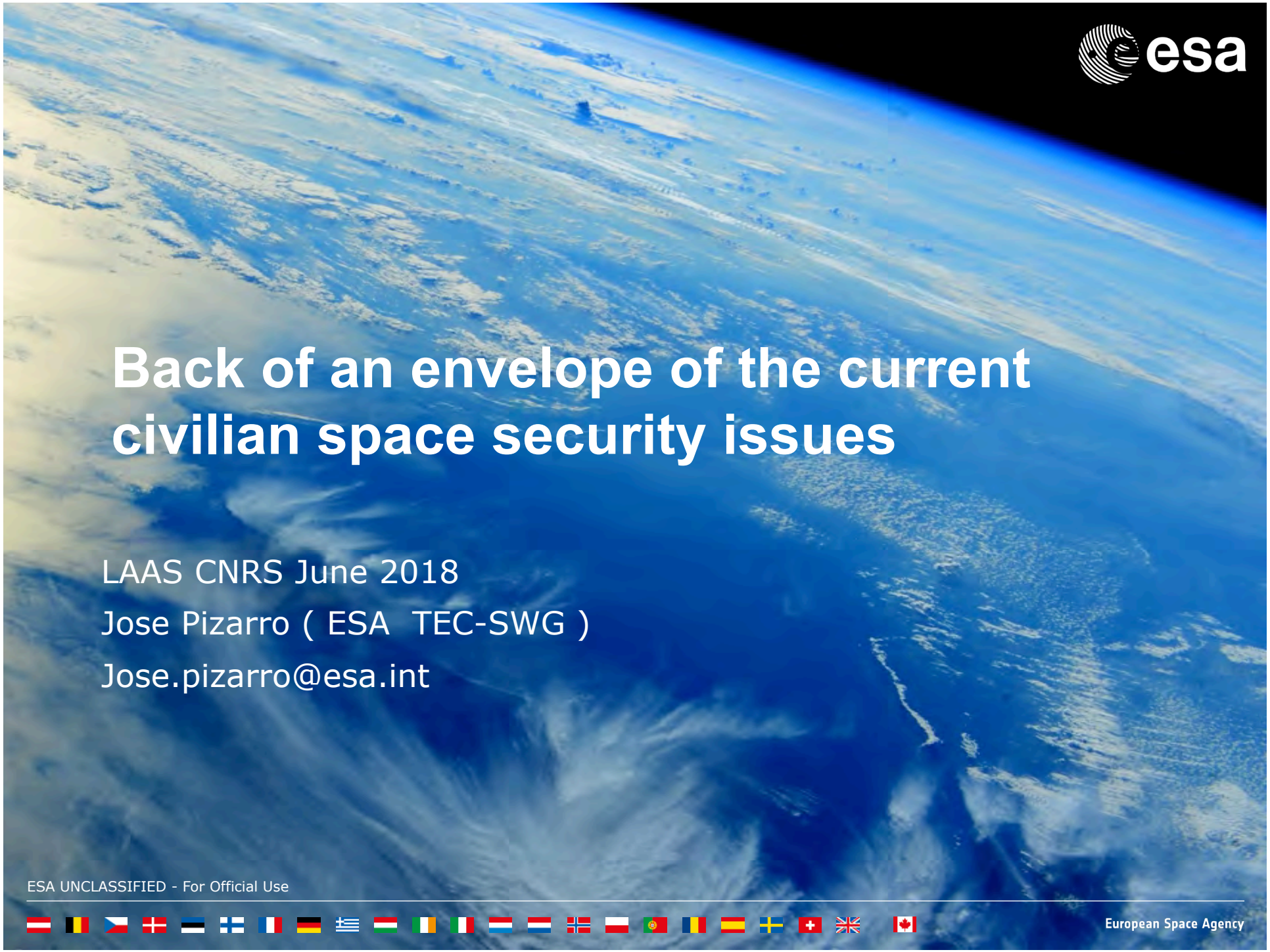


Back of an envelope of the current civilian space security issues

LAAS CNRS June 2018

Jose Pizarro (ESA TEC-SWG)

Jose.pizarro@esa.int

ESA UNCLASSIFIED - For Official Use

Overview

SPACE implementation of security
•Current state of play
•Today's Issues
•Future challenges
DOWN-LINK
UPLINK
GROUND LINK
SVP
Sécurité et Vie Privée
Objectifs :
Partenaires :
Coordinateur :

Security concerns in the world today

Current status in SPACE
What are the current issues?

Conservative (inflexible) Culture

Change measured in years

- Hardware
- Software
- Procedures
- Contracts

Current status in SPACE
What are the current issues?

Young or no security culture in Civilian SPACE

- Commercial
- Science

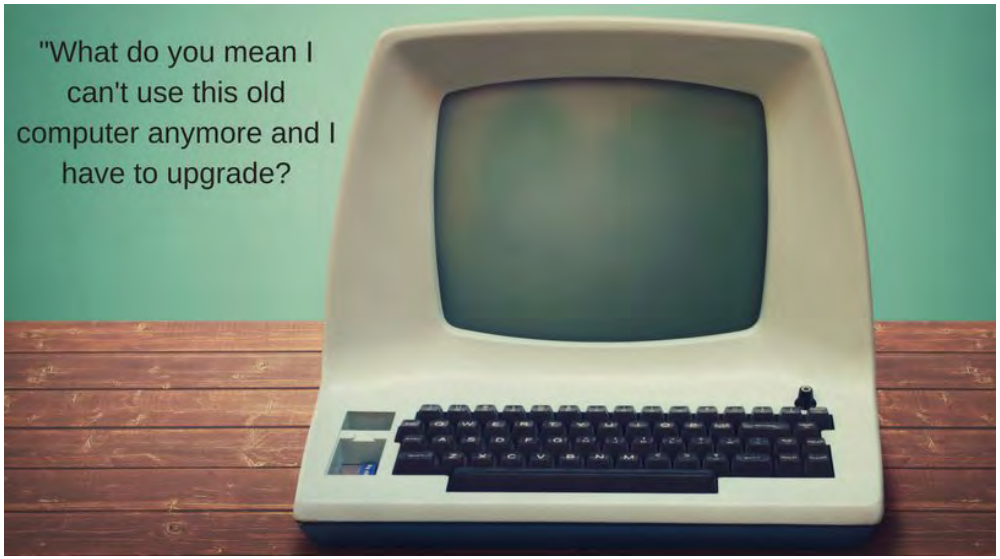
Current status in SPACE
What are the current issues?

- SECURITY IS AN AFTER THOUGHT
- Requirements placed in later stage of program
- Attached on top of the system (not in design)

Current status in SPACE
What are the issues?: Patching

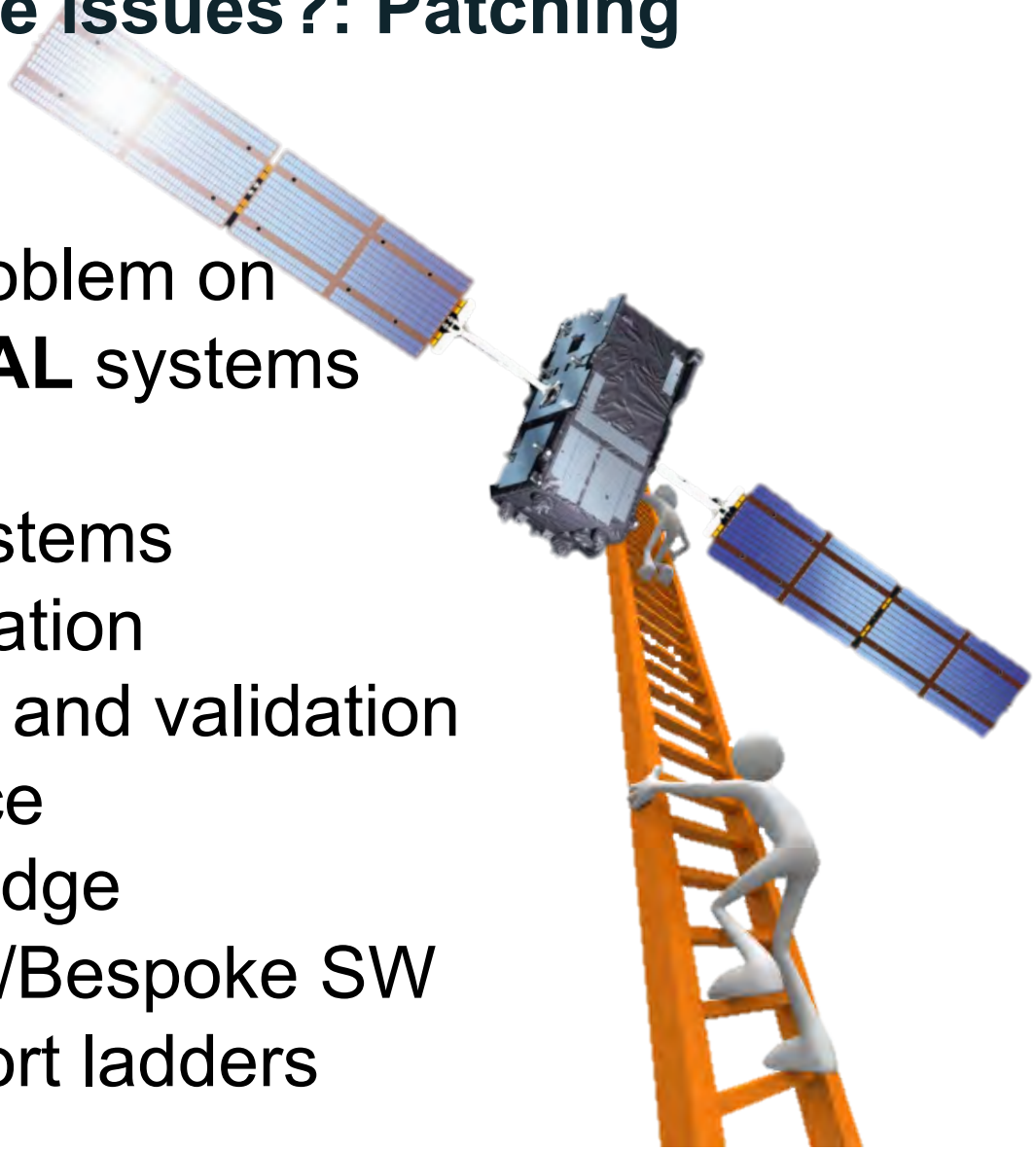
Patching a problem on **OPERATIONAL** systems

- -On ground
  - -Old Systems
  - -Certification
  - -Testing and validation



©https://www.intivix.com/7-big-problems-with-legacy-systems-that-everyone-should-understand/

Current status in SPACE
What are the issues?: Patching



Patching a problem on **OPERATIONAL** systems

- -In Space
  - -Old Systems
  - -Certification
  - -Testing and validation
  - -Distance
  - -Knowledge
  - -Legacy/Bespoke SW
  - -Too short ladders

How do we manage currently in SPACE

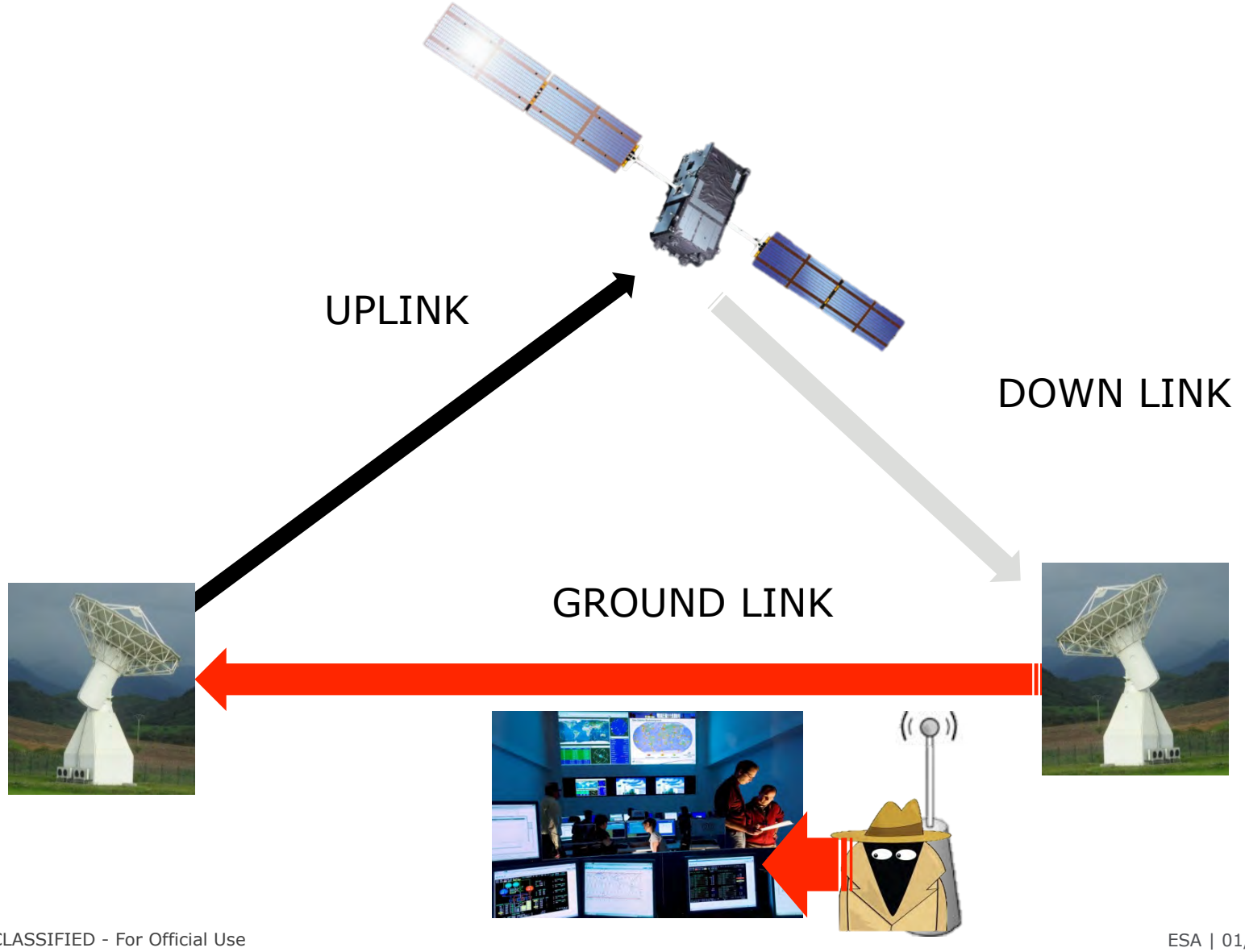
- Hardening CCSDS + TM (Packets and Telemetrv)

- Early SpaceOps in clear mode as lack of experience with encrypted TM

- Simplified Secure OPS

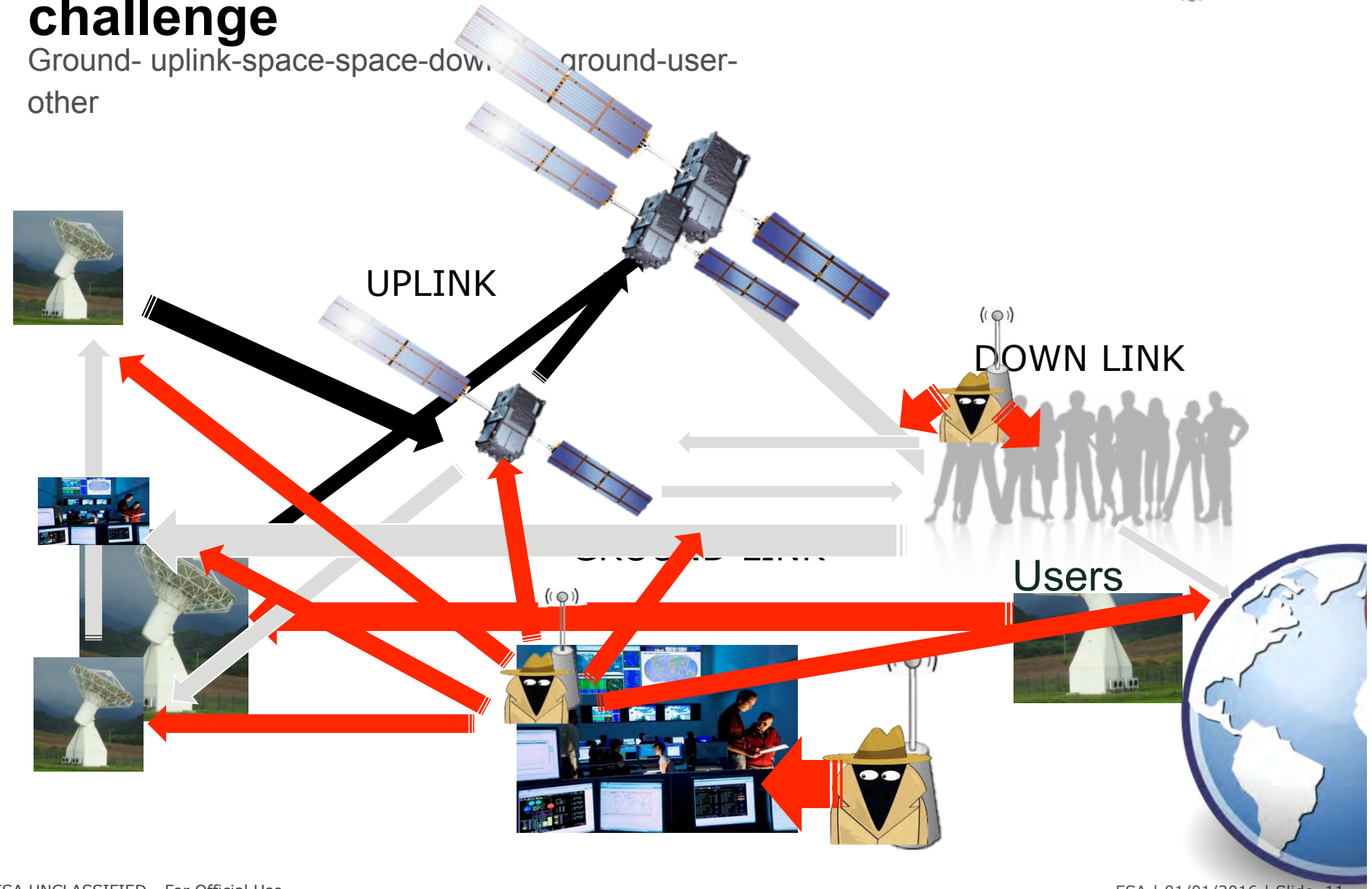
- Secure ground stations and systems

SPACE SECURITY – Traditional triangle



SPACE SECURITY– New ~~triangle~~ err challenge

Ground- uplink-space-space-dow[illegible]ground-user-other



SPACE SECURITY– CHALLENGES : GENERAL

- Configuration management
  - HW/SW
  - Documentation
- Testing
  - Full testing and not just to contract
- VULN management
  - Identify vulnerabilities
  - Which version fixes what
  - How to update

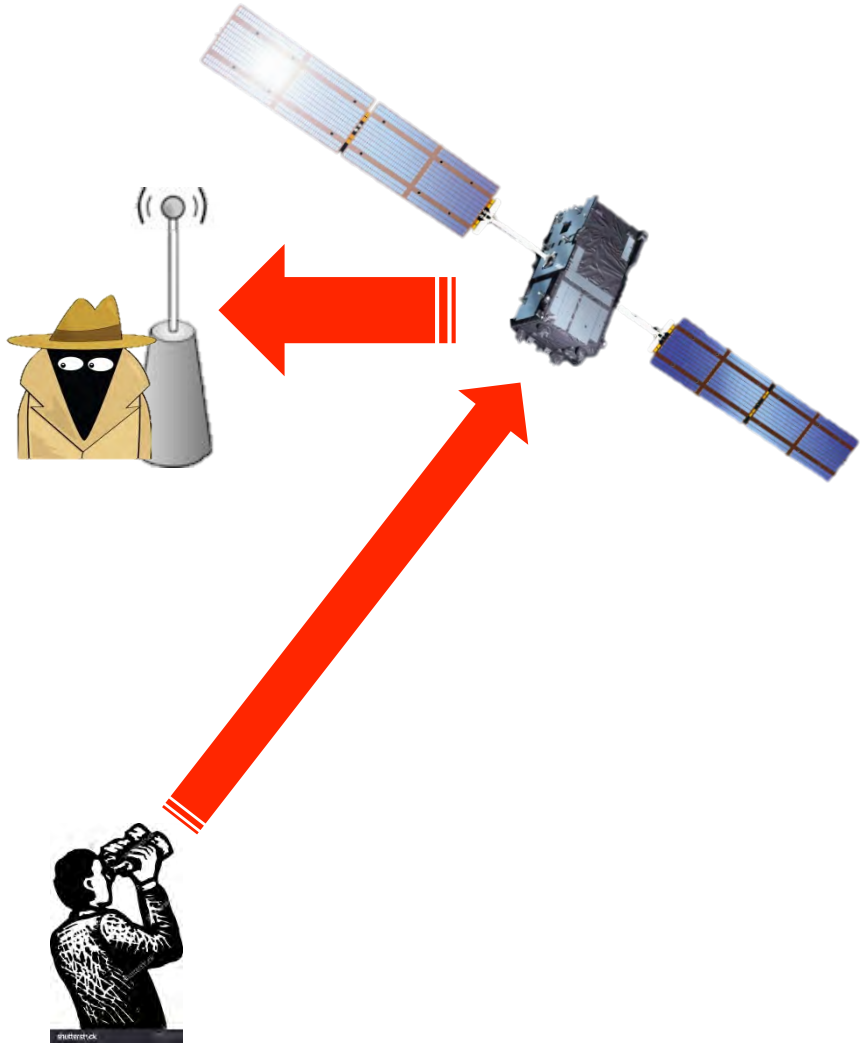
SPACE SECURITY– CHALLENGES : DATA TRAFFIC

- Ground and Space becomes blurred as applications become more distributed

- Data centres
  - Ground segments
  - User Segments
  - Public Service centres (Internet interfaces etc.)

SPACE SECURITY– CHALLENGES : SPACE SEGMENT

- Securing a remote asset from
  - SigInt
    - Uplink
    - Downlink
    - Inter-satellite
  - Physical inspection
  - Visual inspection



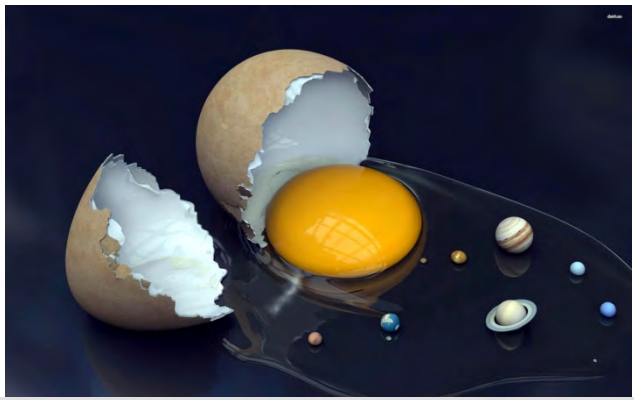
SPACE SECURITY– CHALLENGES : Externals

- Distributed Nature
  - processing on board vs processing on ground or both
- Quantum
  - Entanglement
  - Cryptography
- International partners
  - Distributed teams and Comms

SPACE SECURITY– WHY and WHAT -PR

Public Relations

- Systems could be used to attack other entities
- Possible attack vectors
  - Social
  - Technical
    - Network
    - Interfaces to public & partners



ESA UNCLASSIFIED - For Official Use

SPACE SECURITY– WHY and WHAT :CIAA

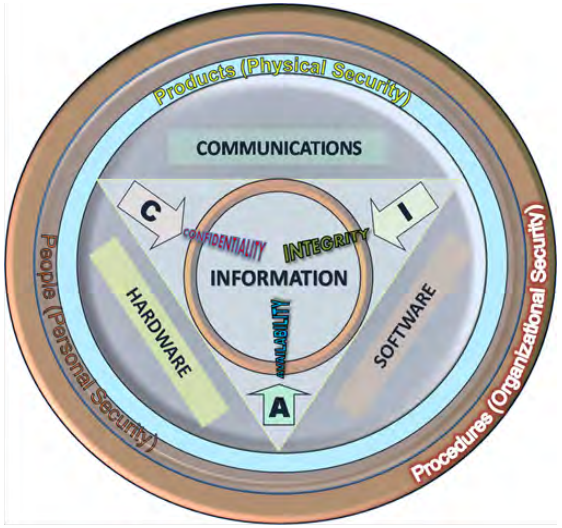
Confidentiality, Integrity and Availability

Accountability

Need to protect against misuse of the systems

Spacecraft & Ground

- SW - data
- HW - chips
- Design “features”



[1] John M. Kennedy; http://commons.wikipedia.org/wiki/File:CIAJMK1209.png; permission granted to copy, distribute, and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.

SPACE SECURITY– HOW to start to REMEDY

- Security audits
- Pen testing
- ISO 27001
- Return to basics
- Knowledge
- Highly Trained engineers & operators

SPACE SECURITY– Current Best Practice

- TM and TC checks
- Encrypted TM after clear operations
- Certification of components and systems
- Protect ground systems
  - Configuration Hardening
  - OS and SW updates
  - Anti Virus/Malware
  - Monitoring changes and events

SPACE SECURITY– Current Best Practice (DESIRED)

Return to Basics

- Robust code
- Defensive programming
- Defensive design
- Defence in depth (Multi-Layer)

SPACE SECURITY– Current Best Practice (DESIRED)

Penetration testing of systems

- in simulated cyber range
- in factory
- in space

SPACE SECURITY– FUTURE ISSUES

- More users have access and communicate with space assets

- Space = Infrastructure and Economy

- Space will be/is a disruptive technology in all market places

SPACE SECURITY– FUTURE NETWORKS

Distributed Delayed Networks

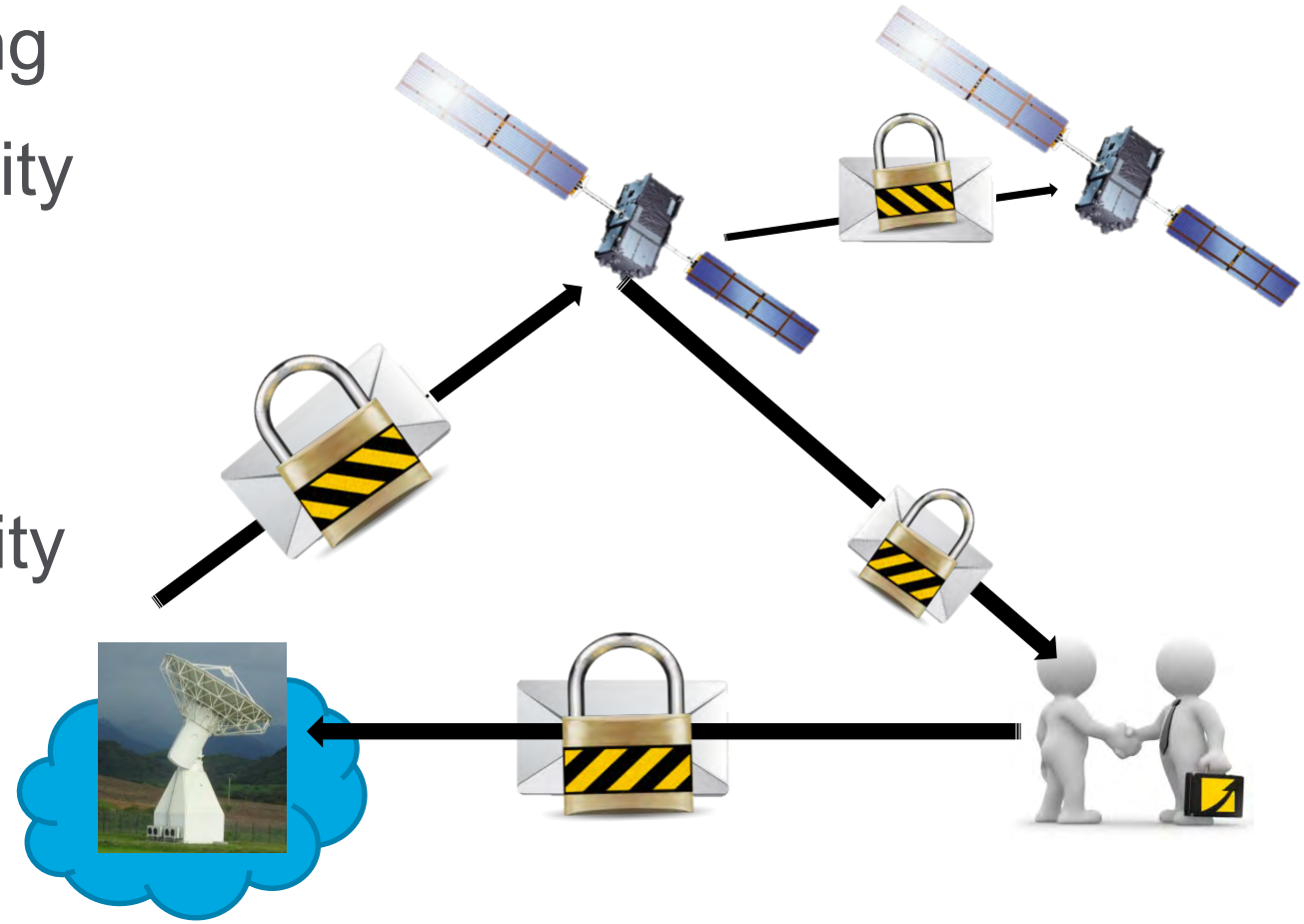
- Moon
- Mars
- Deep Space Inter-planetary

SPACE SECURITY– FUTURE ISSUES

- Block chain/ledger on all TC to provide an audit trail ??
- QUANTUM
  - quantum entanglement for integrity / authentication
  - use of qubits
- Use of CRYPTO
  - Traditional
  - Quantum
  - Quantum proof crypto
  - Encrypted Operations

SPACE SECURITY– FUTURE NEED Summary

- Anti Jamming
- Anti Spoofing
- Confidentiality
- Integrity
- Availability
- Accountability



ESA UNCLASSIFIED - For Official Use

TAKE HOME - SPACE SECURITY

PARANOIA & AWARENESS

- Security By Design
  - Assume your system will be compromised before you even design it and compensate
  - Self protective nodes
- System Integrity
  - Can the you continue the mission and the information still have integrity even with a compromised system?
- Operations and Training
  - Operate as if the system is compromised in nominal situations

ESA UNCLASSIFIED - For Official Use

TAKE HOME - SPACE SECURITY

LEGACY SYSTEMS: PARANOIA

Future Systems:

Build security in at start also for “CIVILIAN & SCIENCE” Systems

ESA UNCLASSIFIED - For Official Use

TAKE HOME - SPACE SECURITY

Knowledge

KNOW :
-What you have
-Why you have
-What you use
-Why you use
-Which open doors that you need to guard

ESA UNCLASSIFIED - For Official Use

TAKE HOME - SPACE SECURITY

REMEMBER

SECURITY FROM THE BEGINNING IS EASY

SECURITY LAST IS HARD

ESA UNCLASSIFIED - For Official Use

Activities

Ongoing:

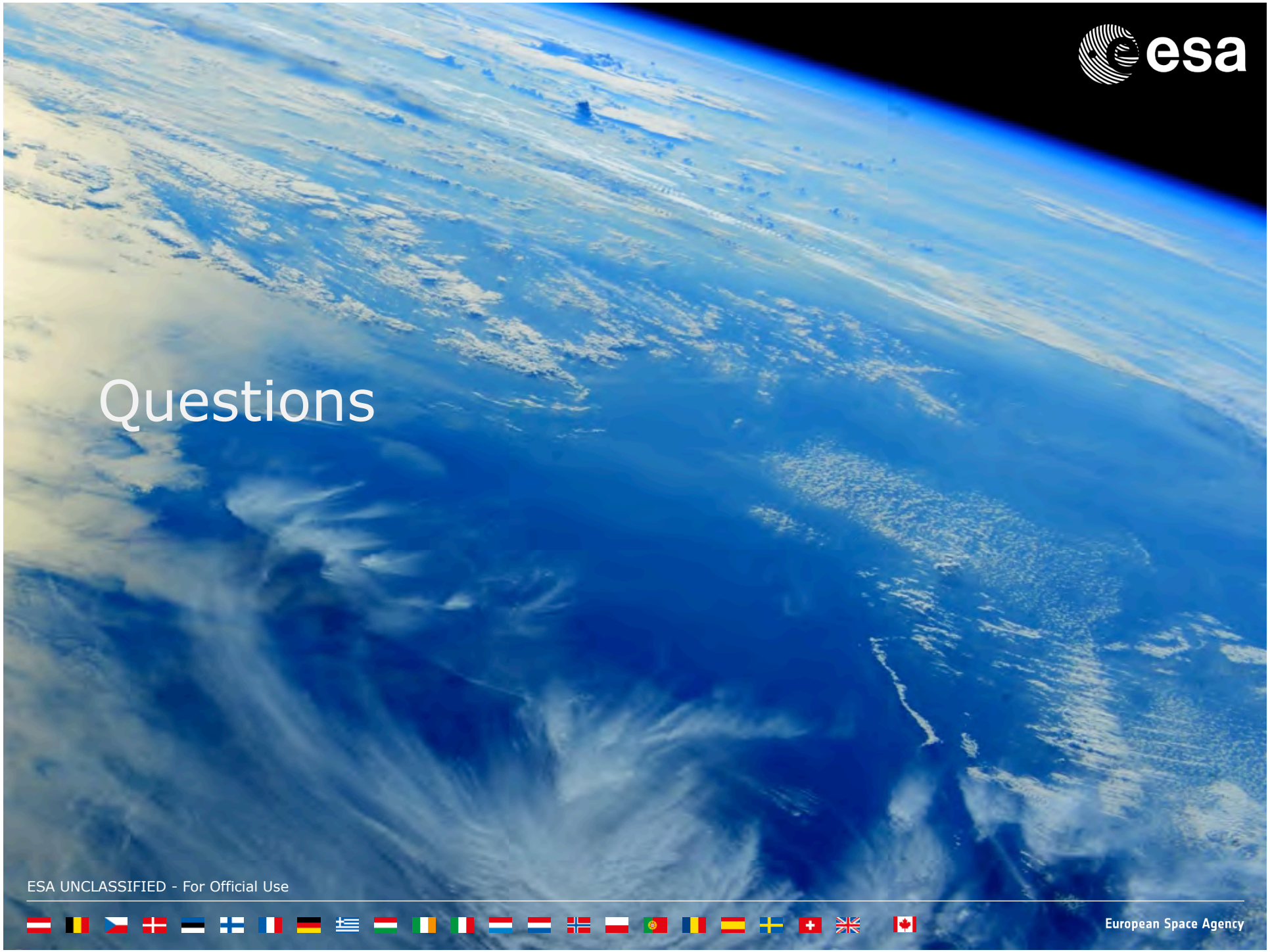
- GSP *"Innovative Security Concepts, Mechanisms and Architectures for Future Space Missions"*
- *TRP "Radio Frequency Interference Scenarios, Application Requirements and Counteraction Techniques"*
- TRP *"Authentication of GNSS Signals by Radio Signal Fingerprinting"*
- TRP *"Penetration Testing and Security Awareness Management in a BOX"*
- Third Party Program *"Generic Application Security Framework Evolution"*
- GSTP *"Space Link Security – Cryptographic Processor"*
- GSTP "Tools support to secure system and software engineering practices and security assurance"

Proposed:

- *GSTP "Flexible Space Data Link Layer Security Protocol implementation and End-to-End Verification"*
- *GSTP "Secure Systems Engineering for Space"*

Standardization:

- CCSDS
- ECSS



ESA UNCLASSIFIED - For Official Use

BACK-UP MATERIAL

Past activities and missions

ESA Missions

- Automated Transfer Vehicle
- MetOp
- GALILEO IOV/FOC
- Copernicus Sentinel-1, -2 and -3 satellites
- ARTES Telecommunication Missions

Telecommand protection (TAS and Airbus)

- SEOSAT
- EUMETSAT Meteosat Third Generation
- MetOp Second Generation
- EDRS / GlobeNet

ESA activities (selection)

"*Study on High Data Rate Encryption Systems for Future Earth Observation Platform Utilization*", Final Report, TN-ENS-IDA-002.

"*Encryption for Space, Present Scenario, Performance and Software Efficient Applications*", Final Report, July 2004.

"*Telecommand and Telemetry System Security Design Study(TT3S)*", D3.5 Final Report, DPAS.TN.11572.ASTR, Is. 2 Rev.0, 07.12.2007.

"*Telecommand and Telemetry System Security Design Study*", Final Report, TMTC-SEC-OHB-RP-016, Is. 1 Rev.0, 08.02.2008.

"Securely Partitioning Spacecraft Computing Resources", End date: May 2011.

"*Cryptographic Pseudo-noise Sequences and related Acquisition Techniques for Direct Sequence Spread Spectrum Transponders*", Final Report, RPT-RFP-ESA-00013-AASI, Is. 2, 13.09.2011.

"*Frequency Hopping Spread Spectrum System for TT&C and Payload Control links*", Final Report, TNO-PTLC-0012-TASI-SPSPTT&C, 19.09.2011.

"*Advanced Coding Schemes for Direct Sequence Spread Spectrum Telecommand Links*", Final Report, Vols. 1 and 2, 18.09.2013.

"Generic Application Security Framework", Final Report, DHSO-STU-TN-1012-HSO-GDA-i1r2, 2014.

"*Cryptographic Key Infrastructure for Security Services Protecting TT&C and Payload Links of Space Missions*", Final Report, NPI University of Waterloo (Canada), 2015.

"*Software Elements for Security - Partitioning Communication controller*", December 2015

"Secure Software Engineering Handbook", ESSB-HB-E-007, 2016.

"Secure Software Engineering Standard", ESSB-HB-E-008, 2016.

"Glossary of Secure Software Engineering Terms", ESSB-ST-E-009, 2016.

"*SatNEx IV Call of Order 1 Part 2 – Physical Layer Security*", 2017.

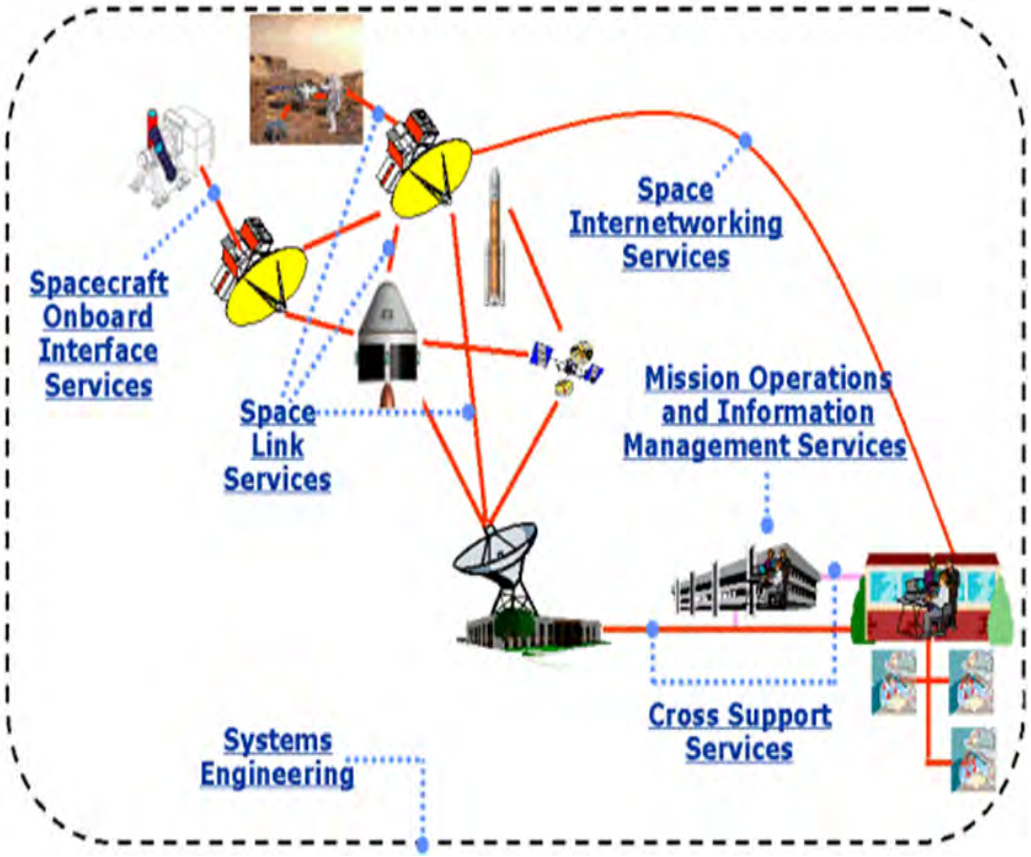
SPACE SECURITY– Current ESA Domains

- GNSS
  - Search and Rescue
  - Authentication and Positioning
- EGNOS
  - Air Traffic control
- ISS
  - Manned Space (lives)
  - Medical Data
  - Control Systems
- TT&C
- TIA(Telecommunications)
  - Communications
  - Privacy
- Corporate (ESA)
- Science
- Earth Observation
  - Sensitivity of the data
  - Outer space treaty implications

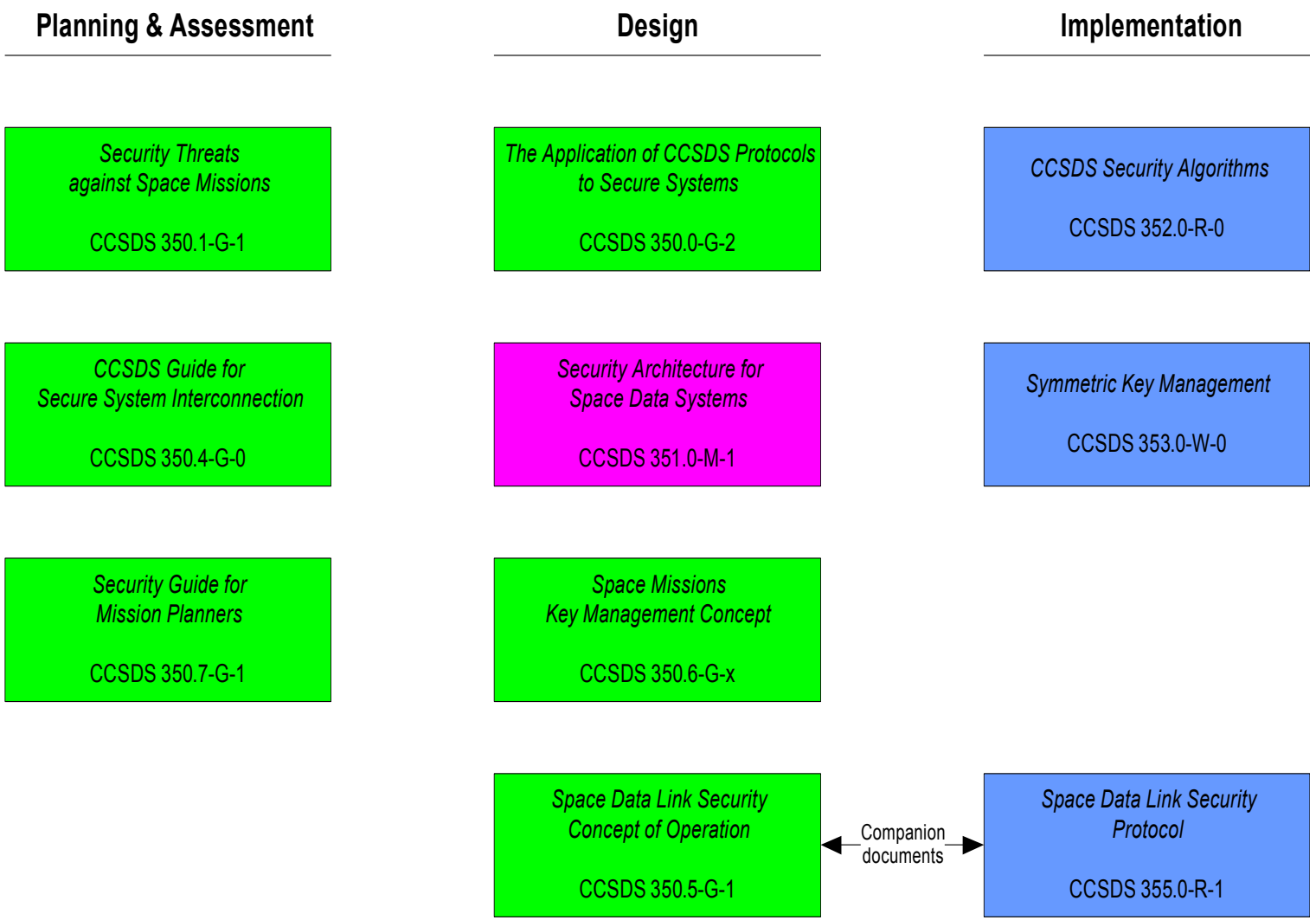
ETC ETC.

CCSDS

Consultative Committee for Space Data Systems

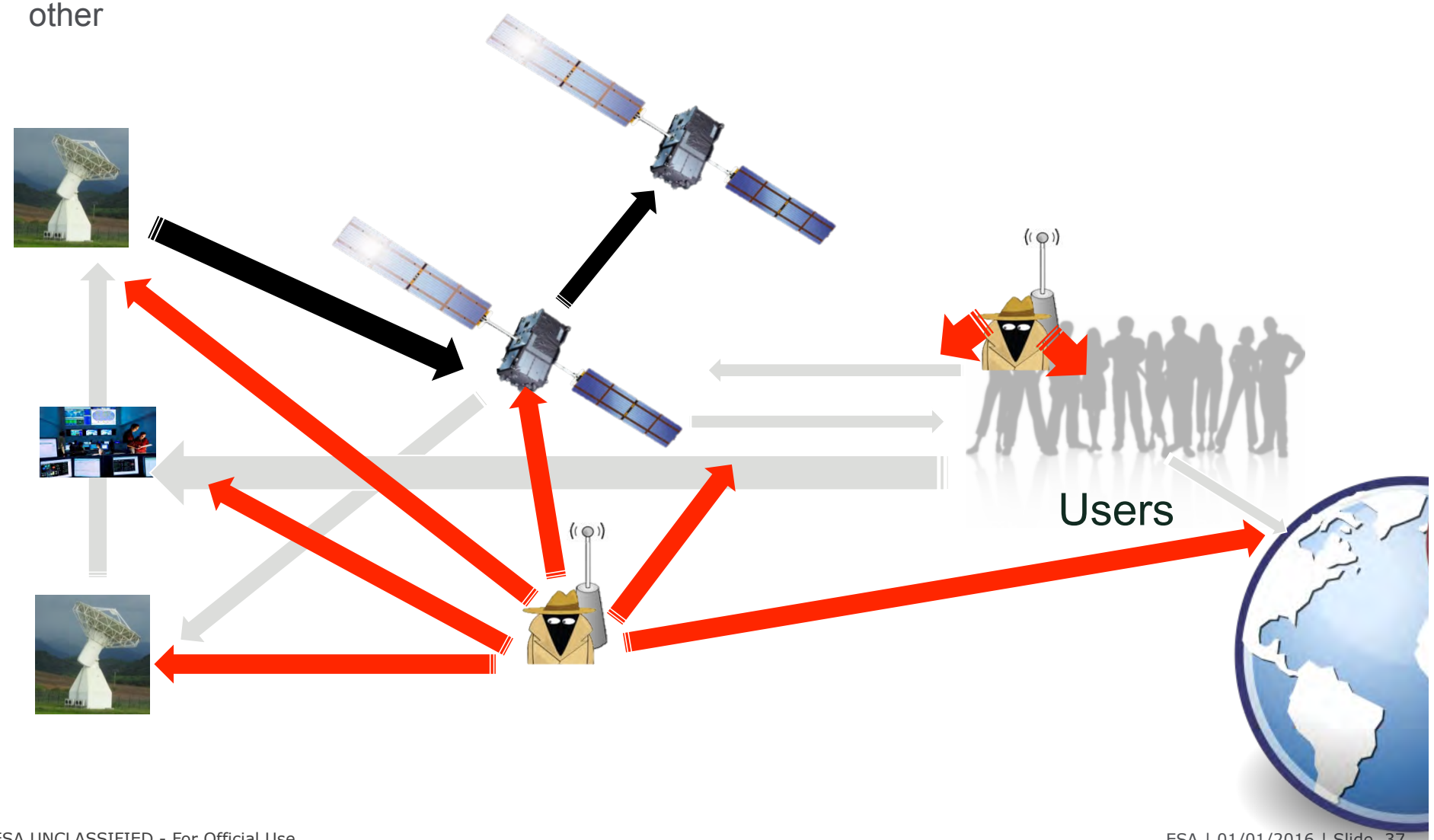


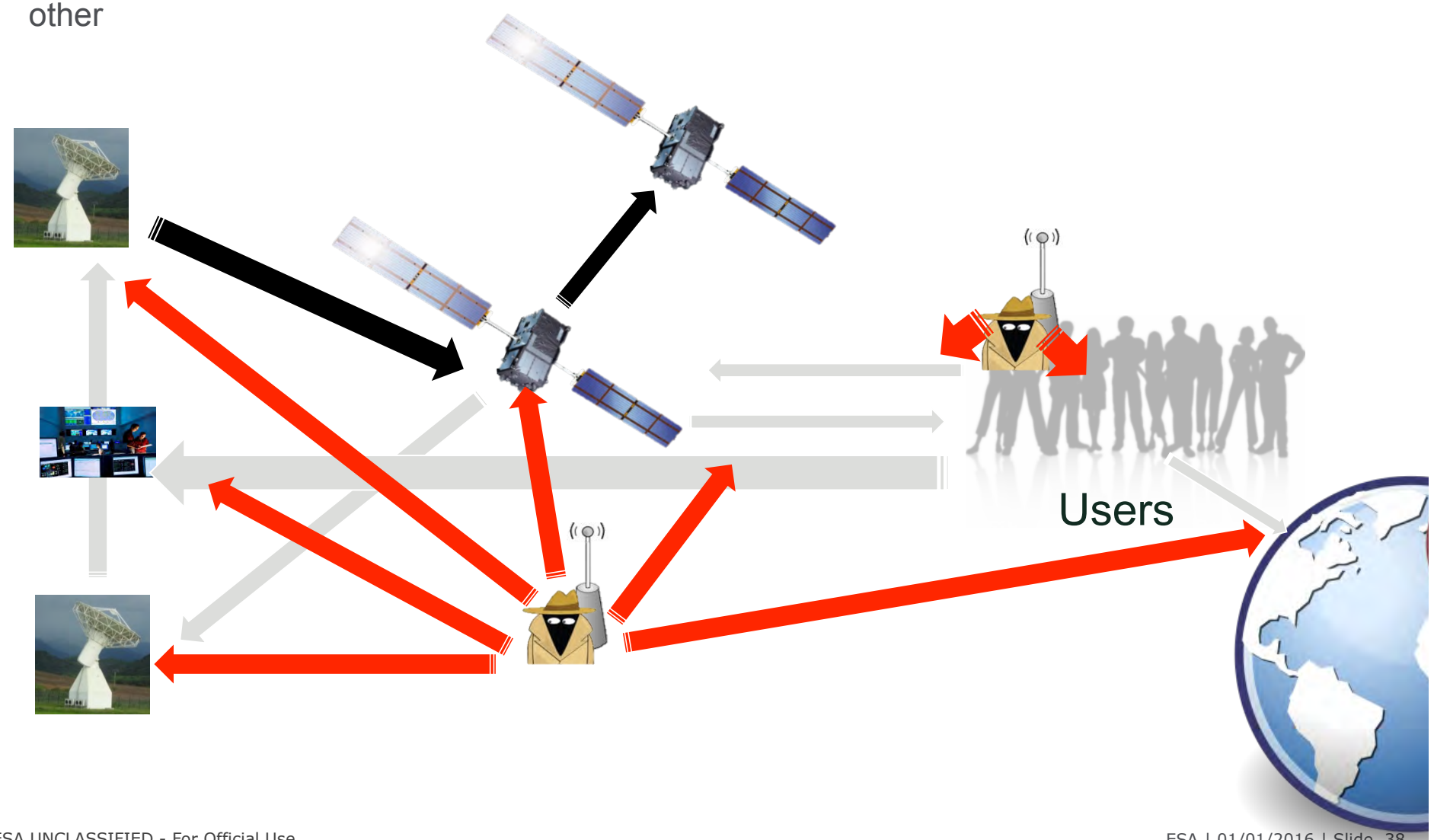
CCSDS Security Documents



SPACE SECURITY– New ~~triangle~~ err challenge

Ground- uplink-space-space-downlink-ground-user-other



SPACE SECURITY– New ~~triangle~~ err challenge

Ground- uplink-space-space-downlink-ground-user-other