Challenges and Solutions in Embedded Security for Space Avionics: GMV’s Perspective and Contributions

dgarjona@gmv.com
www.gmv.com

esa

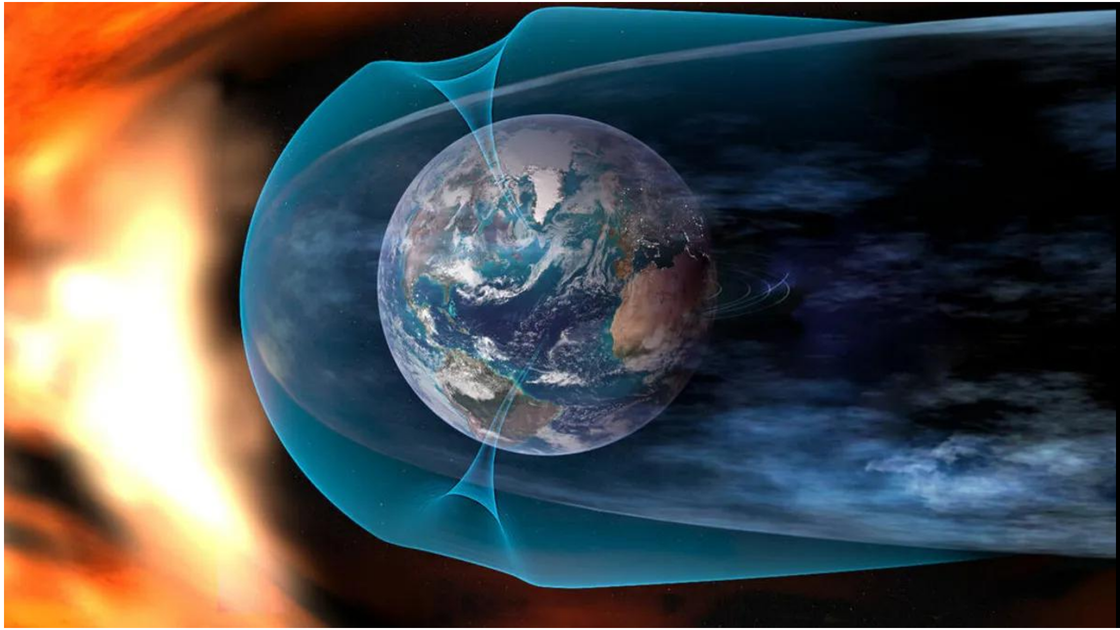
ADCSS 2024

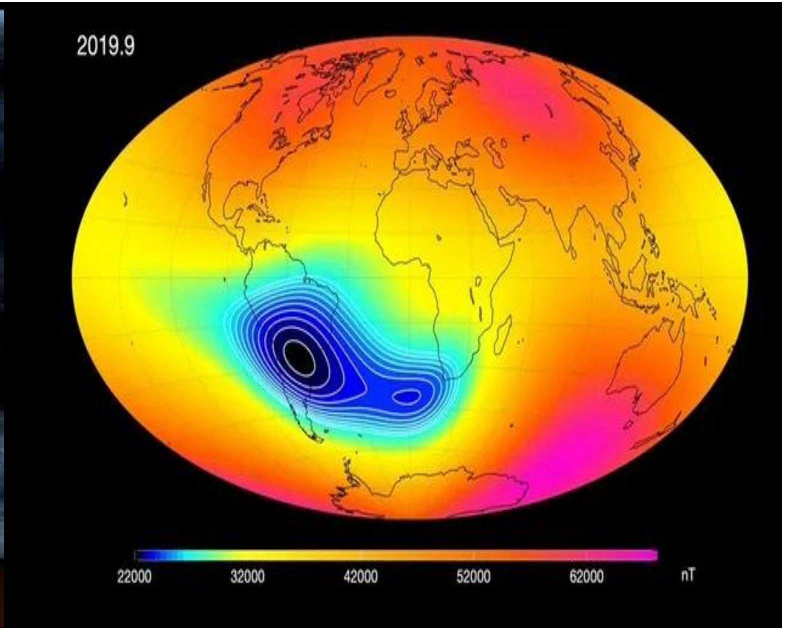
18th ESA Workshop on Avionics, Data, Control and Software Systems

gmv

INNOVATING SOLUTIONS

Anomaly Atlantic South





Agenda

1 Why Embedded Security in Space Avionics?

2 Challenges in Embedded Security for Space Avionics

3 SAVOIR & SECURITY

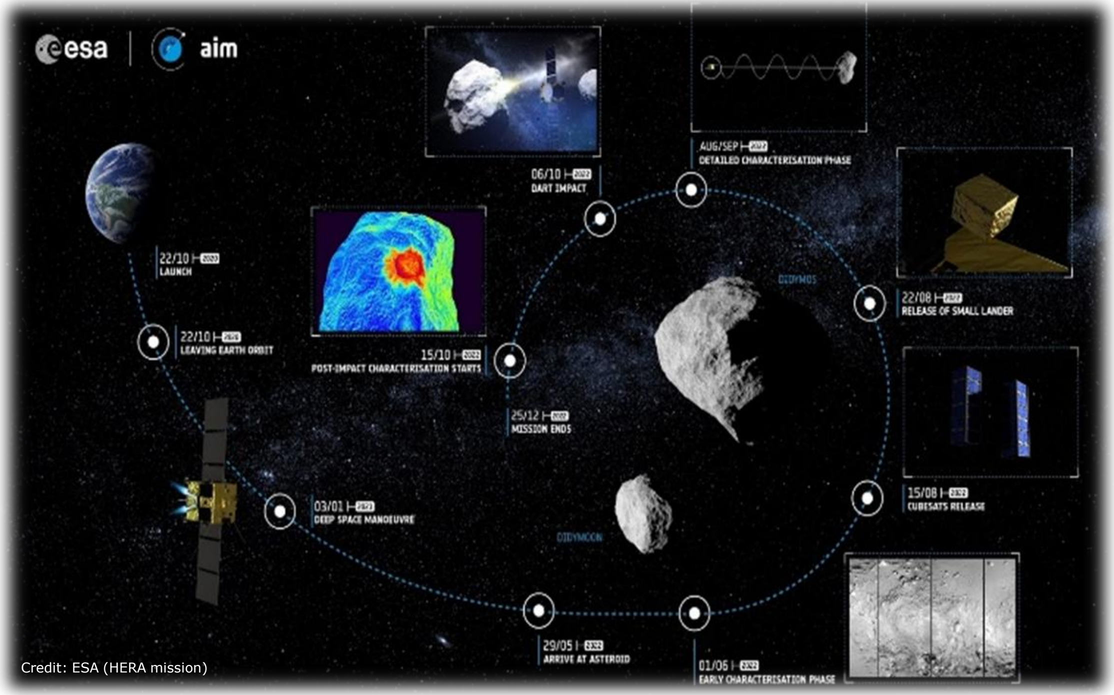
4 GMV View On Avionics & Security Functions

5 Authority – ESA/Integrator Role

6 On-going- GMV projects

Date: 18/01/2024

Welcome to our units' offices



Credit: ESA (HERA mission)

- **Hardened/Ruggedized** Devices protected versus:
  Radiation
  Solar Pressure
  Electromagnetic Waves
  Vibrations (launching environment)
  Wide temperature range
- Hard/Impossible to repair devices (up there):
  Reliability is a must
- **Autonomy** is a key factor
  Independent Systems
  Huge delay/latency in Ground-Spacecraft communication
- **Limited** power consumption on board
- Mass and volume shall be **minimized**
- Design and implementation of **Fault-Tolerance** systems
- Critical, Precise and **Deterministic** systems in Hard Real-Time applications
- Extensive and intensive **Validation** and Verification

- **Ad-hoc** projects for each mission: Nobody went there before
  → how to create **representative** environment, images, conditions?

GMV: A global technology group

Founded in

1984

Multinational technology group. **Private capital**

Headquarters in Spain (Madrid).

Subsidiaries in 12 countries

(ops in 70+)

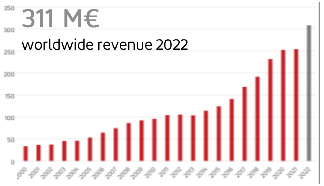
+3,300 employees

Roots tied to the Space and Defence industry

Engineering, development and integration of systems, software, hardware, specialized products and services

CMMI level 5

CMMIDEV/5



311 M€

worldwide revenue 2022

Aeronautics, Space, Defense & Security, Cybersecurity, Intelligent Transport Systems, Healthcare, Banking & finances, and ICT industries

Space

Aeronautics

Defense & Security

Telecommunication

Cybersecurity

Intelligent Transport Systems

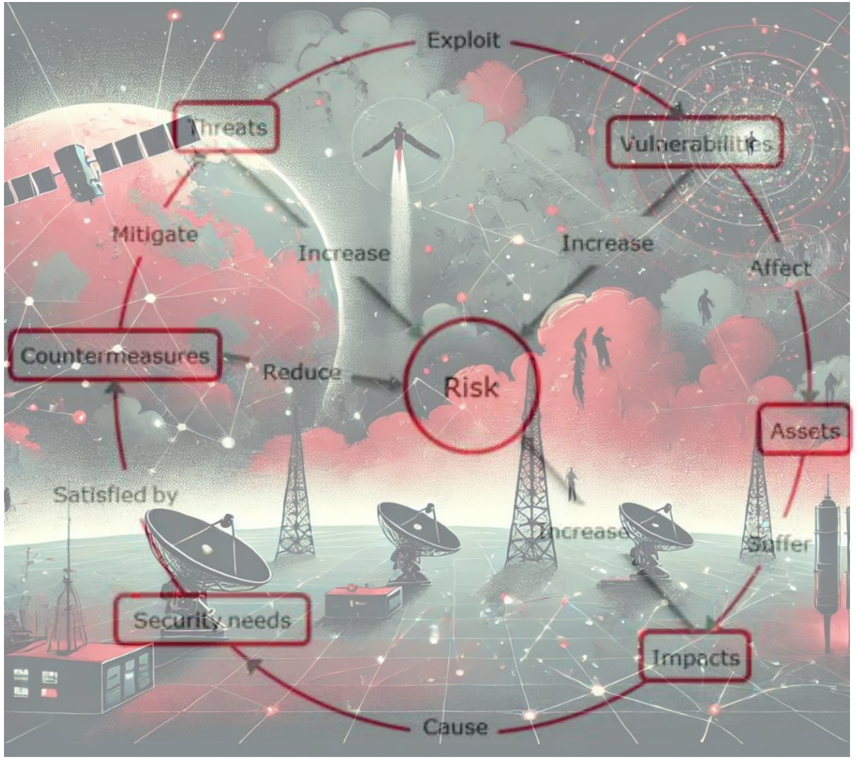
Healthcare

Public Sector and Corporate ICT

Banking & Finances

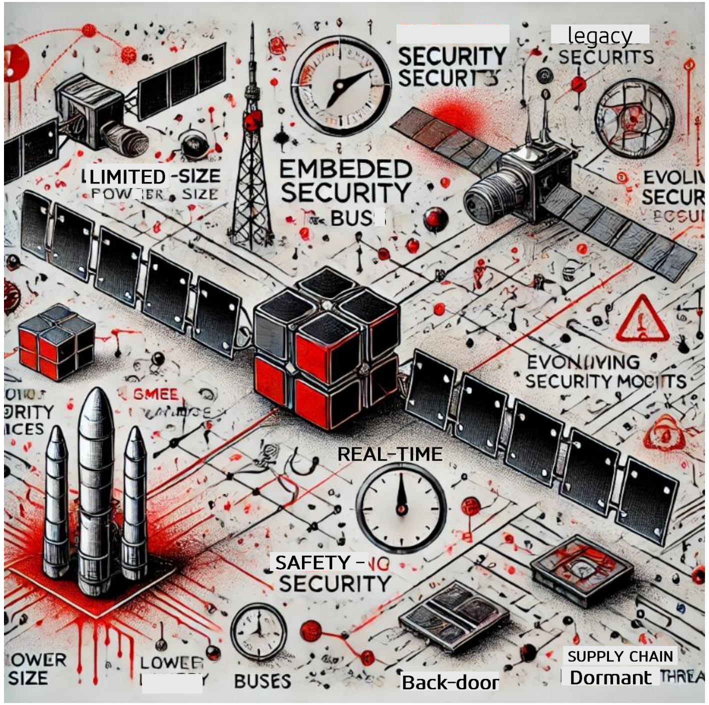
Why Embedded Security in Space Avionics?

- Space is becoming more interconnected and accessible.
- Increasing reliance on space-based infrastructure (communications, PNT, etc.)
- Security is a critical requirement, not a “tax.”
- Intentional Threats and Spying
- Preventing risks and reducing costs in the long run
- Sophisticated cyber threats: Espionage, jamming, spoofing, hacking.
- Space asset vulnerability: Satellites, Rovers, Gateways, Space Stations, Ground stations, communication links.
- Increased autonomy: New threats emerge as systems become more self-reliant.



Challenges in Embedded Security for Space Avionics

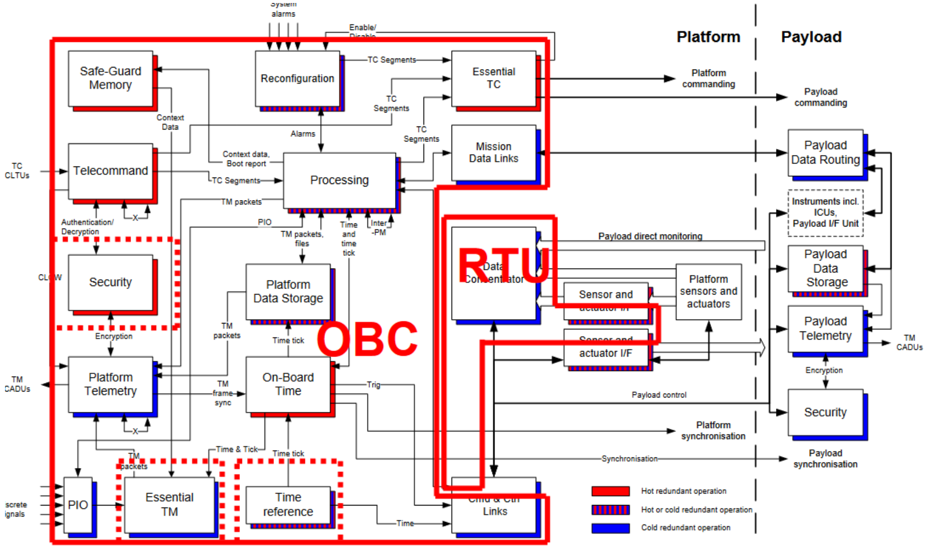
- **Limited resources** in space avionics (power, size, memory, buses, processing).
  → Security features are sometimes overlooked to save resources
- **Latency and remote access issues**: Long delays in communication make real-time response hard.
- **Diverse mission requirements**: from CubeSats to flagship satellite missions.
- **Real-Time Constraints in Critical Operations**
- **Threat models**: Evolving cybersecurity risks, malicious actors
- **Lack of Legacy System Compatibility:** COTS or heritage components, payloads, instruments, HW or SW that cannot accommodate modern security measures
- Interplay between **safety**-critical systems and **security** measures can cause **conflicts**
- **Supply Chain Vulnerabilities:** backdoors, dormant



SAVOIR & SECURITY

SAVOIR
space avionics open interface architecture

- SAVOIR provides a comprehensive framework for developing highly reliable, fault-tolerant avionics systems.
- Ensures interoperability between different components and subsystems, focusing on safety, security, and reusability.
- Adopted for Spacecraft Bus mainly for larger satellites, traditional space missions, and projects with certification requirements.
- Focus on functional chains, decoupling of hardware from software. On-board systems like navigation, communication, or attitude control can be managed independently and react to real-time data.



SAVOIR & SECURITY

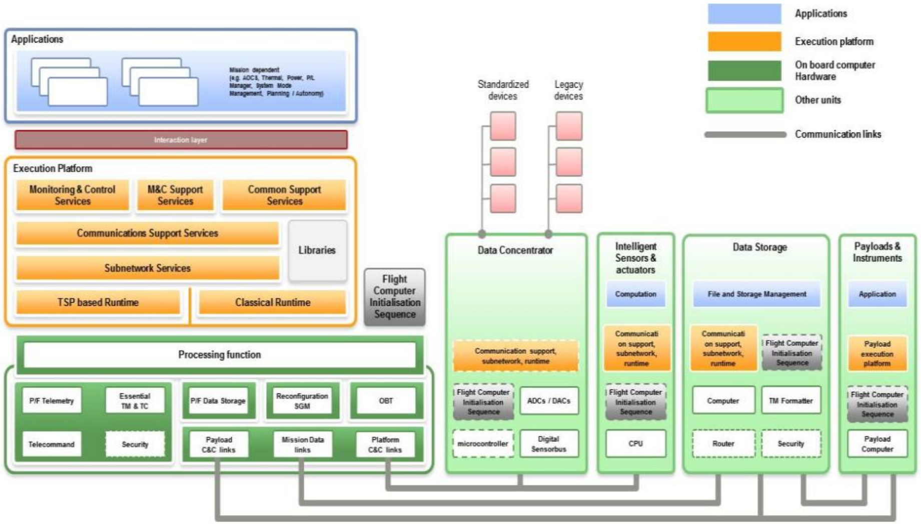
SAVOIR
space avionics open interface architecture

- SAVOIR provides a comprehensive framework for developing highly reliable, fault-tolerant avionics systems.

- Ensures interoperability between different components and subsystems, focusing on safety, security, and reusability.

- Adopted for Spacecraft Bus mainly for larger satellites, traditional space missions, and projects with certification requirements.

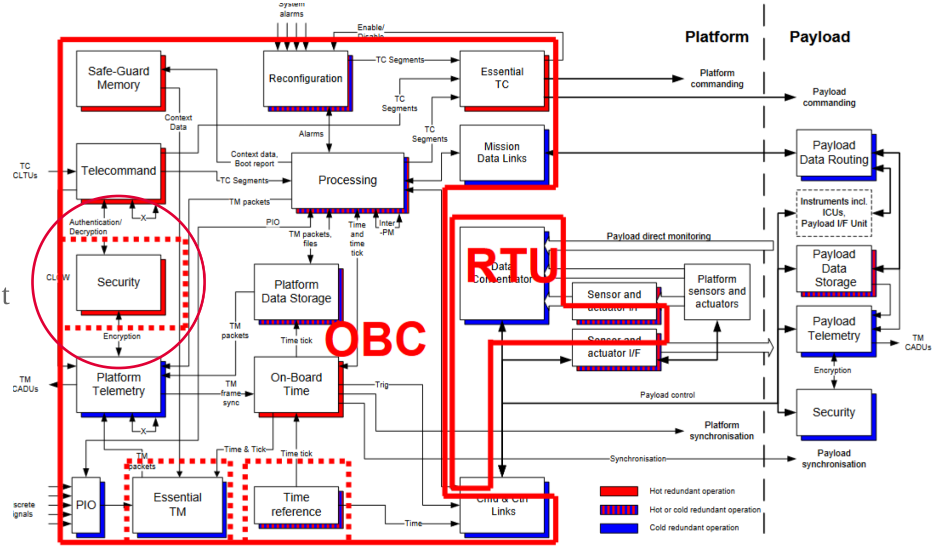
- Focus on functional chains, decoupling of hardware from software. On-board systems like navigation, communication, or attitude control can be managed independently and react to real-time data.


Applications
Mission dependent (e.g. AOCS, Thermal, Power, P/L Manager, System Mode Management, Planning / Autonomy)
Interaction layer
Execution Platform
Monitoring & Control Services
M&C Support Services
Common Support Services
Communications Support Services
Libraries
Subnetwork Services
TSP based Runtime
Classical Runtime
Flight Computer Initialisation Sequence
Processing function
P/F Telemetry
Essential TM & TC
Telecommand
Security
P/F Data Storage
Reconfiguration SGM
OBT
Payload C&C links
Mission Data links
Platform C&C links
Standardized devices
Legacy devices
Data Concentrator
Communication support, subnetwork, runtime
Flight Computer Initialisation Sequence
ADCs / DACs
microcontroller
Digital Sensorbus
Intelligent Sensors & actuators
Computation
Communicati on support, subnetwork, runtime
Flight Computer Initialisation Sequence
CPU
Data Storage
File and Storage Management
Communicati on support, subnetwork, runtime
Flight Computer Initialisation Sequence
Computer
TM Formatter
Router
Security
Payloads & Instruments
Application
Payload execution platform
Flight Computer Initialisation Sequence
Payload Computer
Applications
Execution platform
On board computer Hardware
Other units
Communication links

SECURITY SPACE REFERENCES AND STANDARDS

SAVOIR
space avionics open interface architecture

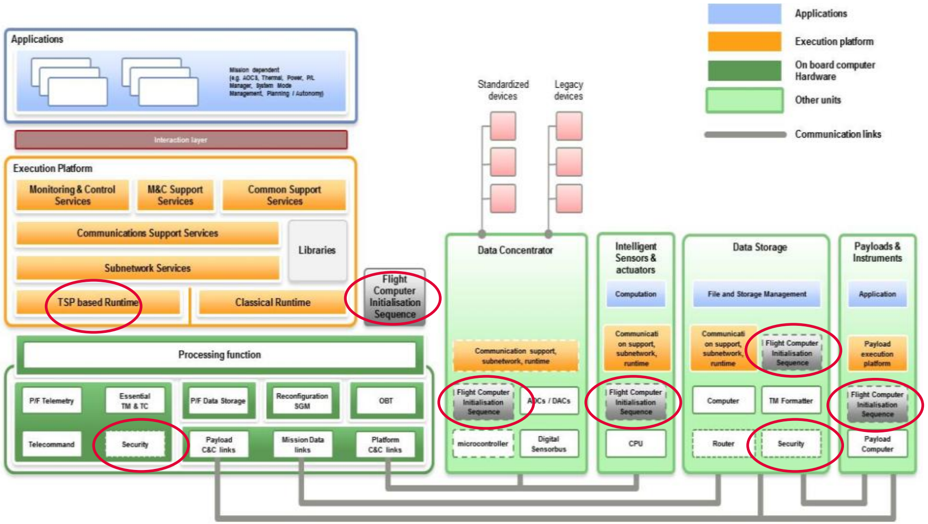
- CCDSS 350.1-G-3 –
  Security Threats Against Space Missions, Informational Report
- CCDSS 355.0-B-2
  Space Data Link Security Protocol, Recommended Standard
- CCDSS 355.1-B-1 –
  Space Data Link Security Protocol - Extended Procedures, Recommended St
- CCDSS 352.0-B-2 –
  Cryptographic Algorithms, Recommended Standard
- ECSS-E-ST-80C –
  Space engineering – Security in space systems lifecycles (1 July 2024)



Cybersecurity is needed, not a tax
Inter-operability & seamless integration vs zero-trust

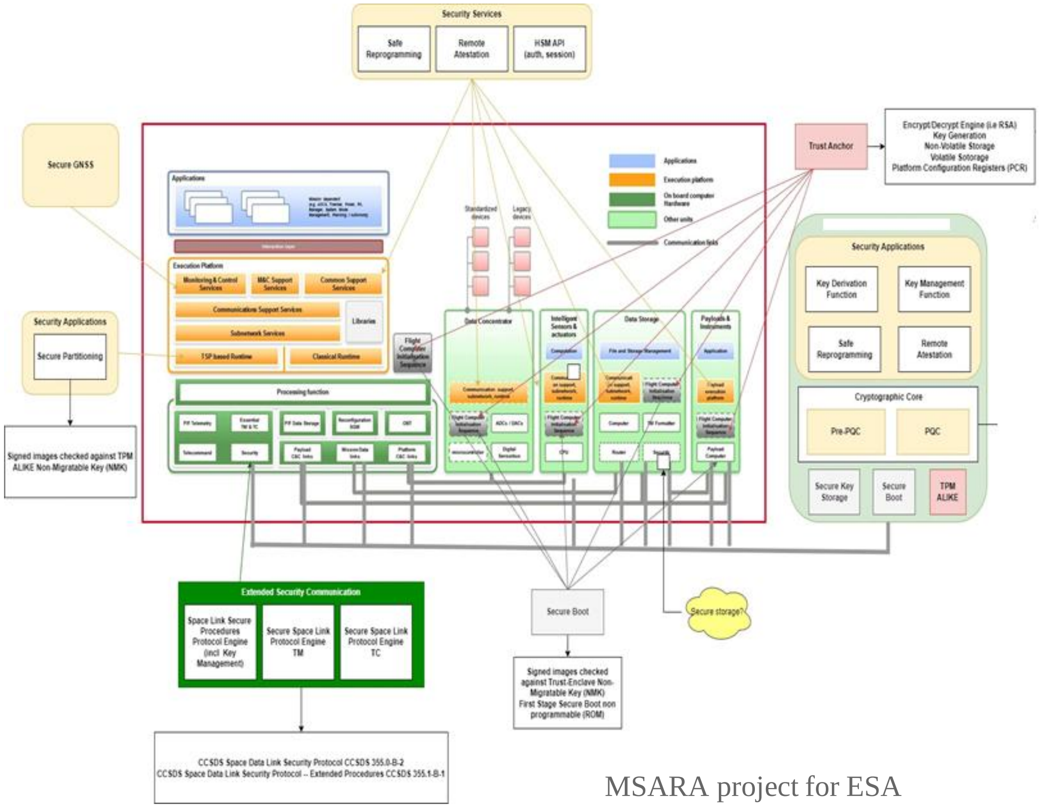
SECURITY SPACE REFERENCES AND STANDARDS

- CCSDS 350.1-G-3 –
  Security Threats Against Space Missions, Informational Report
- CCSDS 355.0-B-2
  Space Data Link Security Protocol, Recommended Standard
- CCSDS 355.1-B-1 –
  Space Data Link Security Protocol - Extended Procedures, Recommended St
- CCSDS 352.0-B-2 –
  Cryptographic Algorithms, Recommended Standard
- ECSS-E-ST-80C –
  Space engineering – Security in space systems lifecycles (1 July 2024)


Applications
Mission dependent (e.g. AOCS, Thermal, Power, P/L Manager, System Mode Management, Planning / Autonomy)
Interaction layer
Execution Platform
Monitoring & Control Services
M&C Support Services
Common Support Services
Communications Support Services
Libraries
Subnetwork Services
TSP based Runtime
Classical Runtime
Flight Computer Initialisation Sequence
Processing function
P/F Telemetry
Essential TM & TC
P/F Data Storage
Reconfiguration SGM
OBT
Telecommand
Security
Payload C&C links
Mission Data links
Platform C&C links
Standardized devices
Legacy devices
Data Concentrator
Communication support, subnetwork, runtime
Flight Computer Initialisation Sequence
ADCs / DACs
microcontroller
Digital Sensorbus
Intelligent Sensors & actuators
Computation
Communication support, subnetwork, runtime
Flight Computer Initialisation Sequence
CPU
Data Storage
File and Storage Management
Communication support, subnetwork, runtime
Flight Computer Initialisation Sequence
Computer
TM Formatter
Router
Security
Payloads & Instruments
Application
Payload execution platform
Flight Computer Initialisation Sequence
Payload Computer
Applications
Execution platform
On board computer Hardware
Other units
Communication links

Cybersecurity is needed, not a tax
Inter-operability & seamless integration vs zero-trust

GMV VIEW ON AVIONICS & SECURITY FUNCTIONS



MSARA project for ESA

- ·Authentication, Encryption/Decryption, Integrity
- Key Management
  (Generation, Distribution/Negotiation, Usage, Renewal)
  Perfect Forward Secrecy
- Secure key storage in volatile and non-volatile memory.
- ·Platform Configuration Registers (PCRs) store current state of the hardware and/or software of the system.
- ·Cryptographic engines (pre-PQC, quantum-resistant, PQC).
- ·A True random number generator.
- Partitioning/Isolation: Trusted Execution Environment (TEE)
- Anomaly Detection, Isolation and Recovery

SECURITY IN SPACE ASSETS

Advance Capabilities in Cryptography to ensure

Quantum Safe Capabilities – PQC

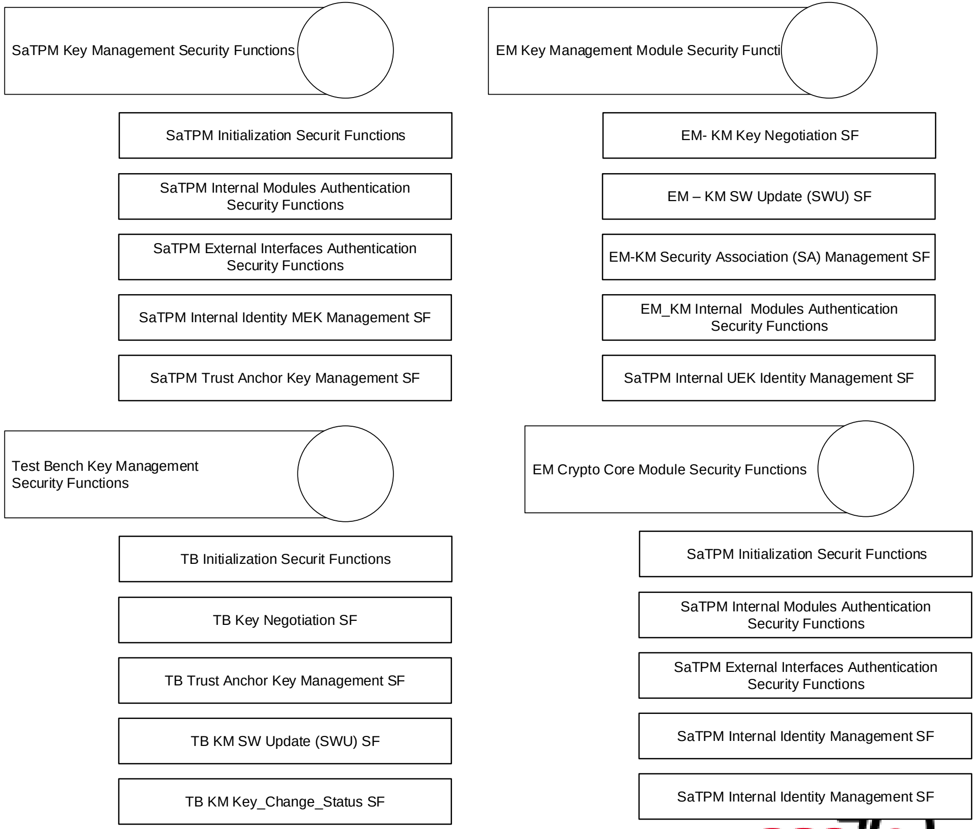
Advance and complete Set of Security Functions to support :

- whole life Satellite Manufacturing Supply Chain

- Informational and operational Mission lifecycle Security requirements

- Enforce the own Satellite Operational and functional Security requirements

Ensure Enhanced key Management with Ground Segment and between SSU end enforce PFS in Communications Space Protocols



SaTPM Key Management Security Functions

SaTPM Initialization Securit Functions

SaTPM Internal Modules Authentication Security Functions

SaTPM External Interfaces Authentication Security Functions

SaTPM Internal Identity MEK Management SF

SaTPM Trust Anchor Key Management SF

EM Key Management Module Security Functi

EM- KM Key Negotiation SF

EM – KM SW Update (SWU) SF

EM-KM Security Association (SA) Management SF

EM_KM Internal Modules Authentication Security Functions

SaTPM Internal UEK Identity Management SF

Test Bench Key Management Security Functions

TB Initialization Securit Functions

TB Key Negotiation SF

TB Trust Anchor Key Management SF

TB KM SW Update (SWU) SF

TB KM Key_Change_Status SF

EM Crypto Core Module Security Functions

SaTPM Initialization Securit Functions

SaTPM Internal Modules Authentication Security Functions

SaTPM External Interfaces Authentication Security Functions

SaTPM Internal Identity Management SF

SaTPM Internal Identity Management SF

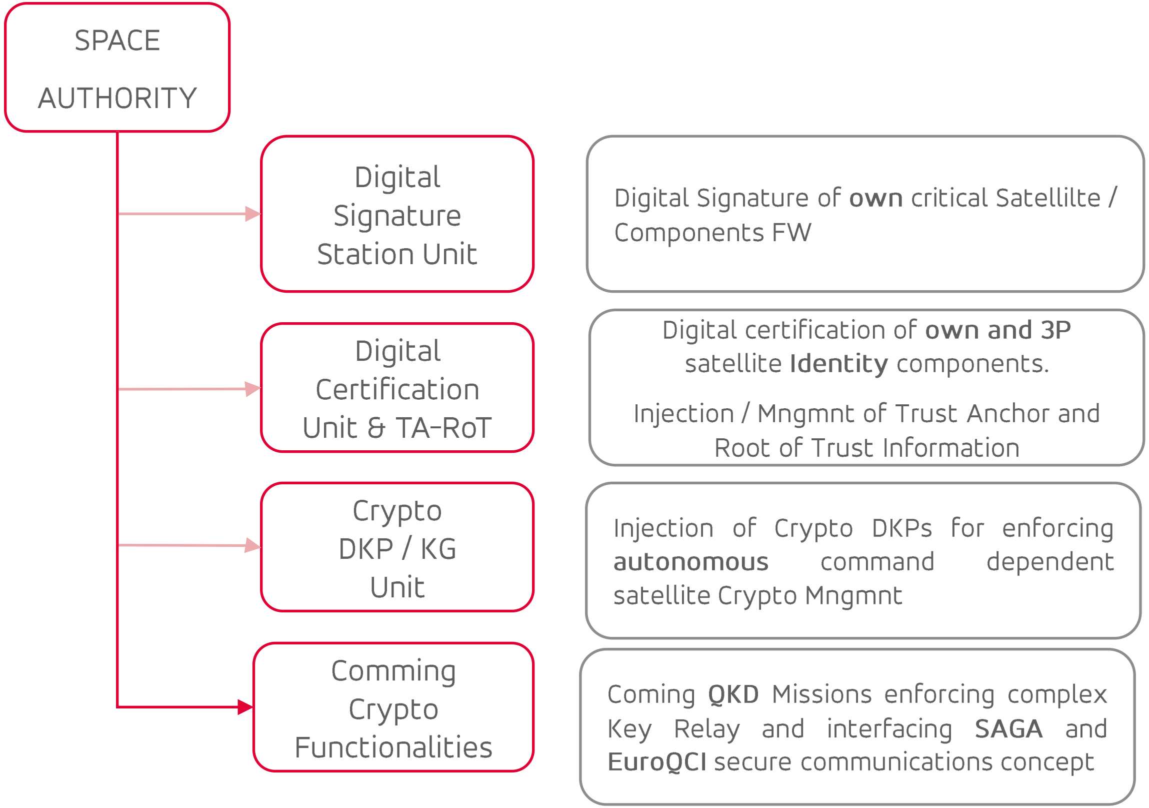
ESA/Integrators's Role

Space Authorities face increasing Cryptographic and Key Management complexities Trust Relations and defined Interfaces

SAVOIR architecture is a Key Security design element to ensure technical feasibility of advance Security functions in Space Segment (inter-satellite and ground centre) comms

- ESA as a SAT owner & certifier: shifting responsibilities.
- Critical space missions: Increased need for secure, resilient systems.
- Focus on standardization: Developing industry-wide security policies for avionics.

CRYPTOGRAPHIC AUTHORITIES and AUTOMATIC KEY MANAGEMENT FUNCTIONS



SPACE AUTHORITY

Digital Signature Station Unit

Digital Signature of **own** critical Satellilte / Components FW

Digital Certification Unit & TA-RoT

Digital certification of **own and 3P** satellite **Identity** components.

Injection / Mngmnt of Trust Anchor and Root of Trust Information

Crypto DKP / KG Unit

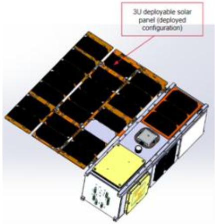
Injection of Crypto DKPs for enforcing **autonomous** command dependent satellite Crypto Mngmnt

Comming Crypto Functionalities

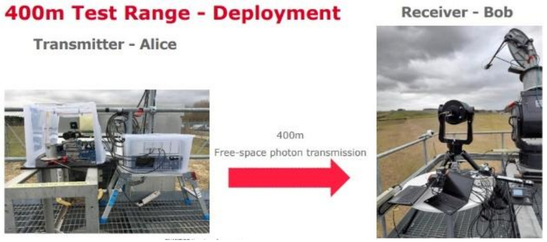
Coming **QKD** Missions enforcing complex Key Relay and interfacing **SAGA** and **EuroQCI** secure communications concept

CURRENT PROJECTS AT GMV

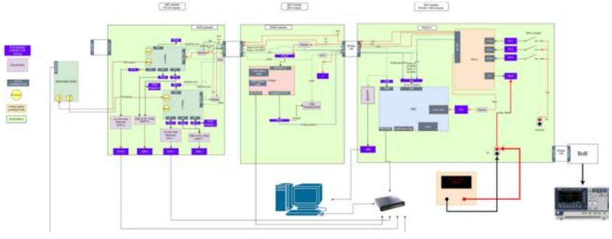
- CYBERCUBE: Security Laboratory Satellite platform on-board. End2end mission with ground control center, flatsat and 3U satellite in LEO orbit to be launched in October 2025



- Definition and specification of a Quantum Key Distribution (QKD) System Based on a Hosted Payload to be flown as piggyback on a Geostationary Satellite. CARAMUEL (+CARIOQA)



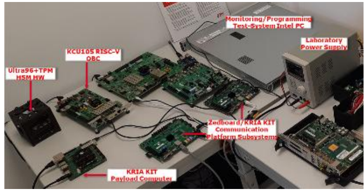
- NEALGALT on-board digital forensics flatsat-like modular avionics demonstrator including collection, monitoring, tag, hashes allowing post-incident forensic work



- GMV's role in Galileo control center security: Protection of European navigation infrastructure. Key management and secure communications for satellite control. Multi-layered security architecture for ground and space

- First phase for 4S system and services test bed. Basic core elements of incremental 4S System & Services Test Bed (4SSTB) to use in support of complex telecommunication systems and services design, verification and validation.

- TRUSTMOD HW-security Module on-board in representative avionics demonstrator with central node, TPM integration offering security to remote agents intra-satellite


Monitoring/Programming Test-System Intel PC
Laboratory Power Supply
KCU105 RISC-V OBC
Ultra96+TPM HSM MW
Zedboard/KRIA KIT Communication Platform Subsystems
KRIA KIT Payload Computer

Glad to get questions or coffee chats!

Thanks