COMET 2019

Cyber Security lessons learnt on Operational System (RLSP: Return Link Service Provider - SAR Galileo Project)

Authors
Maxime FONTANIER - Stephane CHANOINE (CNES)
Olivier FURIO (SCASSI)

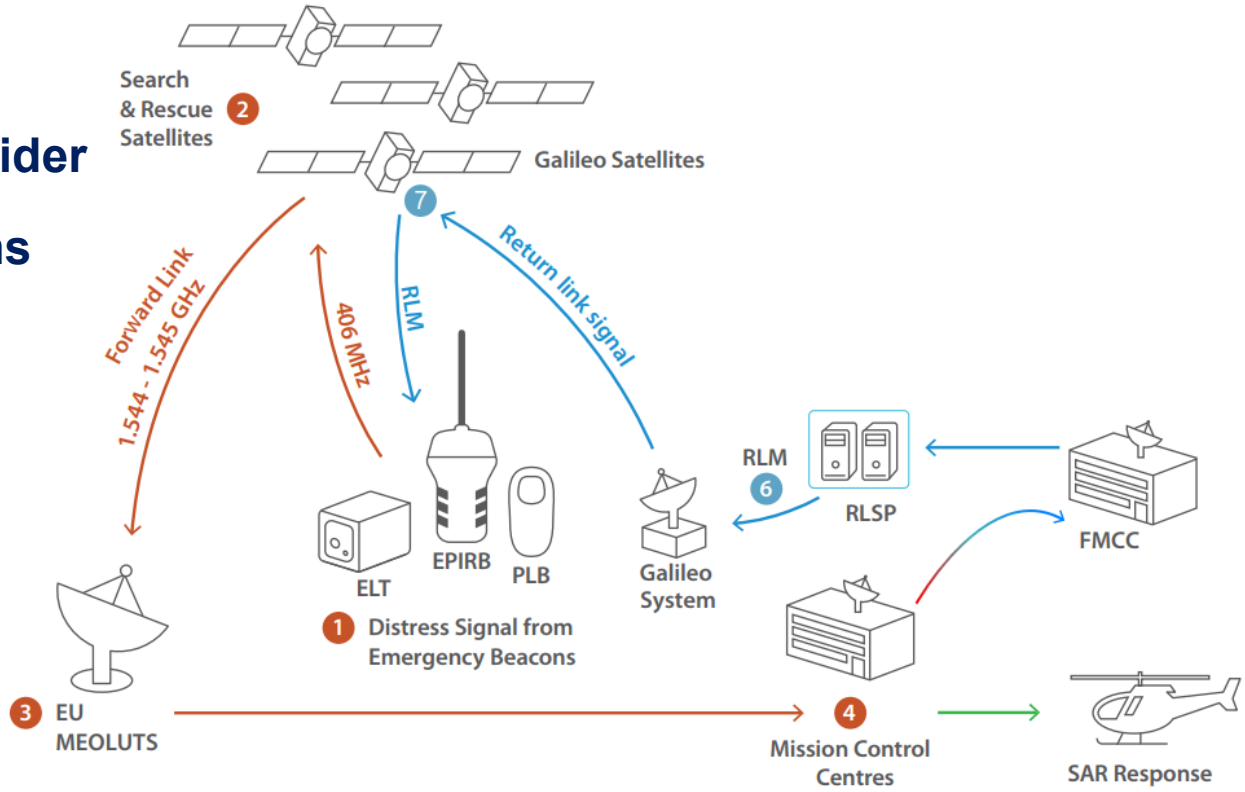
cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

AGENDA

- **SAR Galileo / RLSP Overview**
- **Cyber Security in the RLSP Accreditation process**
- **Impacts of Cyber Security on**
  - Service Infrastructure
  - Service Operations
  - Service Maintenance
  - Service Organization
- **Difficulties and Benefits**
- **Conclusion**

SAR GALILEO / RLSP OVERVIEW

- **RLSP: Return Link Service Provider**
- **Interface with two major Systems**
  1. Galileo Mission Segment
  2. Cospas / Sarsat Project
- **Availability target very high (99,95% i.e. less than 4 hours outage a year)**



CYBER SECURITY IN THE RLSP ACCREDITATION PROCESS

- **Communications with Galileo Segment imposes an high level of security in terms of:**
  - Software, Infrastructure, Operational Procedures, Hosting Site, Resources, … total of 1200 requirements at the beginning of the project
- **Meanwhile, a National cybersecurity strategy is led by ANSSI and by the ENISA for Europe**
- **In 2019, Cyber security rules (415 new requirements) have been applied on top of existing security measures to re-enforce:**
  - Service Infrastructure (275 requirements)
  - Service Operations (50 requirements)
  - Service Maintenance (50 requirements)
  - Service Organization (40 requirements)
- **The "Accreditation process" that grants the authorization to operate the System has been updated accordingly**

CYBER SECURITY OVERVIEW

- **Service Infrastructure (275 requirements)**
  - Hardening (software, network, hardware, logs), IDS – Intrusion Detection System
  - Vulnerability Assessment, Pen tests
  - Configuration control, Patching, Obsolescence
- **Service Operations (50 requirements)**
  - Control of Service Infrastructure solutions (Network map, Vulnerability report, patch)
  - Re-enforce the security monitoring
- **Service Maintenance (50 requirements)**
  - Solution implementation and security checks
- **Service Organization (40 requirements)**
  - Setup of the Cyber Security Team (profiles CIA and CSM)

CYBER on SERVICE INFRASTRUCTURE

- **RLSP manufacturer keeps a constant watch on technological developments in collaboration with CNES security team => vulnerability and obsolescence assessments**
- **Cyber security introduces COTS assessments on a more regular basis**
  - No more than 6 weeks to analyze the impact after a vulnerability publication
  - New classified documents to deliver to the contractual authorities, introducing latency in delivery process
- **Pen tests and external audits are performed on a regular basis on the Operational platform and have an impact on the platform**

CYBER on SERVICE OPERATIONS

- **Security incidents must be reported to the Authority:**
  - Monitoring tool is used by RLSP Operators to react quickly
  - Security Information and Event Management (SIEM) for analysis by Cyber Security team
- **Cyber Security is part of daily Operations**
  - All these tools are used by RLSP Operators on a daily basis
  - Security team is involved in Operational procedures writing
- **Impact of Cyber Management on Log Management**
  - Increase size, retention delay, verbosity

CYBER on SERVICE MAINTENANCE

- **With Cyber requirements, the upgrade frequency is higher but Operators rely on automated tools to validate the RLSP main functionalities:**
  - Simulators and automated tests have been industrialized to automate the tests campaign and mitigate the impact on platform availabilities
  - Non regression tests are run automatically before each Software upgrade or patch on OPE platform
- **Impact of Cyber on Maintenance**
  - Extra workload of RLSP Operational team and Security teams to perform
    - Security and Operational assessment performed for each upgrade
    - Operational procedures updates on a more regular basis
  - Impact of platform availability
    - AIV platform used to mitigate the risk

CYBER on SECURITY ORGANIZATION

- **Security organization (on duty) has been put in place to support Operators in case of security incident**
- **New roles Cyber Security Manager (CSM) and Cyber Internal Auditor (CIA) in addition to existing security function as SIO, SSO**
- **Cyber team is part of the RLSP project and is fully integrated with RLSP Operational team, meaning that they:**
  - Follow the tests campaigns, Assist to the progress meeting, involved in Operational procedures, Train Operators
  - Synergies have been emphasis between Security and Operational actors
- **In addition, a dedicated channel has been established with:**
  - CNES Security Officers
  - GSA Accreditation and Cyber teams

DIFFICULTIES

- **Sometimes it is difficult to clearly state roles and responsibilities between security and operational teams**
  - i.e. password management, firewall/antivirus upgrades and monitoring
- **Daily activities more restrictive, i.e. user management, credentials, timeout sessions, storage media**
- **Communications process with external partners for Ops**

=> Issues managed with more precise and various Operational procedures

BENEFITS

- **Due to the proximity with Cyber Security team:**
  - The RLSP Operators are more awareness with security procedures and Cyber threat
  - Security Incident are raised faster and more easily
  - Relationships between security and operational actors have significantly be improved
- **Security procedure are more practical and understandable by Operators**

CONCLUSION

- **The introduction of Cyber requirements during the development phase has been facilitated because:**
  - High level of Security was already taken into account since the beginning of the RLSP project
  - European and National authorities strongly recommend to apply a Cyber Security policy
  - Synergies between Operational and Cyber teams were found

QUESTIONS