Summary

- ESA: a Space Agency for Europe
- Some ESA missions
- Threats to space missions
- Countermeasures
- Tailoring countermeasures to missions
- Examples
ESA
The European Space Agency

- ESA is an International Organization with the purpose of promoting space research and new technologies and their applications in space, for peaceful purposes.
- ESA is present with its installations in the whole world, but concentrated mainly in Europe:
  - 30 sites interconnected by the ESACOM Wide Area Network
  - 4000+ users on line
  - Extreme variety in usage: Managers, scientists, technicians, administrators, astronauts, politicians, citizens, ...
- ESA designs and implements space missions.
- ESA operates space missions, or transfers them to other operators (e.g., Eumetsat, Eutelsat, ...)
- High degree of interactions with external partners:
  - National Space Agencies/Offices (CNES, DLR, ASI, etc.,..)
  - European Space Industry (EADS, Thales-Alenia Space, etc.,..)
  - International Space Agencies (NASA, CSA, RKA, JAXA)
ESA
European Space Agency

17 Member States

- Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxemburg, Norway, Netherlands, Portugal, Spain, Sweden, Switzerland, United Kingdom.
- Takes part in the definition of the European Space Policy and implements it
- Carries out space programs (and operates some)
ESA world locations
ESA programmes

All Member States participate, based on GNP, in a common set of programmes related to Space Science: mandatory programmes.

In addition, members chose the level of participation in optional programmes:

- Human spaceflight and exploration
  - Microgravity
  - Earth observation
  - Telecommunications
  - Satellite navigation
  - Launcher development
Space: a basic element for the security of the European Citizens

- Space missions have a value that returns to the European Citizens
- Citizens’ lives can be improved by space contributions
- Focus on new needs for security after 9/11
- The security elements of the Frame Program 7 and the European Security and Defence Policy can be supported and complemented by space missions
- In turn, the European Space Policy includes defence-security aspects
- Synergy among civilian and military activities, terrestrial and space-based, with data of different security classification levels
- Key infrastructures providing access to and from space must be protected
- In the EPCIP (European Programme for Critical Infrastructure Protection) directive, Space is considered among Europe’s critical infrastructures
Some of the current ESA missions

- Venus Express
- Mars Express
- Rosetta
- Stazione Spaziale (ISS): ATV & Columbus
Using radar to observe the Earth and its dynamics: ERS & ENVISAT
Missions focussed on Security: Galileo - Satellite Navigation "Made in Europe"

- A new navigation system under European control, developed by ESA and the European Commission

- 30 satellites on three circular orbits, inclined 56° at the Equator, at an altitude of 23,222 km

- To offer to Europe and the world accurate and secure positioning, with various levels of precision

- Users access defined and controlled by EU Institutions and Member States Governments, through an appropriate key management scheme

- Potential applications under consideration: Internal security, law enforcement, customs, critical transports, air and sea navigation, energy, telecommunications, emergency services, defence
# Galileo Services for Europe

<table>
<thead>
<tr>
<th>Service</th>
<th>Receiver</th>
<th>Benefits</th>
<th>Target user groups</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open Service</strong></td>
<td>OS</td>
<td><strong>Single frequency</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Additional satellites for better multi-system coverage (e.g., deep urban)</td>
<td>Low end mass market (e.g., LBS, outdoor)</td>
<td>Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Coding and modulation advances for increased sensitivity and multi-path mitigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Pilot signal for fast acquisition</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Double frequency</strong></td>
<td>High end mass market (e.g., car navigation, maritime)</td>
<td>Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As above + increased accuracy with 2nd frequency</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Commercial Service</strong></td>
<td>CS</td>
<td><strong>Double frequency</strong></td>
<td>Professional markets (e.g., surveying, precision agriculture)</td>
<td>Commercial basis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Increased accuracy using additional frequencies and signals</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Additional features under investigation (e.g., data rate capacity)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Safety of Life Service</strong></td>
<td>SoL</td>
<td><strong>Single frequency (Level B)</strong></td>
<td>Aviation (en route)</td>
<td>Certified receivers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As OS +</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Integrity and authentication of signal</td>
<td>Aviation (A)</td>
<td>Certified receivers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Continuity and service guaranty</td>
<td>Maritime (C)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Double frequency (Level A and C)</strong></td>
<td>Road, Train (A)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As above at higher performance levels suitable for stringent dynamic conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Public Regulated Service</strong></td>
<td>PRS</td>
<td><strong>Dual frequency</strong></td>
<td>Law enforcement</td>
<td>Regulated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As OS +</td>
<td>Strategic infrastructure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- High Continuity (in times of crisis)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Improved Robustness (vs jamming, spoofing)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Search and rescue</strong></td>
<td>SAR</td>
<td><strong>Single frequency</strong></td>
<td>Emergencies</td>
<td>Certified &amp; registered beacons</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Almost instantaneous reception of emergency calls</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Exact positioning of emergency beacon</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: European Commission
GMES – Global Monitoring for the Environment and Security

GMES aims at developing operational services,

... following the example of meteorology...

... but for other domains such as emergency management, air quality monitoring, land monitoring, ocean & sea ice monitoring, etc.

New Science is needed to create and continuously improve operational services
As part of its contribution to the GMES initiative, ESA is currently developing three different Satellites (“Sentinels”), each one in support of a dedicated mission:

- Sentinel 1 – SAR imaging
  - All weather, day/night applications, interferometry

- Sentinel 2 – Multispectral imaging
  - Land applications: urban, forest, agriculture, etc
  - Continuity of Landsat, SPOT data

- Sentinel 3 – Ocean and global land monitoring
  - Wide-swath ocean color, vegetation, sea/land surface temperature, altimetry

The definition of two additional missions (Sentinel-4 and 5) is on-going.
A typical Space Mission

- Space Elements
- Up/Down link
- System/Network
- Data dissemination
- Ground segment
- TeleCommands (TC)
- House-Keeping Telemetry (HKTM)
- Payload Data
- Control
- Users
Tailoring measures to threats: risk assessment

When considering the security needs of a mission, the following elements must be defined:

- Security Policy
- Security Interconnection Policy
- Mission Security Threat Assessment
- Mission Security Architecture
- Security Operating Procedures (SecOps)
Security Policy

☐ The mission security policy must be compliant with any higher level agency security policies but must clearly state:
  ➢ The classification and therefore level of protection of all the information, associated with the mission, both live and archive, telemetry, telecommand and ground systems.
  ➢ The roles of those who have access to the system.
  ➢ The integrity requirements of the system.
  ➢ The availability requirements of the system.

☐ The mission Security Interconnection Policy must clearly state:
  ➢ Which organisations will be allowed to interconnect to fulfil the mission
  ➢ The type of connections that will be made, e.g. continuous or intermittent.
  ➢ The interface of these connections, dedicated link, or Internet or dial up
  ➢ The classification of the information going over those links.
Threat assessment

- The threat assessment needs to consider the type of the mission and what the information security threats are to that mission. It is important to consider all parts of the mission architecture during all phases of the mission as the threat profile to the mission will change as the mission progresses.

- It should be noted that the Threat assessment will use the outputs of the Security Policy and Security Interconnection documents to help identify attack vectors and the value of the data and assets to be protected.
Threats to a typical Space Mission

- Space Elements
  - Space Debris
  - Hardware Failure
  - Uplink Jamming
  - TC Replay/Counterfeition
  - HKTM or Payload interception

- System/Network
  - Interception of Data (Theft/hacking)
  - Social Engineering
  - Unauthorised Access (Insider/Outsider)

- Software Threats

- Control

- Users
Countermeasures and controls

Redundancy – Situational Awareness

Data Encryption

TC/TM Authentication
(authentication-confidentiality-integrity)

Key Management
Key Store on board – Key management for high rate data

End-to-end security: physical, personnel, infosec
## Analysis of threats and countermeasures 1/2

<table>
<thead>
<tr>
<th>Applicable Threats</th>
<th>Security Mechanisms to Counter Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data corruption</td>
<td>• Data integrity schemes (hashing, check values, digital signatures)</td>
</tr>
<tr>
<td></td>
<td>• Resilient hardware</td>
</tr>
<tr>
<td>Ground facility physical attack</td>
<td>• Guards</td>
</tr>
<tr>
<td></td>
<td>• Gates</td>
</tr>
<tr>
<td></td>
<td>• Access control</td>
</tr>
<tr>
<td>Interception</td>
<td>• COTS product use</td>
</tr>
<tr>
<td></td>
<td>• Protection of traffic via encryption, frequency hopping, spread spectrum</td>
</tr>
<tr>
<td></td>
<td>• Protection of archive &amp; distribution systems via encryption</td>
</tr>
<tr>
<td>Jamming</td>
<td>• Multiple uplink paths</td>
</tr>
<tr>
<td></td>
<td>• Multiple access points</td>
</tr>
<tr>
<td></td>
<td>• Frequency hopping, spread spectrum</td>
</tr>
<tr>
<td>Masquerade</td>
<td>• Strong authentication</td>
</tr>
<tr>
<td></td>
<td>• Access control scheme</td>
</tr>
<tr>
<td></td>
<td>• Vetting of staff</td>
</tr>
<tr>
<td></td>
<td>• No use of open networks</td>
</tr>
</tbody>
</table>
## Analysis of threats and countermeasures 1/2

<table>
<thead>
<tr>
<th>Applicable Threats</th>
<th>Security Mechanisms to Counter Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replay</td>
<td>• Data integrity schemes (e.g., authenticated command counter, timestamps)</td>
</tr>
<tr>
<td>Software Threats</td>
<td>• Acceptance testing in simulated environment</td>
</tr>
<tr>
<td></td>
<td>• System evaluation (e.g., IVV, code analysis)</td>
</tr>
<tr>
<td></td>
<td>• COTS product use</td>
</tr>
<tr>
<td></td>
<td>• Continuous threat Monitoring, continuous risk management</td>
</tr>
<tr>
<td></td>
<td>• Auditing</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>• Encryption of TT&amp;C and mission data</td>
</tr>
<tr>
<td></td>
<td>• Authentication of commands</td>
</tr>
<tr>
<td></td>
<td>• No use of open networks</td>
</tr>
<tr>
<td></td>
<td>• Access control in control center</td>
</tr>
<tr>
<td></td>
<td>• Access control in cross support network</td>
</tr>
<tr>
<td></td>
<td>• Access control in control and dissemination systems</td>
</tr>
<tr>
<td></td>
<td>• Multiple access paths</td>
</tr>
<tr>
<td></td>
<td>• Auditing</td>
</tr>
</tbody>
</table>
The security architecture for the mission is the logical system design with a focus on security. It must be developed in step with the system architecture. The security architecture will shape how the system architecture is formed and will have to be developed and adapted as the system design matures to ensure that the mission goals will be achieved while keeping compliant to the Security Policy.

The Security Architecture will use the System Security Policy, the Security Interconnection Policy and the results of the Threat Assessment as inputs.

Never attempt to develop the security architecture after the system design has been developed! This will make it extremely difficult to produce a security compliant system, experience shows that changes will need to be made to the system design which will delay the project and increase costs considerably. Plan ahead!
TC/TM Security Solutions

- **Scenario 0: no specific security**
  - No TC authentication and encryption
  - No HKTM or science data encryption
  - Standard terrestrial links security (firewalls, etc)
  - Implemented in ERS/ENVISAT and Earth Explorers

- **Scenario 1: static TC protection**
  - TC authentication and anti-replay
  - Authentication key pre-loaded on board
  - TC authentication can be enabled/disabled automatically or by ground
  - Currently implemented on MetOp

- **Scenario 2: dynamic TC protection**
  - TC authentication and anti-replay
  - Authentication keys are loaded by ground using preinstalled Master Keys for the encryption of the related TCs
  - TC authentication can be enabled/disabled automatically or by ground
Scenario 3: dynamic TC + payload data protection

- Payload data is encrypted
- 4 types of keys: Master key, TC authentication key, payload data encryption key, TC encryption key
- Payload data encryption can be enabled/disabled automatically or by ground

Scenario 4: dynamic TC + payload + HKTM data protection

- HKTM data is encrypted
- 5 types of keys: Master key, TC authentication key, data encryption key, HKTM data encryption key, TC encryption key
- HKTM data encryption can be enabled/disabled automatically or by ground
The new ESA Security Context

- General increase of the attractiveness of space assets for good *and bad* citizens
  - Space organizations cannot afford to wait for the problems to happen to apply countermeasures: risk assessment (instead of crystal ball)
- The increased degree of interconnection of ground networks introduces new vulnerabilities in space missions
- The basic technology is increasingly available commercially - also bad people can obtain basic components
- Many of the new applications require a new approach to availability and reliability and data protection - Data classification systems
- The protection of the critical infrastructures is essential for the business continuity and the integrity of such high risk missions
- Need to be part of the overall European efforts for critical infrastructures