Threats and Security of Future Avionics Systems

Antonios Atlasis
System Security Section
End-to-End Systems Division
Directorate of ***Technology, Engineering and Quality***

ADCSS 2024, 24 October 2024, ESTEC

e Security @ Breaking News

esa

NL TIMES

TOP STORIES HEALTH CRIME POLITICS BUSINESS TE

SATURDAY, 6 APRIL 2024 - 10:20

Cyber attack on TV channel BabyTV: Toddlers suddenly exposed to Russian propaganda

The TV channel BabyTV has been the victim of a cyber attack in which a Russian propaganda film was suddenly shown on the children's channel. Insiders are now warning that

of the hackers but "possibly a harbinger of more," NU.nl

On Thursday, March 28, Baby suddenly broadcast instead the sound cut out and then

sian propaganda was the incident clearly. First ren's channel, he told NU.nl

V was not the actual target

Apache - The ASF
@TheASF
Follow

Did you know that Ingenuity, the Mars 2020 Helicopter mission, is powered by Apache Log4j? logging.apache.org #Apache #OpenSource #innovation #community #logging #services

December 16, 2021, Update:

NASA's Ingenuity helicopter does not run Apache or log4j nor is it susceptible to the log4j vulnerability. NASA takes cybersecurity very seriously and, for this reason, we do not discuss specifics regarding the cybersecurity of agency assets.

Source: https://science.nasa.gov/blogs/flight-17-discovering-limits/

Viasat

News Home | Corporate | Enterprise & Mobility | Defense | Satellite Internet

Corporate News

KA-SAT Network cyber attack overview

Viasat is providing an overview and incident report on the cyber-attack against the KA-SAT network, which occurred on 24 February 2022, and resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service.

March 30, 2022 04:55 AM • Viasat, Inc.

Source: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

MATT BURGESS SECURITY AUG 10, 2022 10:00 AM

The Hacking of Starlink Terminals Has Begun

It cost a researcher only $25 worth of parts to create a tool that allows custom code to run on the satellite dishes.

Want to pwn a satellite? Turns out it's surprisingly easy

PhD student admits he probably shouldn't have given this talk

Iain Thomson Fri 11 Aug 2023 13:01 UTC

BLACK HAT A study into the feasibility of hacking low-Earth orbit satellites has revealed that it's worryingly easy to do.

Source: https://www.theregister.com/2023/08/11/satellite_hacking_black_hat/

In this paper, we first provide a taxonomy of threats against satellite firmware. We then conduct an experimental security analysis of three real-world satellite firmware images. We base our analysis on a set of real-world attacker models and find several security-critical vulnerabilities in all analyzed firmware images. The results of our experimental security assessment show that modern in-orbit satellites suffer from different software security vulnerabilities and often a lack of proper access protection mechanisms. They also underline the need to overcome prevailing but obsolete assumptions. To substantiate our observations, we also performed a survey of 19 professional satellite developers to obtain a comprehensive picture of the satellite security landscape.

Source: Space Odyssey: An Experimental Software Security Analysis of Satellites
J. Willbold, et al, 44th IEEE Symposium on Security and Privacy (S&P)

Why we need to protect our missions and what has been changing

1. Space missions are part of our **critical infrastructure** (Galileo, Earth Observation, Meteo, IRIS2, etc.).
    - The disruption of operation of these missions will affect our everyday life.
2. We have to **protect the investment** of ESA Member States.
    - Implementing the appropriate security measures is certainly less costly than losing a mission, or its data, etc. due to a security incident.
3. We need to **protect our** (ESA and ESA Member States) **reputation**.

motivation

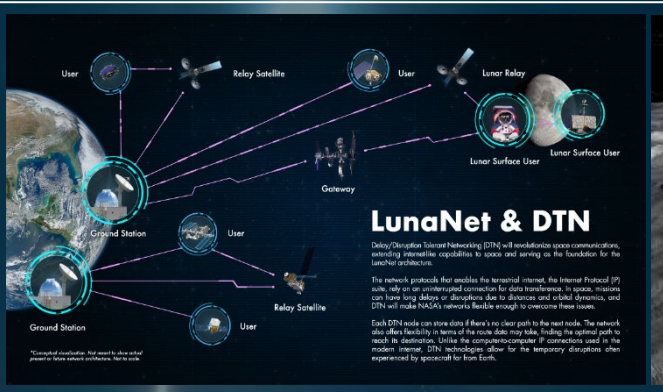
1. Importance/criticality of space infrastructure attracts the attention of potential adversaries with significant capabilities (e.g. state actors).
2. *Technology evolution* (e.g. Software Defined Radios) makes space "accessible" to wider "audience".
3. **Interconnectivity** trends (e.g. 5G NTN) will **increase the attack surface**.
4. Latest development trends (e.g. more reliance on COTS) "bring" "terrestrial" vulnerabilities to space.
5. **New** technological **threats** arise (e.g. Quantum computing threat to cryptography)

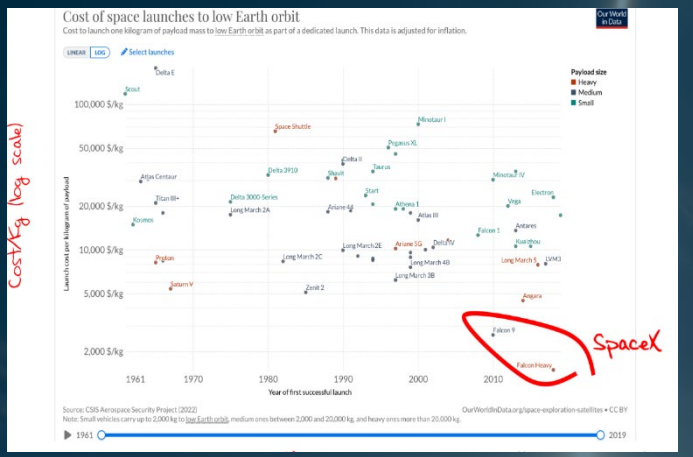
Increased exploitation opportunities

motivation

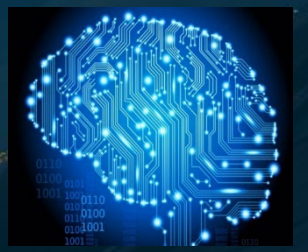
6. Space is "sexy"; hackers / crackers / security researchers will do everything to find vulnerabilities in space systems for self-advertisement / promotion.

Space Scenario 2040 - Key Elements





SpaceX Starlink Gen 1	4,408
SpaceX Starlink Gen 2	29,988
OneWeb, Phase 1	718
OneWeb, Phase 2	6,372
Amazon Project Kuiper	7,774
China Guowang	12,992
Astra	13,620
Boeing	5,842
Globalstar	3,080
Lynk	2,000
Telesat Lightspeed	1,969
Spin Launch	1,190
TOTAL	**89,953**
E-Space	337,323

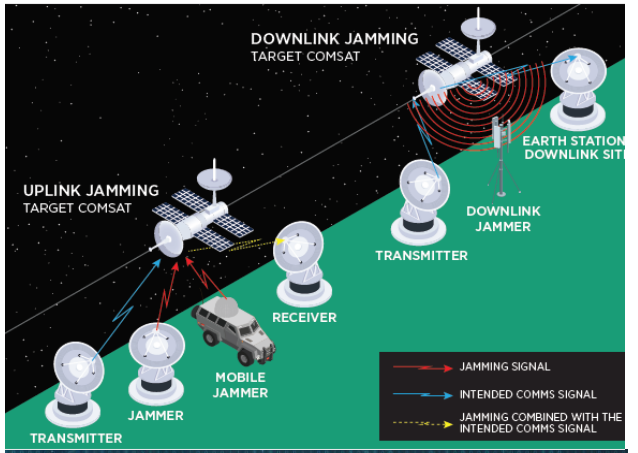


The “traditional” challenges and security implications

- Distributed architecture: ground / space / user
- Physical / Cyber hybrid systems
- Exposed communication links (space-ground, space-space)
- Massive service coverage area / Millions of users in footprint

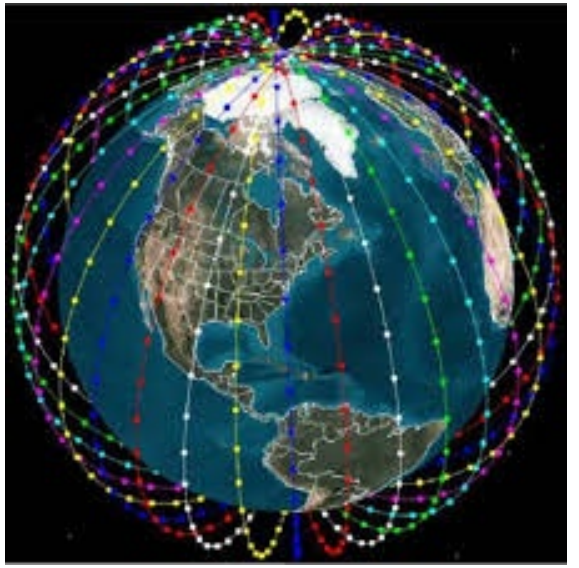
Large attack surface

- Constrained and harsh environment (weight, space, power, EM, etc.)
- Large distance / Long Comms delay / Intermittent communications
- Long development cycles / Long lifetime of the missions
  - ➔ / Obsolescence issues
- Lack of physical access (for space segment)



The new trends and their impact to security

- Large constellation ➔ scalability challenges (in terms of key management, etc.)
- Integration with terrestrial networks (e.g. 5G NTN,)
- Emerging Quantum Threats for crypto
- New Space mindset
  - COTS solutions also onboard satellite
  - Faster development cycle ➔ more streamlined security is needed
- Requirements for enhanced situational awareness
- Supply chain security
- Integration of new technologies:
  - AI and Security
  - Optical and Quantum Comms security



Governance and Programmatic Changes

Cyber security requirements are flown down gradually to more space missions

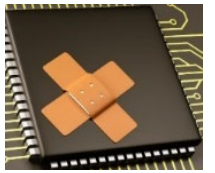
- Started with Galileo, continued with IRIS2, other EC mission may follow
- Baseline security measures will also be applied to other ESA missions

A platform hosts more than one payload (and not necessarily from the same stakeholder)

- Platform sharing between governmental, semi-governmental and commercial
- Platform sharing between different commercial actors; payload sharing

What are the challenges specifically related to space Avionics ?

- New technologies for already applied security measures; examples:
  - Crypto boxes ➔ we need to migrate to **quantum resistant solutions**
    - PQC is more resource demanding than typically used symmetric crypto ➔ impact on avionics.
    - **Crypto agility** needs to be introduced.
    - On board True Random Number Generators
- Payload and platform sharing
  - **Segregation**
    - Software (e.g. hypervisors)
    - Hardware / platform (e.g. Avionics busses) ➔ more research is needed
  - **On-board** security **detection** and protection mechanisms
- **On-board patching** ➔ how to patch without “breaking” it (read: CrowdStrike case)
- **Remote attestation** mechanisms ➔ **Recovery** is possible only remotely



Already Ongoing Research and Developments Activities

- Coordination at ESA-wide level under ESA Cyber Coordination Board
- GSTP Cyber Security Compendia (2019, 2022) have been proven very successful
- As part of Basic Activities to complement ESA Cyber Resilience
  - ✓ Modular security reference architecture
  - ✓ Spacecraft digital forensics and incident handling
- As part of GSTP Cyber Security compendium 2022:
  - ✓ Post Quantum Crypto with crypto agility
  - ✓ Supply chain protection
  - ⇨ Security protocols building blocks (IPsec, BPsec)
  - ⇨ Software Defined Radio security
  - ⇨ On-Board Security (hardware, software, platform bus, etc.
  - ⇨ RF Firewall

GSTP Cyber Security Compendium 2022

GEN - Generic Technologies - Cybersecurity

CD3 - Avionic Systems

Programme Reference	Activity Title	Budget (k€)
GT1Y-601ES	Intrusion detection prevention module for secure avionics bus	2,500
GT1Y-602ES	Confidential computing: implementing spacecraft operations using trusted execution environments	2,000
GT1Y-603ES	Security segregation and isolation in a satellite	2,000
GT1Y-604ES	Agile post-quantum space data link security protocol hardware module	3,300
GT1Y-605ES	End-to-end supply chain protection	3,000
GT1Y-606ES	CCSDS delay-tolerant networking BPSec module	2,000
GT1Y-607ES	IP over CCSDS including internet protocol security module	1,200
	Total CD3	16,000

CD5 - Radiofrequency & Optical Systems and Products

Programme Reference	Activity Title	Budget (k€)
GT1Y-608ES	Low-cost resilient software defined radio platform for satellite applications	450
GT1Y-609ES	Radiofrequency firewall for satellites	4,000
	Total CD5	4.450

Our Vision for Securing our Space Systems

Mission specific

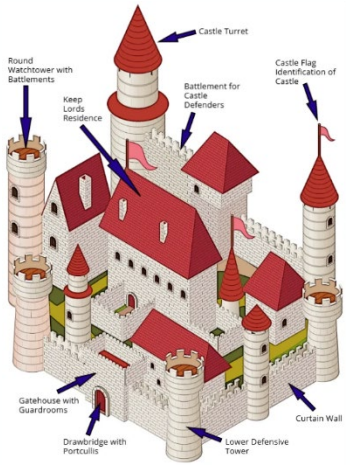
0. Basic Security Principles

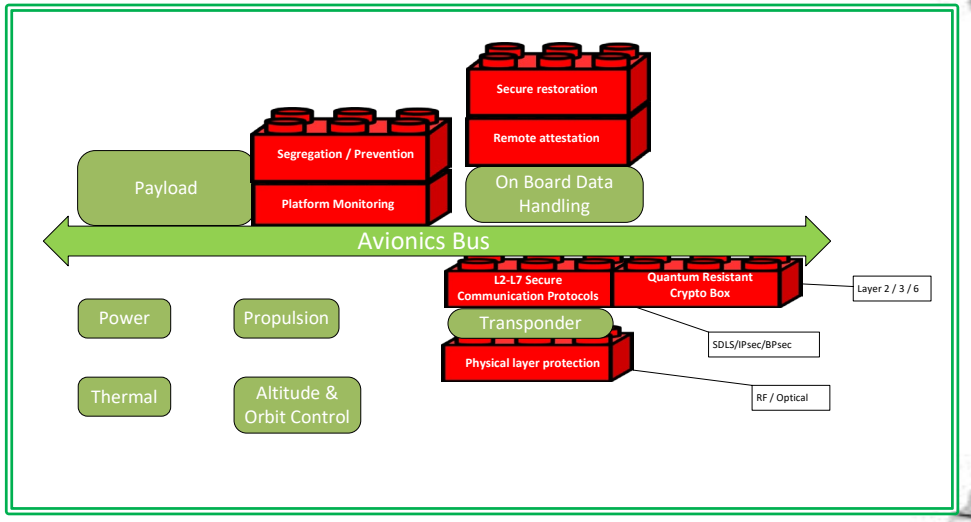
1. Modular Security Reference Architecture

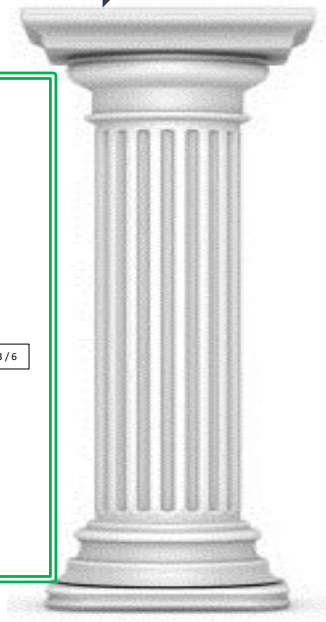
2. Identify Building Blocks and Create COTS products

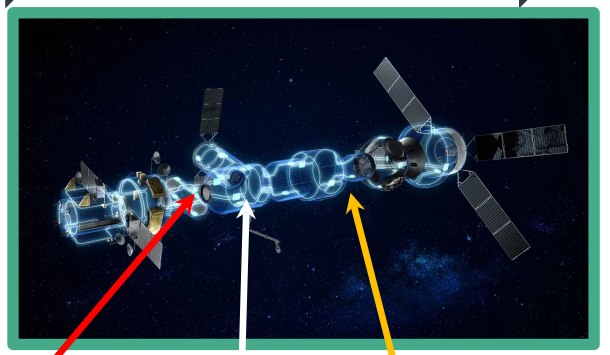
3. Tailor the architecture to mission specific needs

4. Select required COTS









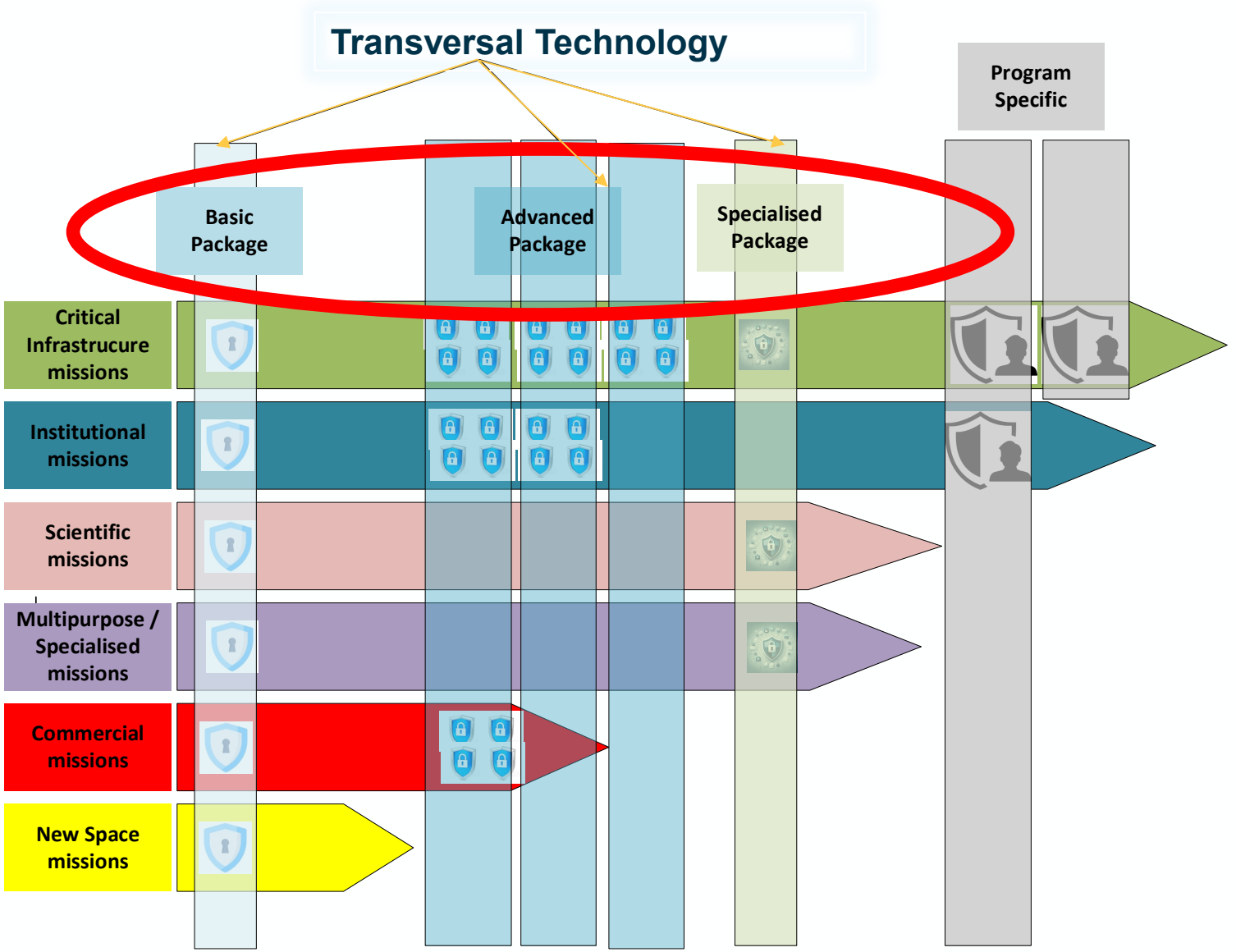
On-board Security Protection

RF and Optical Security Protection

Quantum Resistant Crypto

Secure-by-design

Security technologies coverage

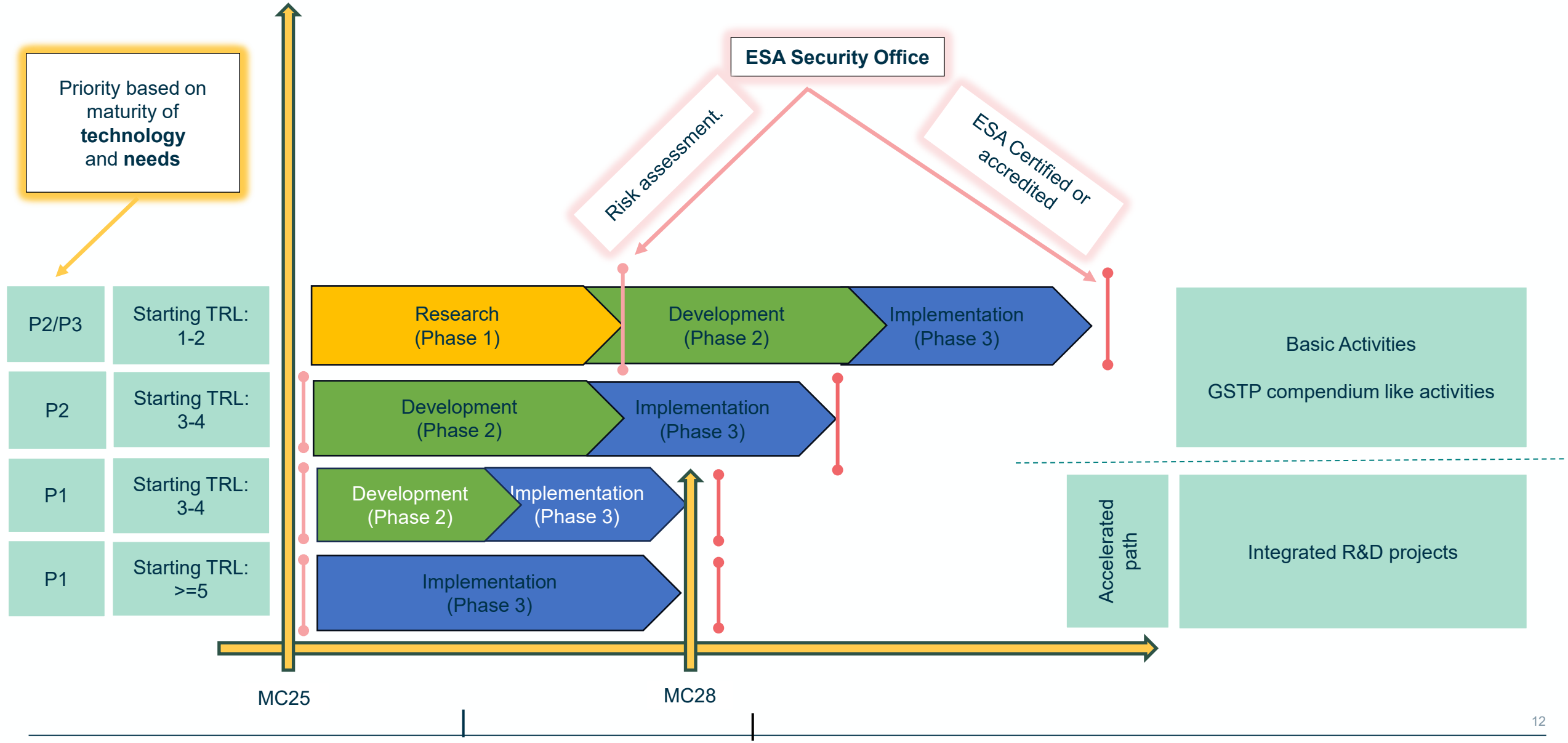


SES ASTRA An SES GLOBAL Company

Viasat

eutelsat

Development cycle and Programmatic element



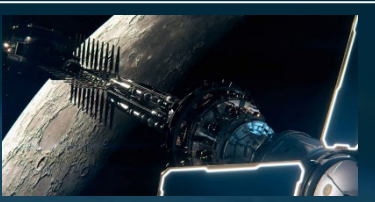
Space Vision 2024 – 2040: Space Security Technologies

Space Security Technologies (Push)

- Quantum Resistant Cryptography
- RF Security Protection / Antijamming
- Optical Security
- Crypto Agility
- Quantum Technologies for Security
- Supply Chain protection
- Physical / Hardware Security
- High Speed TRNG
- Trusted Platform Modules / Trusted Execution Environments
- Zero-trust, cloud native & next gen access control
- Segregated payload & ground segment ops
- AI for Security / Security for AI
- Satellite Active Défense
- Homomorphic Encryption
- Space Threat Intelligence / Situational Awareness
- Secure Space Protocol Implementation
- Space Digital Forensics and Spacecraft Recovery

Space Security Technologies (Mission Pull)

- High Speed Crypto (HydRON, IRIS2)
- Avionics (hardware, software) segregation (HydRON, IRIS2)
- (Asymmetric) PQC (IRIS2)
- 5G/6G Security (IRIS2, LEO PNT)
- Quantum Resistant Space PKI (Lunanet)
- BPsec, IPsec (Deep Space / Interplanetary Missions, Lunanet)
- Quantum Security (EuroQCI)



Programmatic Objectives & Considerations

Objectives:

- Develop **products** of generic security technology **to be used transversally**, suitable to be picked-up as COTS by missions (Directorates participated in their definition).
- Make products available for all segments (space, ground, etc.), and technologies, across the full OSI stack, to allow **implementation of defence-in-depth** approach .
- Adhere to and promote standardised solutions (SAVOIR, CCSDS, ECSS, etc.) to **ensure interoperability and allow collaborations**.

Programmatic considerations:

- Create the programmatic considerations **to go fast**.

The **security technology development roadmap** reinforced by the ESA Security Office, to become a security enabler for future ESA space missions.

Questions ?

Space Security Technologies (Push)

2030

2040

Satellite Active Défense

Supply Chain protection

Space Threat Intelligence / Situational Awareness

Space Digital Forensics and Spacecraft Recovery

Zero-trust, cloud native & next gen access control

Physical / Hardware Security

Security Protocols

Cyber Security

Crypto

RF Security

Quantum Security (EuroQCI)

Avionics (hardware, software) segregation

Segregated payload & ground segment ops

BPsec, IPsec

5G/6G Security (IRIS2, LEO PNT)

Trusted Platform Modules / Trusted Execution Environments

AI for Security

High Speed TRNG

Quantum Resistant Cryptography

Crypto Agility

Optical Security

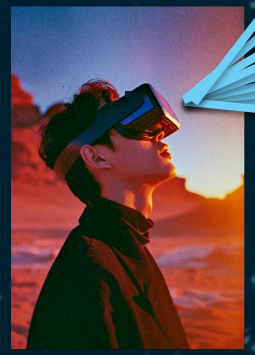
Security for AI

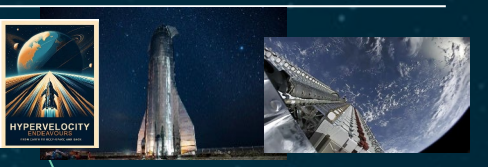
(Asymmetric) PQC

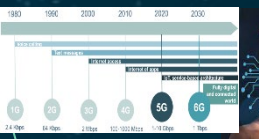
High Speed Crypto

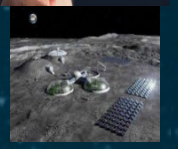
Quantum Resistant Space PKI

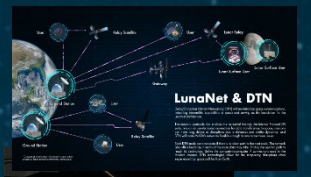
Homomorphic Encryption

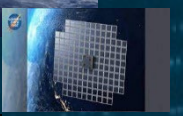


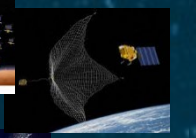












→ THE EUROPEAN SPACE AGENCY