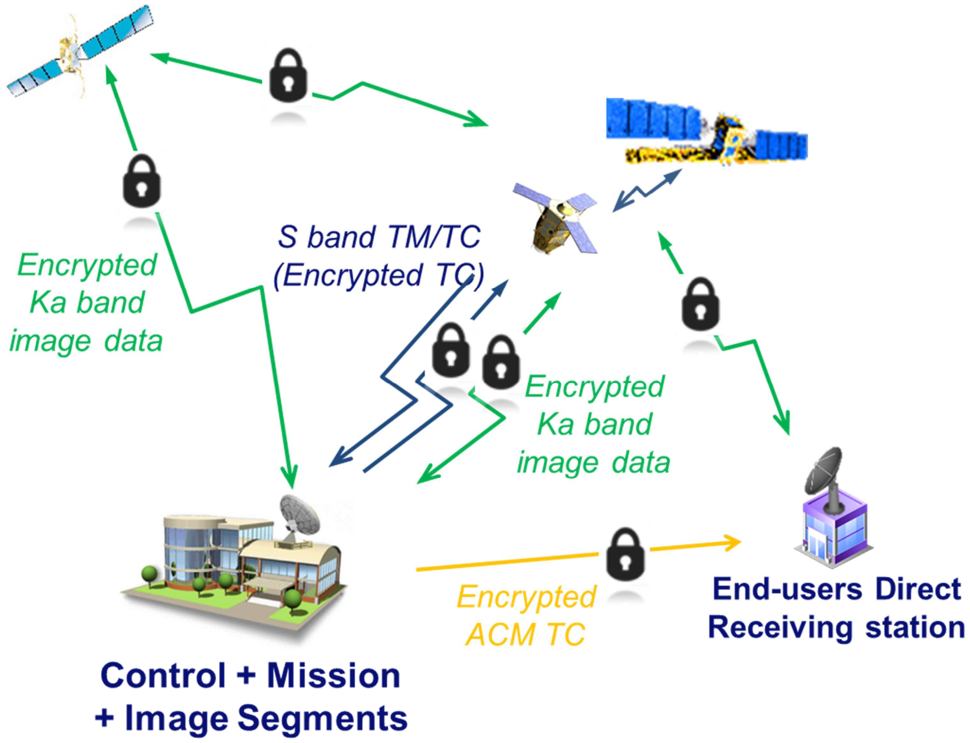

Encrypted Ka band image data
S band TM/TC (Encrypted TC)
Encrypted Ka band image data
Encrypted ACM TC
End-users Direct Receiving station
Control + Mission + Image Segments

Figure 2-1: Global architecture for the Observation mission scenario

The Ground Segment composed of

- A <u>Control Ground Segment</u> (CGS) performing the monitoring & control of the satellites
- A <u>Mission Ground Segment</u> (MGS) for Mission Planning and image processing.
- A Dual Band Station (DBS) able to receive the image data in Ka-Band and send telecommand and receive house-keeping telemetry in S band.
- A data relay Segment (telecommunication geostationary satellite and its ground segment),
- A direct receiving station (DRS) owned by the end users equipped to receive Image Telemetry (ITM) in Ka band and send ACM Telecommands (TC) in S band.

2.2. NAVIGATION MISSION

Two scenarios are considered for Navigation mission

- MEO Collect Solution for Machine to Machine (M2M) fast growing market
- Alternative LEO Collect Solution using LEO & nano satellites

⇒ The benefit of that solution is to allow to address the two major issues arising when it is question of collecting M2M signals by satellites:

⇒ The first one is the link budget.

⇒ The second one even more complex refers to the strong probability of signals collisions (intra-system interference).

The MEO Collect Solution Architecture relies on :

- A space segment based on Galileo constellation with new repeater payload on next generation satellites for the forward link.
- A ground segment based on a M2M mission control center interfacing with:

⇒ Galileo GMS (Ground Mission System) for the return link through an evolution of Return-Link Service Provider (RLSP) component,

⇒ A dedicated ground stations network for the forward link.

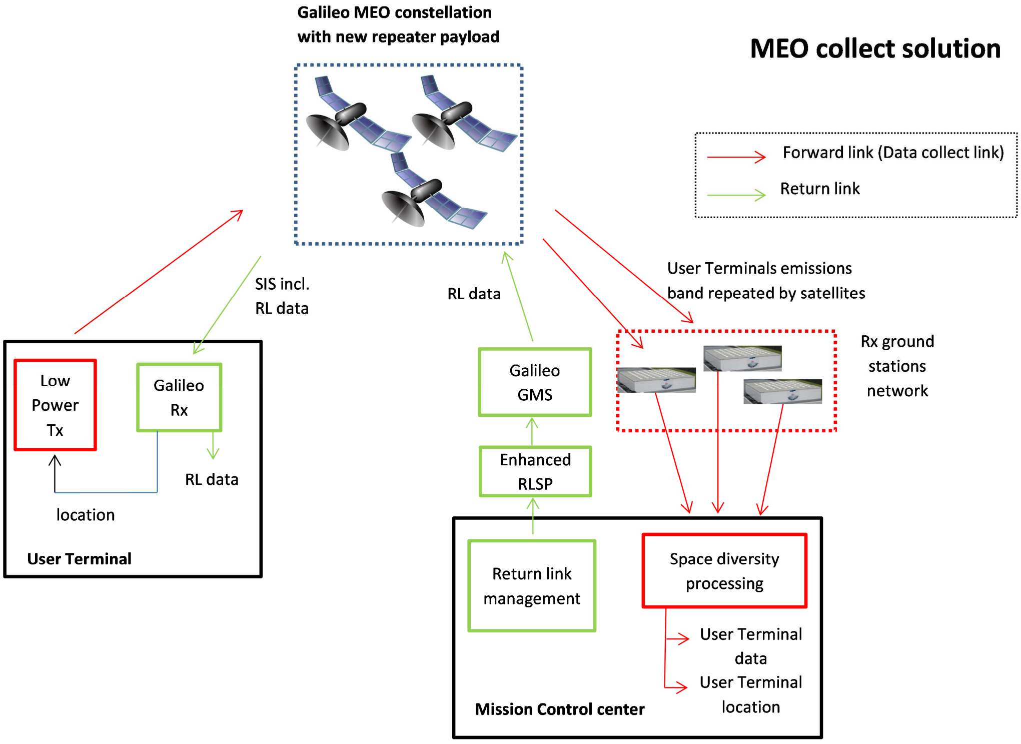


Figure 2-2: MEO solution system architecture

Alternative LEO Collect Solution Architecture : detailed in DR01

2.3. TELECOMMUNICATION MISSION

Two reference scenarios are considered for Telecom mission

- Scenario 1: GEO Telecom satellite with Hosted payloads (HPL).
- Scenario 2: LEO Telecom Constellation with inter-satellite link (satellite network system).

2.3.1. Scenario 1: GEO Telecom VHTS Satellite with Hosted Payload (HPL)

General Architecture is illustrated in Figure 2-3.

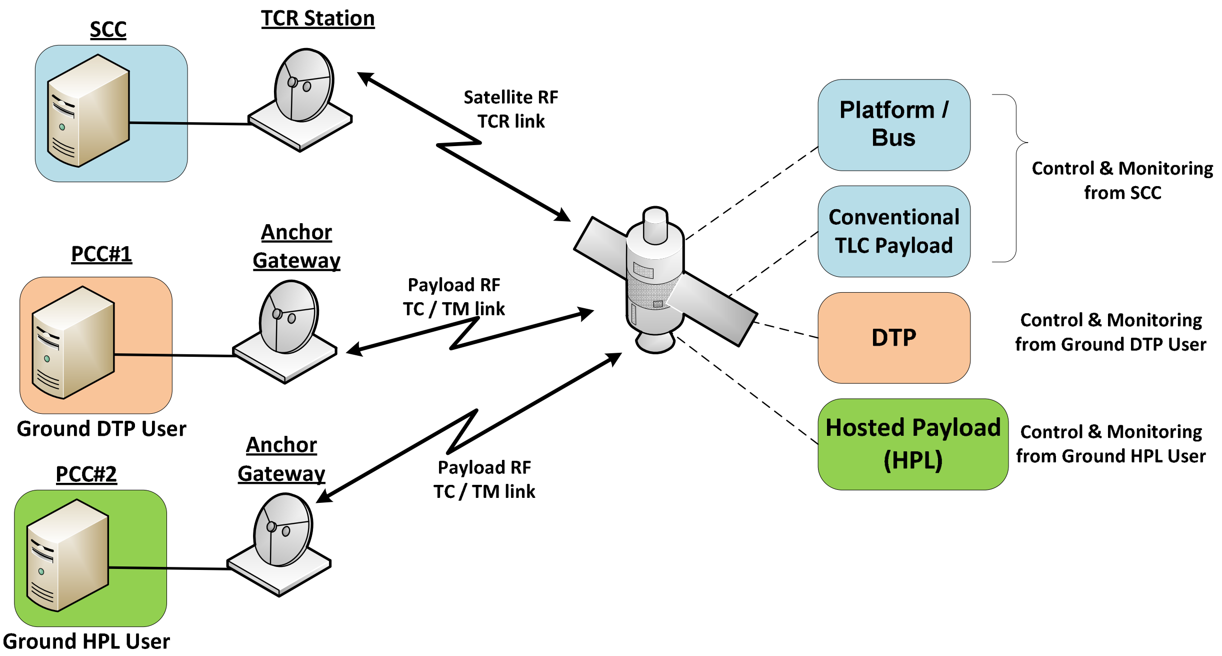


Figure 2-3: Telecom Scenario 1: GEO VHTS Satellite with Hosted Payload (HPL)

The Satellite Operator accesses to satellite via SCC and classical TCR RF link in order to control & monitor the bus / platform and the commercial (neither VHTS nor HPL) payload.

The Ground DTP User accesses to satellite via dedicated PCC (Payload Control Centre) and Payload TC/TM RF link in order to control & monitor the DTP for VHTS mission.

The Ground HPL User accesses to satellite via dedicated PCC (Payload Control Centre) and Payload TC/TM RF link in order to control & monitor the Hosted Payload

2.3.2. Scenario 2: LEO Satellite Constellation with ISL (Satellite Network)

Use Case is illustrated in and involves

- Two satellite monitoring and control links : primary link (nominal link used during OOC phase) and secondary link (direct link use during IOT and emergency)
- An OBP (on-board processor) as main payload computer
- Satellite data network with TC/TM flows routing via ISL

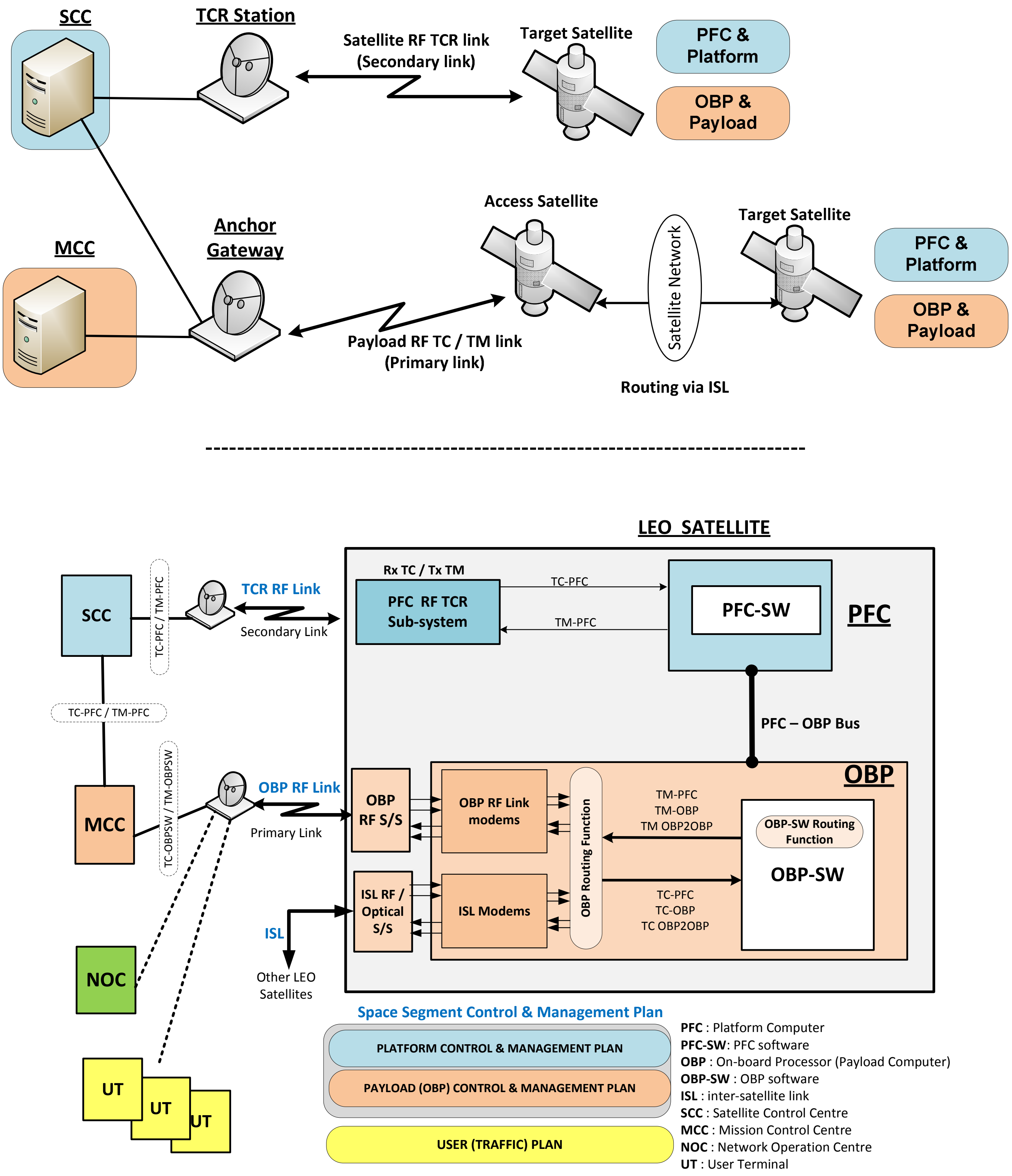


Figure 2-4: Telecom Scenario 2: LEO satellites constellation – System Architecture

3. FUTURE SPACE MISSIONS RISKS ANALYSIS (WP1220)

Risk Analysis performed on target future missions as addressed by task WP1210 relies on ISO 27005 security risk management process.

Major risks identified for Observation , Navigation & Telecom Missions are given in following tables

Risk ID	Risk Description	Initial risk level (without measures)	+ Existing Technical measures only	+ Existing and proposed Technical measures only	+ Technical & Operational & Site measures
obs_005	Modification of input data used for computing ACM commands (ACMC-SFW) by an attacker. ACM settings are incorrect and cause potential disruptions.	4- Critical	4- Critical	3 - Major	1 - Minor
obs_015	Insider stole DRS ACM keys (KDRS-SFW). An attacker could send and have a look on ACM commands generated by the DRS.	4- Critical	3 - Major	3 - Major	1 - Minor
obs_032	An attacker replays nebulosity map transfer messages. Nebulosity map is a wrong one and the new computed plan is not the optimum one.	4- Critical	3 - Major	3 - Major	1 - Minor
obs_003	An attacker modifies the image taken by the radar satellite either by modifying the image itself (NEBP-SFW) or by creating an illusion (NEBC-SFW)). No capture seems possible regarding the nebulosity map. Delay to take picture.	3 - Major	3 - Major	3 - Major	1 - Minor
obs_025	An attacker from ground (antenna) or space (nano satellite) jams ISL (Radar <-> Optical) traffic. Nebulosity map cannot be used any more.	3 - Major	3 - Major	3 - Major	1 - Minor

Table 3-1: Observation Mission Major Risks

Risk ID	Risk Description	Initial risk level (without measures)	+ Existing Technical measures only	+ Existing and proposed Technical measures only	+ Technical & Operational & Site measures
SCEN_010	Processing Center is attacked physically (fire, bombs, ...) by an attacker. Services are no more available	4- Critical	4- Critical	4- Critical	1 - Minor
SCEN_008	1 Antenna Rx Ground station is physically attacked (Antenna, Buildings, Rooms, Servers...) by one or several attackers. Services are no more available for a specific area.	4- Critical	3 - Major	3 - Major	1 - Minor
SCEN_014	An attacker targets one or several Galileo satellites and jams their receivers. Services are disrupted.	4- Critical	3 - Major	3 - Major	1 - Minor
SCEN_015	An attacker targets Galileo satellite - Rx Ground network (GGRD-NET) and jams the antenna. Services are disrupted.	4- Critical	3 - Major	3 - Major	1 - Minor
SCEN_013	Commercial and SoL context: Interception of data on Rx Ground Stations network (RXGRD-NET), or between Rx Ground Stations and mission centers networks (GMIS-NET) by an attacker. No encryption on this network. Disclosure of potential Confidential data. Financial Loss.	3 - Major	3 - Major	3 - Major	1 - Minor

Risk ID	Risk Description	Initial risk level (without measures)	+ Existing Technical measures only	+ Existing and proposed Technical measures only	+ Technical & Operational & Site measures
SCEN_018	Commercial and SoL context: An attacker sends false signals to the Galileo satellites or to Rx ground station which are processed. End user received useless data. Bandwidth used. Financial loss.	3 - Major	3 - Major	3 - Major	1 - Minor

Table 3-2: Navigation Mission Major Risks

Risk ID	Risk Description	Initial risk level (without measures)	+ Existing Technical measures only	+ Existing and proposed Technical measures only	+ Technical & Operational & Site measures
HITS_013	An attacker spoofs HILINK module and provides false configuration. Service is disrupted for one or all Service Providers.	4- Critical	4- Critical	3 - Major	1 - Minor
HITS_023	An attacker exploits flaws in HILINK processing software and get control of the platform or of the other payload. Service is disrupted for all Service Providers.	4- Critical	4- Critical	3 - Major	1 - Minor
LEOTS_006	An attacker change behaviour of routing table (injecting false routing information, spoofing other satellite) to get messages (man in the middle), or to send messages to another ground segment. Disclosure of privacy messages and potentially military messages.	4- Critical	4- Critical	3 - Major	1 - Minor
LEOTS_007	An attacker change behaviour of routing table (RTSAT-SFW) (injecting false routing information, spoofing other satellite) to block messages. Service is disrupted.	4- Critical	4- Critical	3 - Major	1 - Minor
LEOTS_010	An attacker emits signal on inter satellite receiver (INSAT-HRD) and jammed traffic. Traffic is slowed down, due to rerouting traffic.	4- Critical	4- Critical	3 - Major	1 - Minor
LEOTS_012	An attacker emits a lot of routing messages to the router (RTSAT-SFW) and slowed down the traffic. Traffic is slowed down due to taking into account routing messages.	4- Critical	4- Critical	3 - Major	1 - Minor
LEOTS_017	An attacker replays messages between satellites directly from ground or from a malicious satellite. Traffic overload on inter satellite link (ISAT-NET). Service is slowed down. Bandwidth used.	4- Critical	4- Critical	3 - Major	1 - Minor
LEOTS_001	Data are corrupted by another source emitting some interference and changing integrity of the message (routing or users) on the inter satellite link (INSAT-NET). The message becomes invalid and is rejected. Service could be disrupted, waiting a new route to reach the destination.	3 - Major	3 - Major	3 - Major	1 - Minor
LEOTS_014	Through a malicious satellite, which sends false routing information to a legitimate satellite, an attacker got all messages (man in the middle) of the Telco network. Disclosure of privacy messages and potentially military messages.	3 - Major	3 - Major	3 - Major	1 - Minor
LEOTS_015	Solar activity is more intensive than expected and disturbs inter satellite transmissions (ISAT-NET). Service is disrupted.	3 - Major	3 - Major	3 - Major	1 - Minor

Table 3-3: Telecom Mission Major Risks

Synthesis

Figure 3-1 summarizes for each mission

- Number of scenario / risks identified
- Number of associated countermeasures

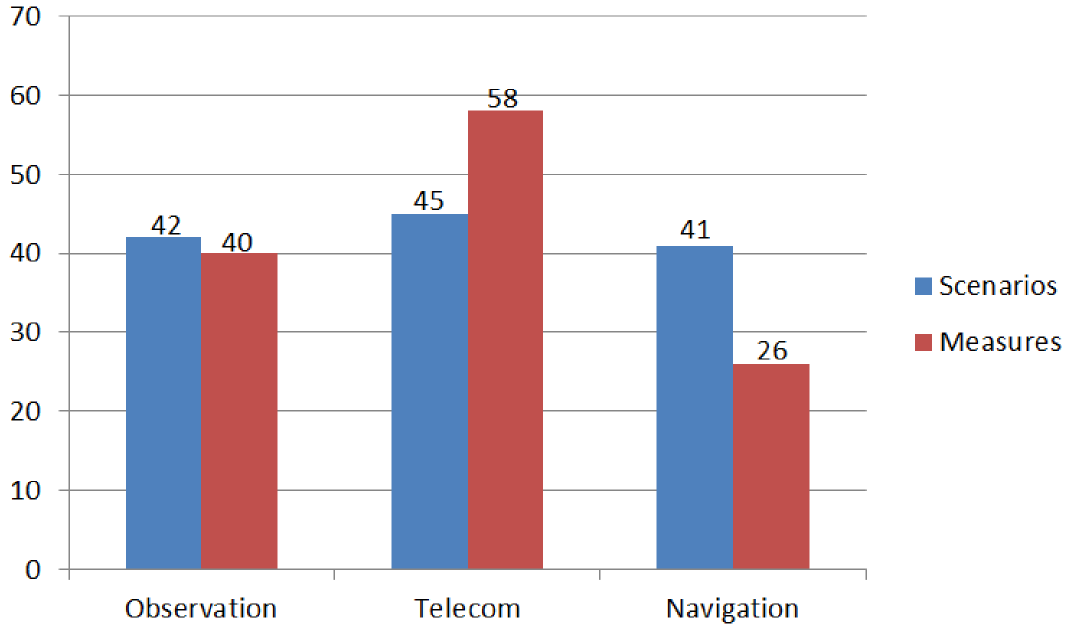


Figure 3-1: Number of Risks and Associated Countermeasures for each Mission

Figure 3-2 summarizes number and criticality of risks identified for each mission

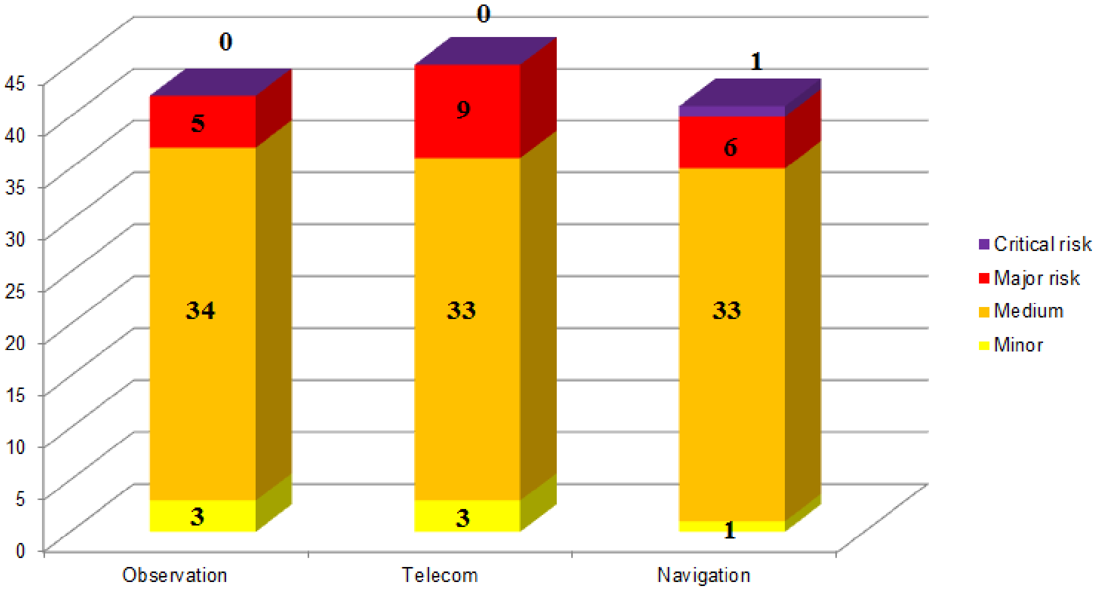


Figure 3-2: Number and criticality of risks identified for each mission

4. SECURITY CONCEPTS & TECHNICS REVIEW (WP1300)

Task WP1300 reviewed a set of security concepts techniques & technologies listed below.

4.1. POST-QUANTUM CRYPTOGRAPHY (PQC)

All public-key protocols actually deployed rely either:

- On the hardness of factoring (IFC: Integer Factorization Cryptography).
- Of the discrete logarithm problem (DLC: Discrete Logarithm Cryptography).
- Or on both.

Shor (Shor, 1994) showed that both problems are easy to solve with a quantum computer, which renders all current protocols virtually insecure in a quantum world.

The solution to this situation is to use alternative mathematical objects to build cryptographic protocols, which are all regrouped under the umbrella term of “**post-quantum cryptography (PQC)**”.

The 4 main existing PQC propositions reviewed in the frame of present study are the following

- Code-based cryptography.
- Lattice-based cryptography.
- Multivariate cryptography.
- Hash-based signatures.

4.2. PHYSICALLY UNCLONABLE FUNCTION (PUF)

The concept of Physically Unclonable Function (PUF) is based on the idea to use intrinsic random physical features to identify objects, systems or people. PUF idea is to exploit the random physical disorder or the manufacturing variations that occur in almost all physical systems.

- Those disorders cannot be fully controlled during the fabrication of the system and cannot be re-fabricating intentionally.
- Therefore, it is based on physical properties, it is unclonable and so it constitutes an **individual fingerprint of each system**.

Today, PUFs are usually implemented in integrated circuits and are typically used in applications with high security requirements.

- Authentication
- Post processing

4.3. QUANTUM CRYPTOGRAPHY (QKD)

The principles of quantum cryptography are based on one of the main laws of the quantum mechanics:

- The fact that a quantum state cannot be completely measured without perturbation (unclonable principle).

- It is not based on any mathematical assumption, and so is secure against quantum computing.

The main application is the Quantum Key Distribution (QKD)

- In a first step, two parties exchange quantum bits (qbits) over a quantum channel.
- Then classical exchanges on a non-quantum channel allow them to extract a common secret and to verify than an attacker has not been able to gain information on this secret.
- It may also include an authentication step.

4.4. LIGHTWEIGHT CRYPTOGRAPHY

Lightweight cryptography is a subfield of cryptography that aims to provide solutions tailored for resource-constrained devices

- Consumption, gate area (hardware), code-size (software)…

Applications

- Target Devices
  - ⇒ Embedded systems, RFID, Sensor networks.
  - ⇒ For high security (random generation for masking against side-channel attacks).
- Different target algorithms
  - ⇒ Block ciphers.

4.5. PHYSICAL LAYER SECURITY (PHYSEC)

PHYSEC techniques relies on following principle

1- Complex wave propagation + unpredictable (fine) scattering characteristics; as consequence:

- The fine structure of signals at B and A cannot neither be recovered nor predicted by Eve.
- The same applies for receiving noise of B and A.

2- Propagation Reciprocity (when Time Division Duplex radio protocol and stationary propagation during channel extraction); as consequence:

- A et B share the same propagation. Random.

Application cover the following

- Secrecy Coding
- Secret Key Generation (SKG)

4.6. KEY GENERATION MANAGEMENT & DISTRIBUTION

Activity addressed following key management relevant techniques

- Conventional Cryptography (SKI / PKI) – Key Generation

- Conventional Cryptography – Key Management
- Conventional Cryptography – Key Distribution
- Quantum Cryptography – Key Distribution
- Post-Quantum Cryptography – Key Distribution

4.7. INTRUSION DETECTION / PROTECTION

Intrusion detection: process of monitoring the events occurring on network and analysing them for signs of possible incidents

IDS (Intrusion Detection System): automation of intrusion detection process.

IPS (Intrusion Protection System): IDS + capability for stopping incidents

- Also known as IDPS ((Intrusion Detection and Protection System).

NGIPS: Next-generation of IPS with features for example like application awareness, user control and integration with external threat intelligence sources

Satellite systems can take advantage of CTI by incorporating feeds into the existing infrastructure including NGIPS and Security Information and Event Management (SIEM)

In the SOC of satellite system, in the backend, a cyber Threat Intelligence Platform (CTIP) can be deployed with a connection to the SIEM

4.8. PENETRATION TESTING (PT)

Process enabling security tests upon a network, a system or an application.

Find and exploit vulnerabilities by mimicking the behaviour of a normal user

- Do not make confusion with vulnerability scanning (only find).

Applicability to Space Missions

During a cyber-attack in Ground systems, decision-making cannot be reduced to technical decisions. Information prioritization and structuration are required to support the Ground operations for mitigation/remediation activities. Indeed, an assessment of the impacts on the services and/or security key performance indicators is required.

In the first part, vulnerabilities detected and exploited during pentesting campaigns shall be managed according to the configuration of Ground systems.

In the other parts, attack trees defined for each Feared Event can be computed in order to define whether a threat scenario has been covered or not.

PT techniques are addressed in Security Architecture Portfolio via

- Vulnerability Assessment Tool.
- Risks Analysis Tool.

4.9. SECURE PARTITIONING

Secure Partitioning addressed following:

- Containers and secure partitioning
- Differences with virtualization.
- Container as a service (CaaS)
- Management and orchestration.
- State of the art.
- Containerization usages

Containers as a lightweight technology to virtualize applications have recently been successful, particularly to manage applications in the cloud. Often, the management of clusters of containers becomes essential and the orchestration of the construction and deployment becomes a central problem.

Despite a lack of security maturity, the growing market of containerized applications may conduct vendors to develop solution to mitigate this issue.

Applicability to spatial missions

- Concept of logical multiple independent levels of security (MILS)
- Utilizario of PikeOS

4.10. SOFTWARE/DATA INTEGRITY IN VIRTUALIZED ENVIRONMENT

Cloud Computing as a disruptive technology

- impacts on Information Systems.

New model of IT management based on virtual machines allowing operating remotely applications, servers or infrastructures through a network, with flexibility, elasticity and a consumption monitoring.

To provide additional IT capacity, on an ad hoc basis, for unforeseen or planned needs. The protection of cloud computing must be taken into account by a specific security policy. Cloud Computing Top threats (CSA) detected and listed yearly by security experts.

Cloud computing has impacted the information systems by providing a shared virtual computing environment.

Security solutions deployed in traditional physical environments do not answer the security requirements for this new environment.

Vormetric transparent encryption offers seamless data protection wherever, with a transparent mode of data encryption for servers, applications and cloud.

It is important to observe that the security is a shared responsibility for the cloud providers and cloud consumers. Cloud consumers must ensure that cloud providers support the portability of data and the portability of system via the service level agreements.

4.11. HOMOMORPHIC ENCRYPTION

Objective

To perform meaningful computations on encrypted data.

Partially homomorphic encryption (PHE)

- Different possibilities (RSA is multiplicatively homomorphic).
- “Standard” problems (but subject to a quantum computer).

Applications

PHE: e-voting. Effective schemes.

FHE: potentially countless applications. But:

4.12. SOFTWARE BASED ANYTHING

The security of information cannot rely only on software-based protection.

- Unauthorized users can intend to boot the server with bootable media and with hacking tools to access, modify or copy critical data contained into the drive.

Trusted Platform Module (TPM) has been formalized and standardized in early 2000s under the Trusted Computing Group (TCG) ➔ concept of hardware-based security

- TPM can scan at boot for signs of change and attest that the information systems meet the security requirements before the execution of boot.
- TPM can check the integrity of the information systems during the process boot activating protection and detection mechanisms to perform in hardware, at pre-boot and then in secure boot process.

Study covered

- Concept of Root of Trust
- Secure Boot
- TPM (Trust Platform Module)
  - ⇒ New advanced threats have appeared and are undetectable by software-based tools like anti-virus. Thus, TPM is ready for prime time.
  - ⇒ The acquisition costs of the TPM standards-based technology become lower and the industry supports more widely the trusted computing standards. Indeed, TPM technology is more and more pervasive in the processors or chips used by the major device manufacturers.
  - ⇒ As a consequence, hardware security with the concept of TPM has reached a maturity and becomes a critical component in the security architecture.

4.13. MOVING TARGET DEFENSE

IT systems are built to operate in relatively static environments with traditional security approaches è static, deterministic and predictable target.

Moving Target Defense (MTD) is the concept of controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts.

Relevant Technics

- Dynamic Network Technics
- Dynamic Platform Technics
- Dynamic Runtime Environment Technics
- Dynamic Software Technics
- Dynamic Data Technics

The MTD technics have not been widely spread in commercial solutions, only few concepts (ASLR, IP hopping, Port knocking) have been implemented with known limitations.

4.14. SELECTION OF APPLICABLE SECURITY TECHNICS

The resulting security technics selected for detailed analysis during WP1300 are the following:

- Post Quantum cryptography.
- Physical layer security.
- Key Generation, Management and Distribution
- Extending securing technics generalized on generalist systems to ground segments
  - ⇒ Intrusion Detection,
  - ⇒ Penetration Testing,
  - ⇒ Software/data integrity on board software.
- Software-based anything
  - ⇒ TPM.
- SDLS Protocol.
- Spread spectrum.

5. SECURITY ARCHITECTURE PORTFOLIO (WP1420)

Task WP1420 allowed establishing a complete portfolio of security techniques

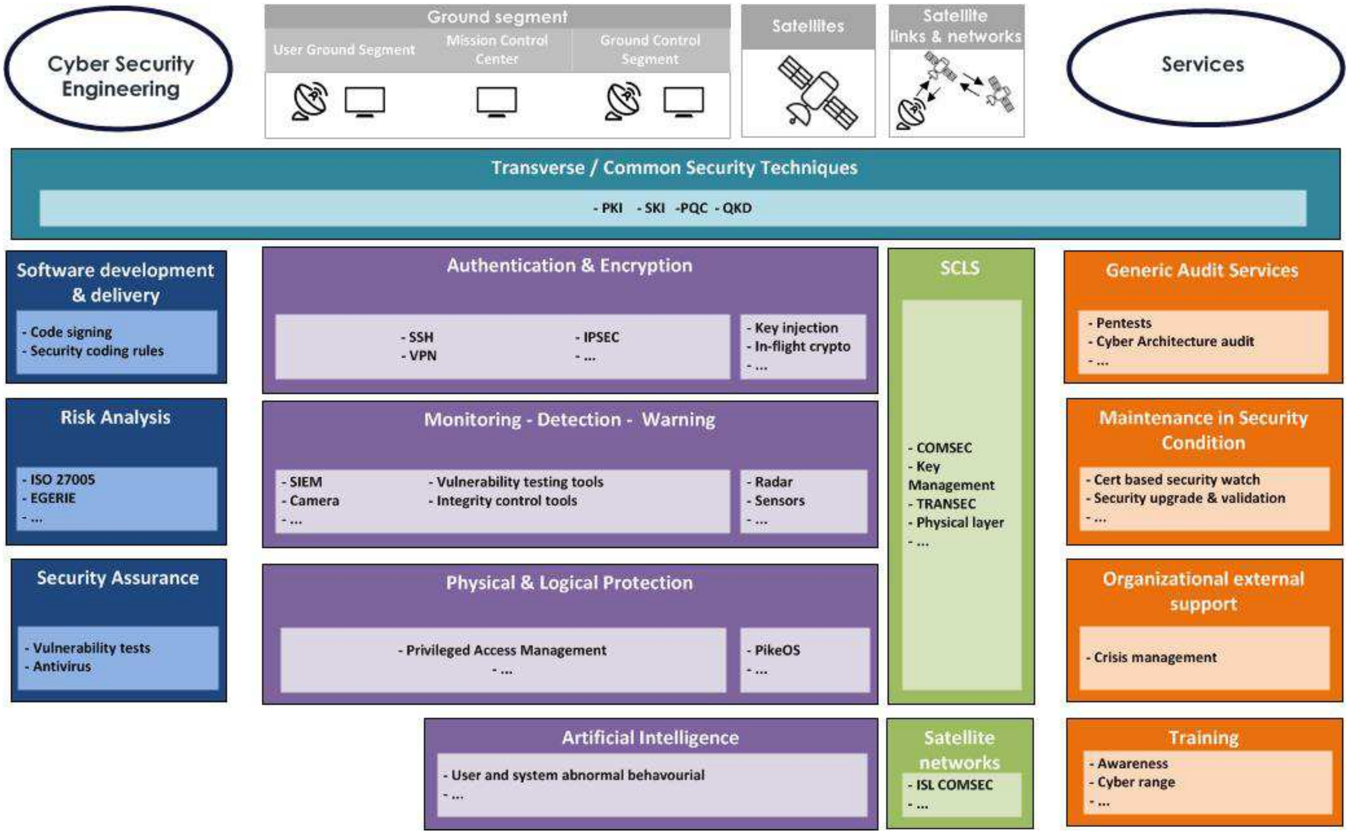
- Achieving the security objectives resulting from Risk Analysis run for future space missions covering Observation, Telecommunication and Navigation missions.
- And through the entire information processing lifecycle of a space program

Recall : notion of « Security Technic » used in the Portfolio covers any candidate security technic, technology, concept, solution, product, or service, acting as a countermeasure.

Portfolio Architectural Model

In order to cover as indicated the lifecycle of a space program, the Security Architecture Portfolio is described through five domains derived from NIST Cybersecurity framework.

- Cybersecurity Engineering, Ground Segments, Satellite, Satellite Links and Networks, Services, and is completed by an Transverse Security Technics domain covering common basic security technics used by the five previous domains



Cyber Security Engineering

Ground segment

User Ground Segment

Mission Control Center

Ground Control Segment

Satellites

Satellite links & networks

Services

Transverse / Common Security Techniques

- PKI - SKI -PQC - QKD

Software development & delivery

- Code signing
- Security coding rules

Risk Analysis

- ISO 27005
- EGERIE
- ...

Security Assurance

- Vulnerability tests
- Antivirus

Authentication & Encryption

- SSH
- VPN

- IPSEC
- ...

- Key injection
- In-flight crypto
- ...

Monitoring - Detection - Warning

- SIEM
- Camera
- ...

- Vulnerability testing tools
- Integrity control tools

- Radar
- Sensors
- ...

Physical & Logical Protection

- Privileged Access Management
- ...

- PikeOS
- ...

Artificial Intelligence

- User and system abnormal behavourial
- ...

SCLS

- COMSEC
- Key Management
- TRANSEC
- Physical layer
- ...

Satellite networks

- ISL COMSEC
- ...

Generic Audit Services

- Pentests
- Cyber Architecture audit
- ...

Maintenance in Security Condition

- Cert based security watch
- Security upgrade & validation
- ...

Organizational external support

- Crisis management

Training

- Awareness
- Cyber range
- ...

Figure 5-1 – Security Architecture Portfolio detailed Model

Security Technics included in the Security Architecture Portfolio

- Note : one or more individual (Level 2) security technics is defined in the portfolio for each Level1 security technic

Domain#1: Cybersecurity Engineering

Topic	Security Technic (Level1)
Software Development and Delivery	Code Signing Security Coding Rules
Risk Analysis	RA Standards / Methods RA Tools (Security Assessment)
Security Assurance	Vulnerability assessment tools & services Virus / Malware free software delivery Protection

Domain#2: Ground Segments

Topic	Security Technic (Level1)
Authentication and Encryption Management	Ground Communications Authentication & Encryption Machine network / User Authentication
Monitoring - Detection - Warning	NGIPS Cyber Threat Intelligence (CTI) Antenna Motion Detection Security Operating Center Situational Awareness
Physical and logical Protection	Backup and Restore principles Real-Time Embedded Ground Systems Segregation Segregation of Duties and Traceability for Administrator Site Protection Trusted Platform Module (TPM) Logical Protection Physical Protection Logical Access Control Denial of Service Protection Security Qualification & Certification
Artificial Intelligence	Abnormal Behavioural Detection of a System from Inside

Domain#3: Satellite (Bus & Payload)

Topic	Security Technic (Level 1)
Authentication and Encryption management	Secure on-ground Key Injection schemes using PKI technology In-flight Satellite Cryptography Upgrade
Monitoring - Detection - Warning	Dynamic Routing Issues Detection Situational Awareness On-board software (OBSW) Integrity Data reliability
Physical and logical Protection	Physical protection Logical segregation

	Physical segregation Trusted Platform Module (TPM)
Artificial Intelligence	Abnormal Behavioural Detection from On-board Software

Domain#4: Satellite Links and Networks

Topic	Security Technic
Space Communication Link Security	Satellite / Ground links COMSEC Protection Satellite / Ground links TRANSEC Protection for GEO satellites Satellite / Ground links TRANSEC Protection for LEO / MEO satellites Conventional Satellite Key Management using SKI Technology Enhanced Satellite Key Management using PKI Technology Inter Satellite Link Integrity Inter satellite Link technology Physical layer security (PHYSEC) Advanced Satellite Key Management using PQC technology QKD based satellite keys distribution
Space Networks Security	Space Network Control Plane Protection

Domain#5: Services

Topic	Security Technic
Generic Audit Services	Pentests Cybersecurity Architecture Audit
Maintenance in Security Condition	Cyber Threat Intelligence (CTI) CERT/CSIRT Based Security Watch Security Upgrade & Validation
Organizational External Support	Incident Response Team Crisis Management
Training	Training

Domain#6 : Transversal/Common Security Technics

Topic	Security Technic
Authentication and Encryption Management	Public Key Infrastructure (PKI) Secret Key Infrastructure (SKI) Post Quantum Cryptography (PQC) Quantum Key Distribution (QKD)

6. RECOMMENDATIONS FOR FUTURE ACTIVITIES (WP1430)

To establish a set of recommendations for helping ESA to formulate a technology strategy for the security domain, the following 3 steps process has been established:

- Step 1
  - ⇒ Identify the security technics that need an improvement to mitigate emerging threats (due to Cybersecurity or space missions evolutions) or to mitigate already known threats.
- Step 2
  - ⇒ Identify the most effective security technics from the previous emerging security technics priority list (output of Step 1).
- Step 3
  - ⇒ Identify the security technics from the last list (output of Step 2) that are legitimate to be promoted or supported by ESA.

The proposed ten recommendations for future activities (R&D actions) proposed in support of ESA Security domain Technology Strategy / Plan elaboration, are listed in Table 6-1.

REC#01	Migration from Conventional PKI to Post Quantum Cryptography (PQC) based PKI in Future Space Missions
REC#02	In-Flight Satellite Cryptography Upgrade
REC#03	Enhanced PKI based Satellite Key Management – Secure In-flight Satellite Keys Establishment & Recovery
REC#04	Space communication links Security - TRANSEC TCR Protection for LEO/MEO Satellites
REC#05	Space CTI (Cyber Threat Intelligence) for Cybersecurity Information Sharing
REC#06	On-board Physical / Logical Segregation - Standard and Secured satellite Avionics Bus Definition
REC#07	On Board Artificial Intelligence Algorithms Selection
REC#08	Physical Layer Security for Satellites (PHYSEC with SP /SKG/SC security services)
REC#09	Space Network Control Plane Protection
REC#10	Satellite On-Board Situational Awareness

Table 6-1: List of Proposed Recommendations

Additional Proposed Optional Activities

- **OPT#01**: Demonstrator of Satellite Quantum Key Distribution (S-QKD)

7. CONCLUSION

Present ESA study led to analyse future space missions and to define a set of five scenarios with description of associated detailed architectures covering the target missions

- Observation (1 scenario), Telecommunication (2 scenarios), Navigation (2 scenarios).

Risk Analysis run for each mission/scenario and focusing on new features / risks has identified:

- Observation mission: 5 major risks and 13 countermeasures (over 40) with high priority.
- Telecommunication mission: 9 major risks and 8 countermeasures (over 26) with high priority.
- Navigation mission: 1 critical risk and 5 major risks, and 22 countermeasures (over 58) with high priority.

In parallel, a preliminary and then deep review of emerging security technics / technologies / concepts has been performed covering an important set of distinct and complex technics

- Security Technics retained as part of selected technics
  - ⇒ Post-quantum cryptography (PQC), Physical Layer Security (PHYSEC), Key Generation Management & Distribution, Intrusion Detection / Protection,
  - ⇒ Penetration Testing (PT), Secure Partitioning/ MILS & PikeOS, Software/data integrity, Software Secure Boot, TPM (Trust Platform Module),
- Other Security Technics (not retained as part of selected technics)
  - ⇒ Quantum Cryptography (QKD), Lightweight Cryptography, Homomorphic Encryption,
  - ⇒ Physically Unclonable Function (PUF), Moving Target Defense.

From analysis of security objectives coverage by Security technics a detailed Security architecture Portfolio has been built;

- Achieving the security objectives resulting from Risk Analysis run for all analysed missions.
- And through the entire information processing lifecycle of a space program
- Involving 73 security technics / products / services / technologies / concepts.

Lastly, from the input set of Portfolio security technics, a detailed evaluation process has been run to select the most important / high priority emerging security technics to be subject to R&D Actions initiated by ESA in the frame of ESA Technology Plan for Security domain.

- This led to define a set of 10 recommendations plus one optional recommendation

Beside fundamental security technics, study results showed the growing and critical importance role of Cybersecurity relevant technics for both satellite and ground segment for achieving future space missions security objectives, and requiring a new cultural approach

- Study also showed the importance of Cybersecurity information handling (threat intelligence) and great interest to establish a CTI platform for space domain.

END OF DOCUMENT