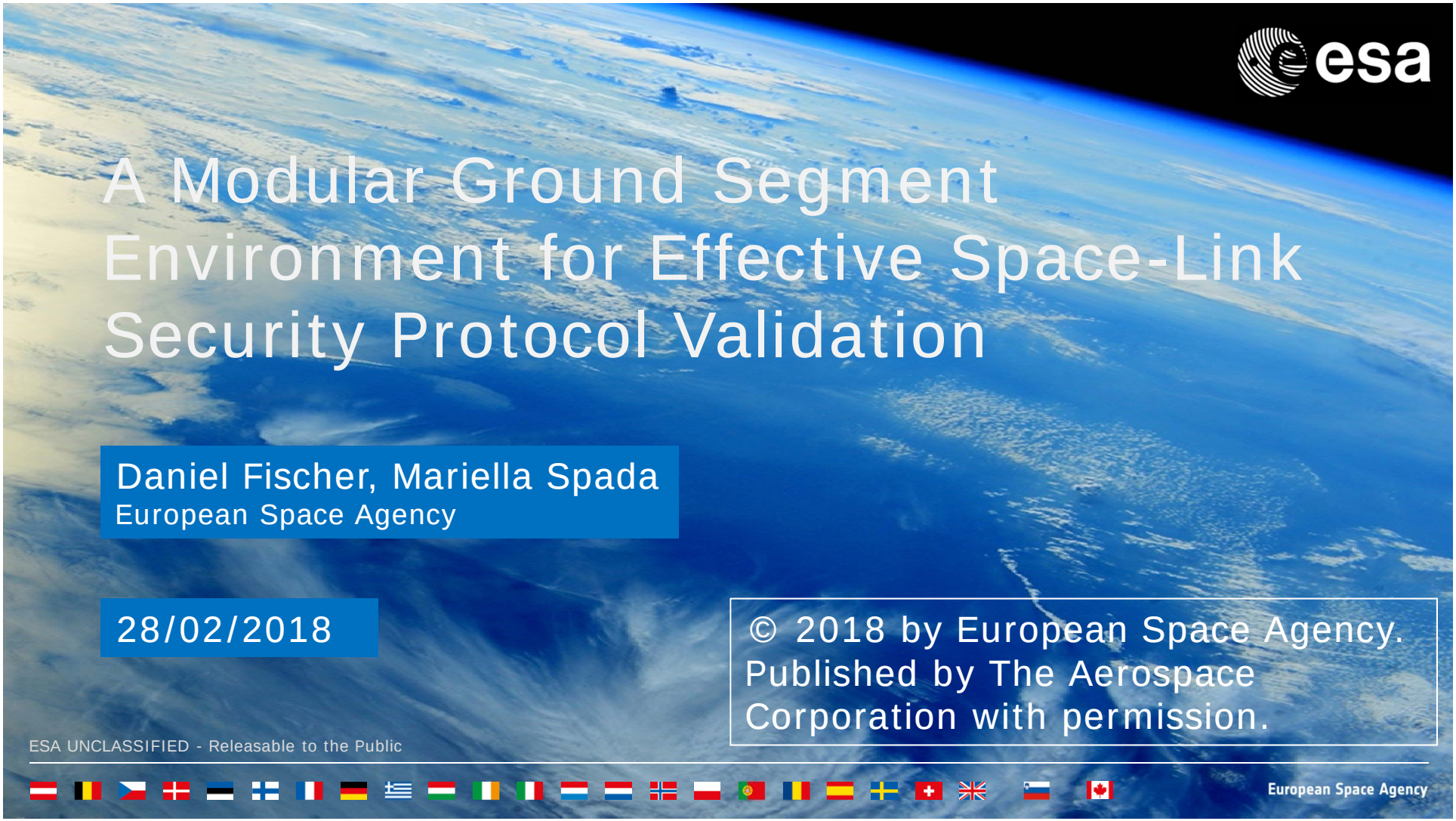


A Modular Ground Segment Environment for Effective Space-Link Security Protocol Validation

Daniel Fischer, Mariella Spada
European Space Agency

28/02/2018

Agenda

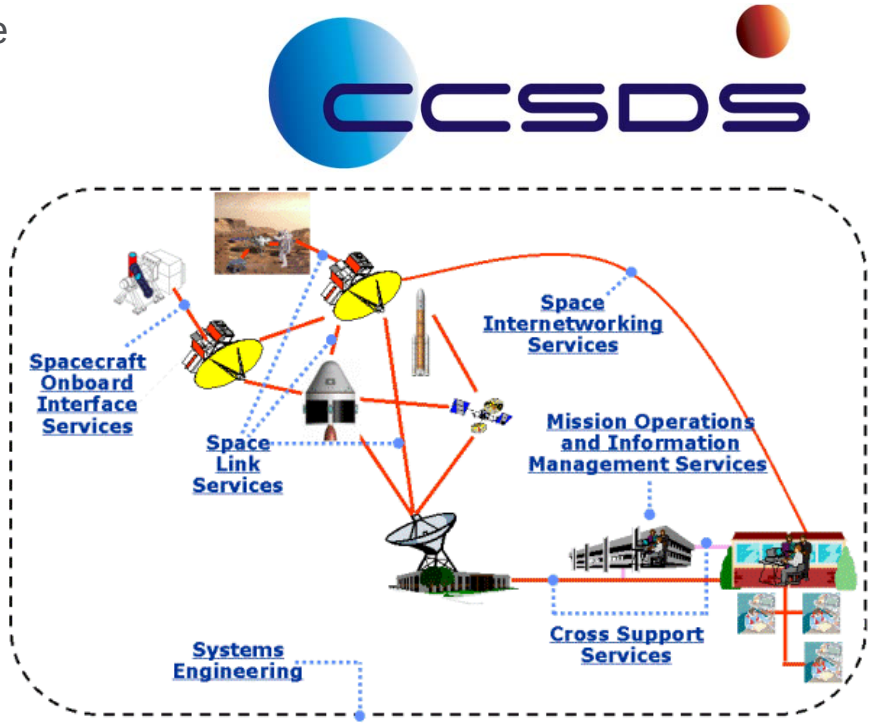
- Motivation: CCSDS Space Data Link Layer Security Protocol Interoperability Testing Campaign
- Concept:
  A Generic Approach for security testing
- First Use Case: SDLS Extended Procedures Interoperability Testing
- The Way Ahead

CCSDS & Interoperability Testing

- CCSDS = The **C**onsultative **C**ommittee for **S**pace **D**ata **S**ystems

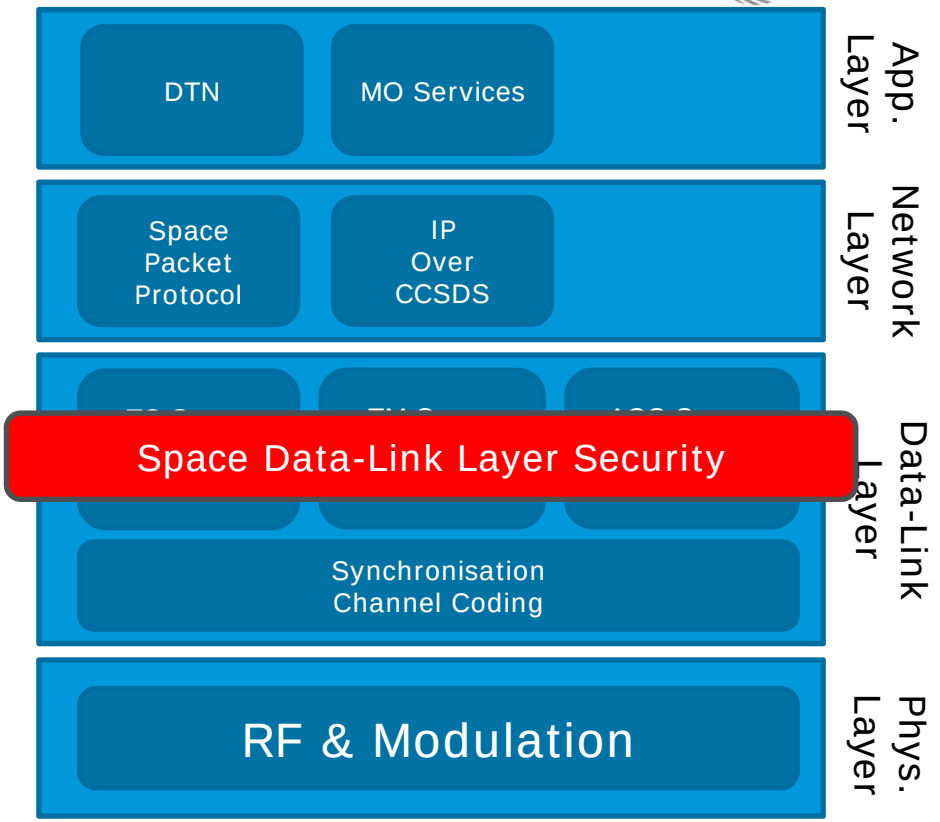
- CCSDS is an international committee for the development of standards in space communications and data systems
  - 11 Members and 29 Observers
  - More information: www.ccsds.org
  - Serving 500+ missions

- New CCSDS standards require two independent implementations that complete a series of interoperable test cases between each other

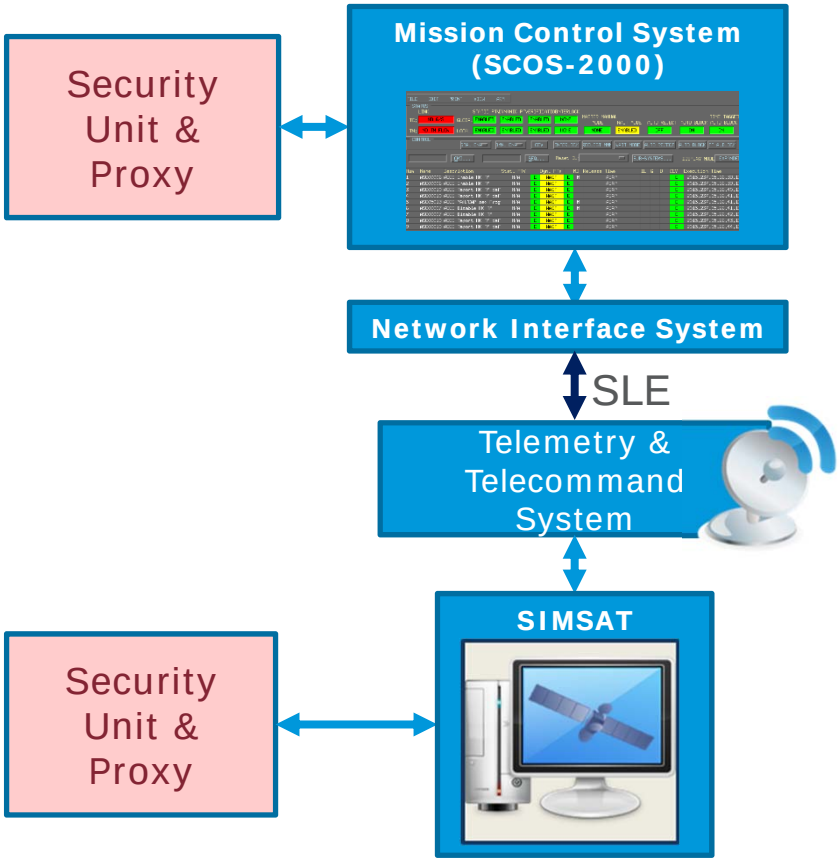


Space Data-Link Layer Security (SDLS) Protocol

- SDLS is a data-link layer security service protocol that provides:
  - Authentication
  - Authenticated Encryption
- Designed to be compatible with:
  - TC (VC/ MAP)
  - TM (VC)
  - AOS (VC)
  - (USLP)



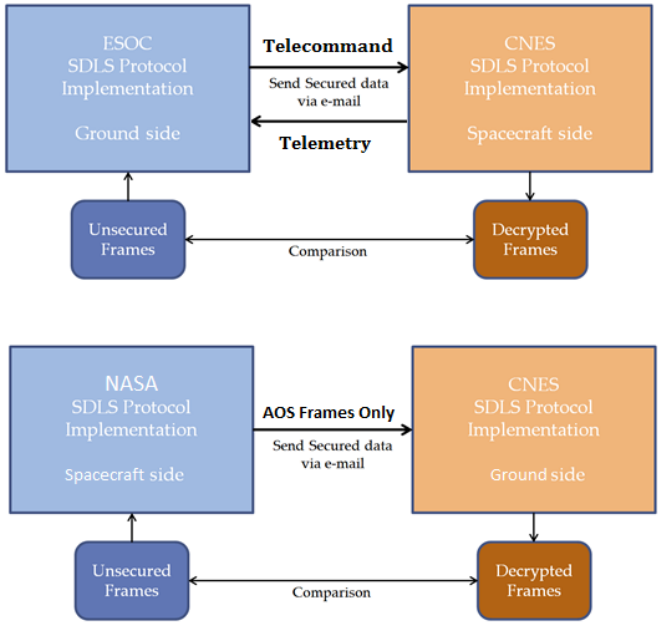
SDLS ESA Initial Testbed



- ESA SDLS interoperability testing prototype
  - Deployment of a realistic command & monitoring chain
  - Using the operational software products & configurations
  - Full simulation of space segment through operational simulator
  - Support for CCSDS Telemetry & Telecommand protocol suites

SDLS Interoperability Testing - Limitations

- SDLS Interoperability Testing Approach (ESA/NASA/CNES)
  - Offline test execution
  - Exchange of recorded TM/TC/AOS frames via secure email
- Interoperability Testing Immediate Problems
  - Firewall and network restrictions for interconnectivity of two testing environments
  - Differing data policies
  - Software Licenses
- This approach would not work for more complex testing campaigns
  - E.g. SDLS Extended Procedures
  - Any kind of communications performance testing



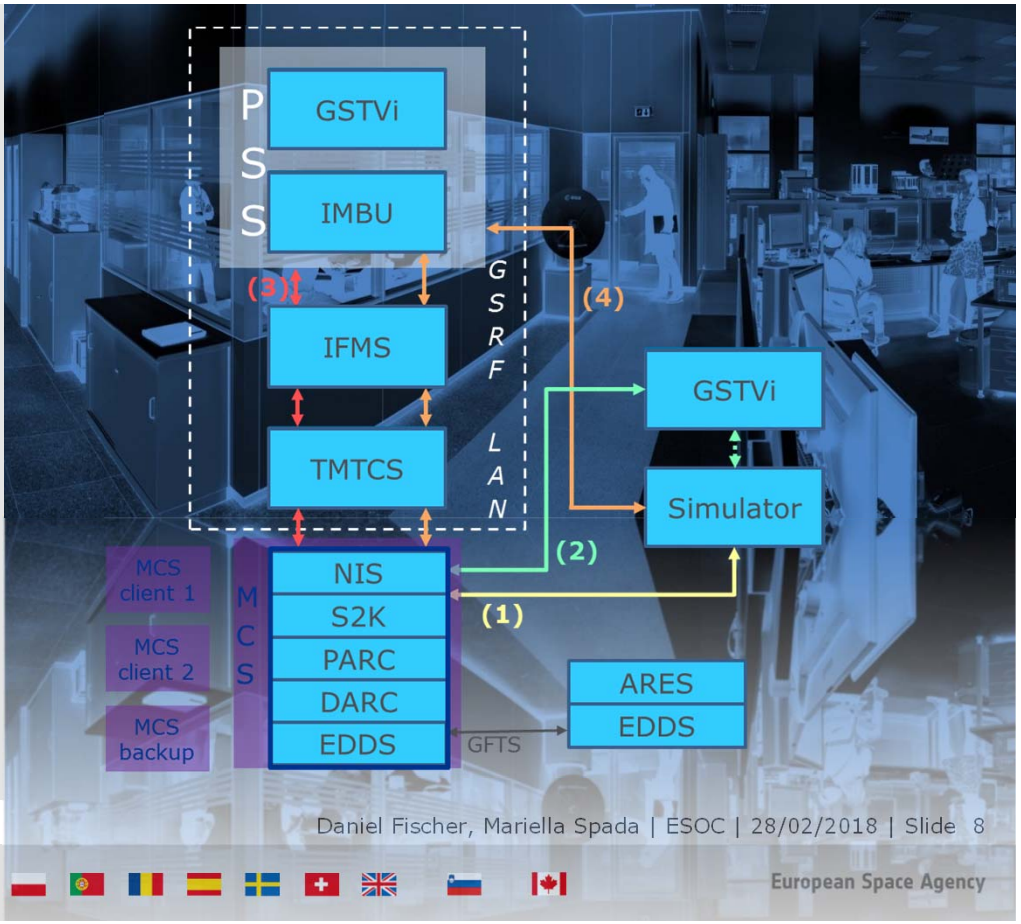
Security Testing Environment Requirements

- What should the environment support?
  - ✓ Validate space-link security protocols and contribute to interoperability testing
  - ✓ Execute other security testing campaigns
    - Security configuration tradeoff
    - Security performance testing

- This environment should be
  - ✓ Fully representative of the operational environment(s)
  - ✓ Flexible and modular
  - ✓ Allow easy accommodation of new interfaces

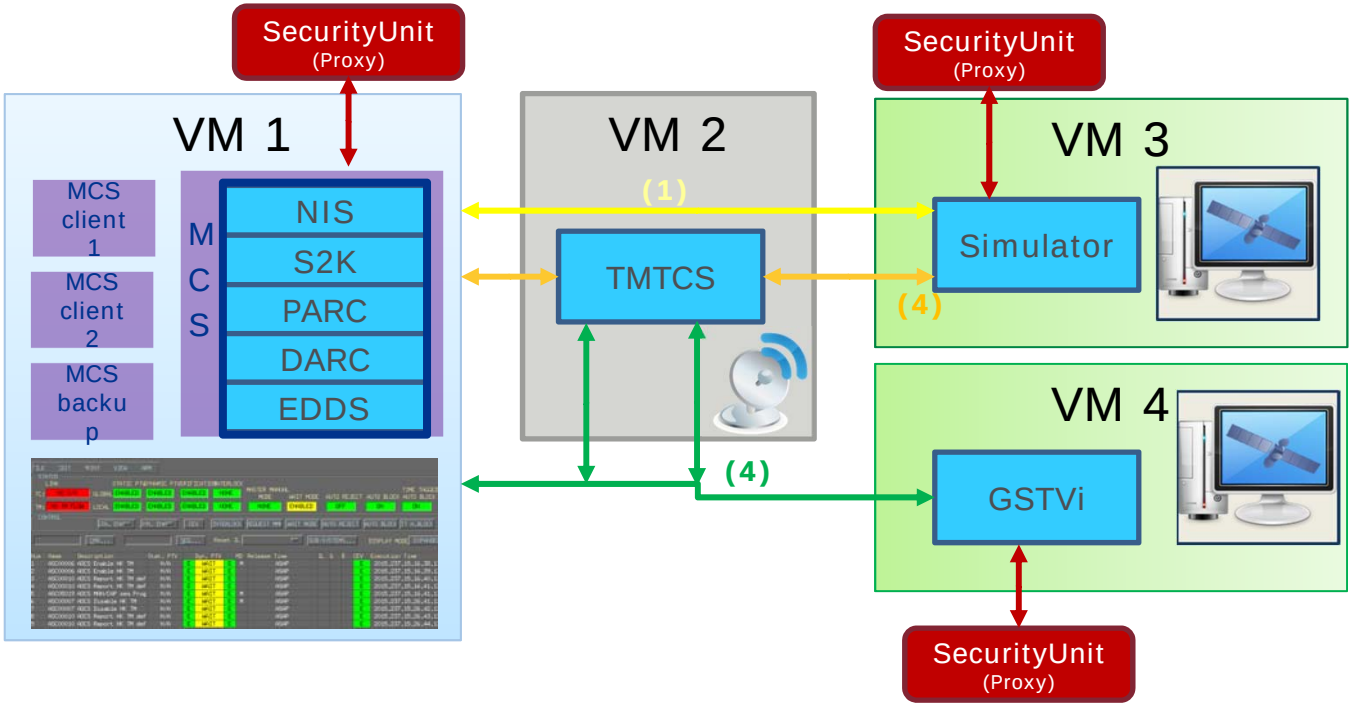
The ESA OPS Engineering Development Lab

- ESA lab for ground systems integration testing
- Fully representative end-to-end test & validation environment
- Capable of implementing different end-to-end chains
- Capable of integrating real hardware components e.g. from ground stations
- Software systems fully virtualized
- Fully automated GUI-based end-to-end integration testing capabilities



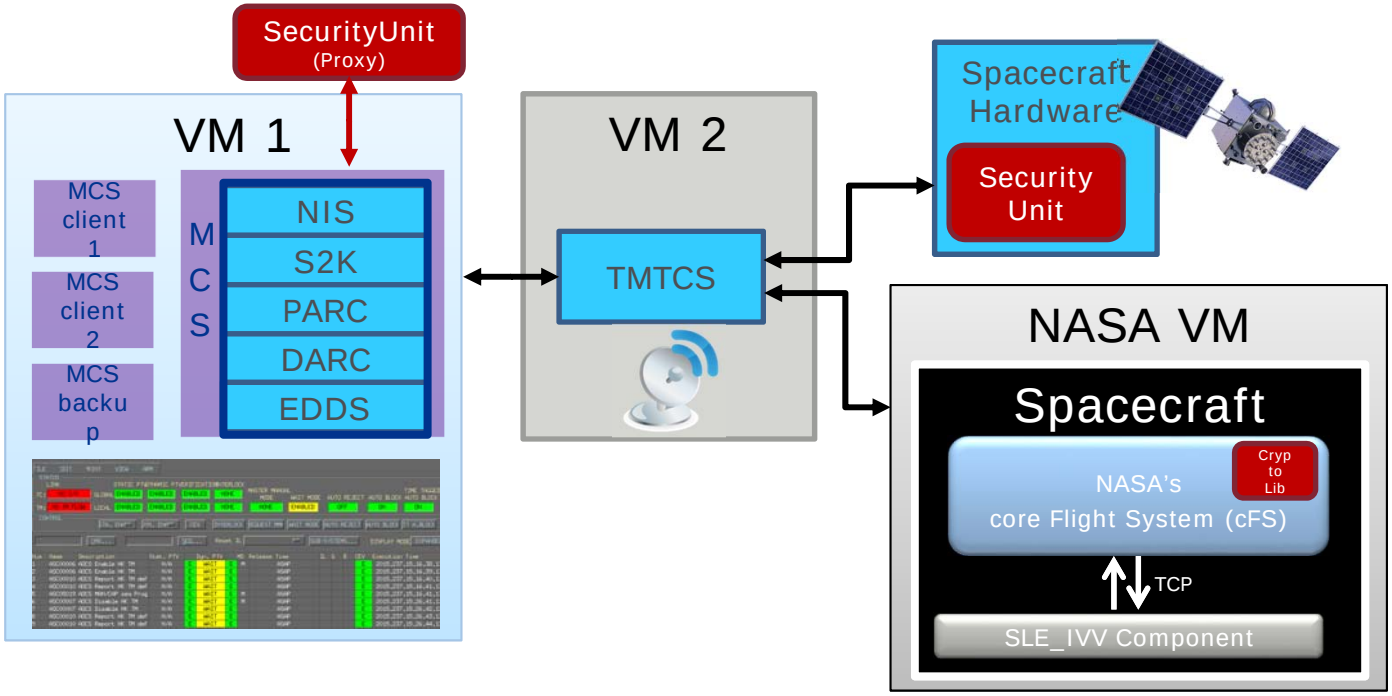
Architecture & Modularity

- Flexibility requires modularization → component-based design using virtualization technology
- Integration of interfaces for security units



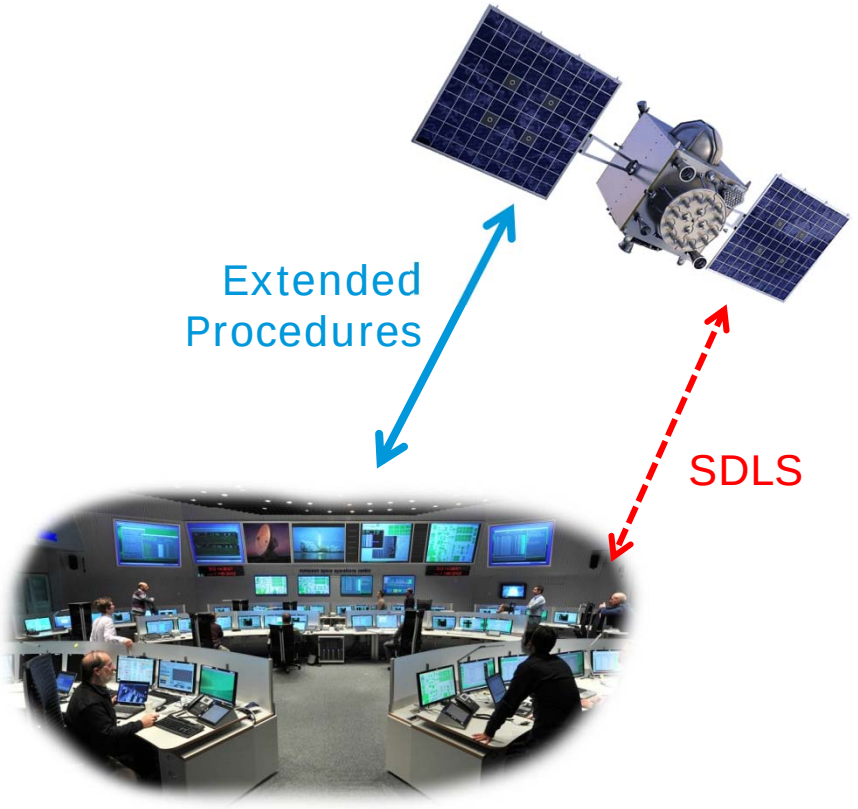
Architecture & Modularity

- Modular approach allows easy replacement of components
- Enabling new components (SW/HW) validation
- Enabling interoperability testing

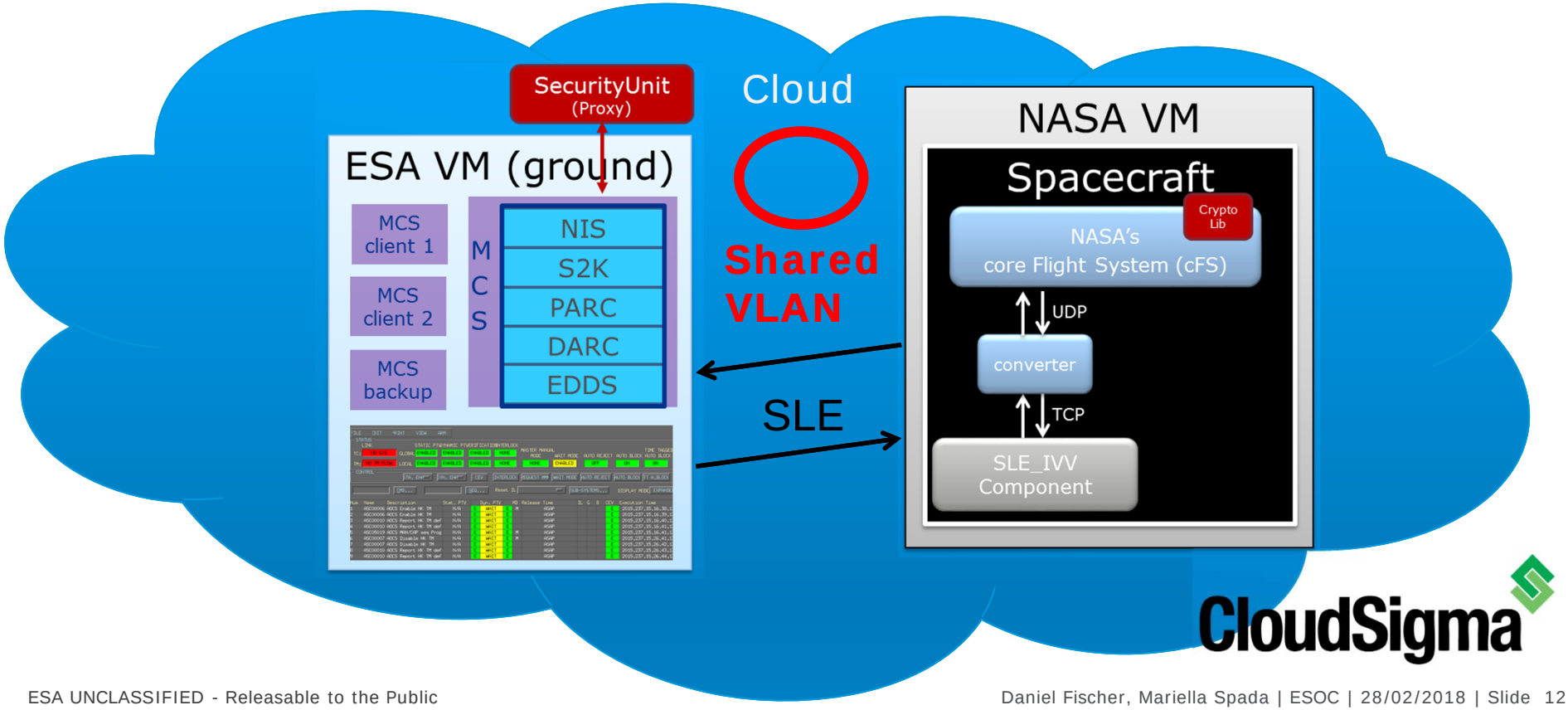


First Use Case: SDLS Extended Procedures

- SDLS Extended Procedures provide security management services for SDLS
  - How to synchronize the SDLS configuration → Security Association Management
  - How to monitor the security unit → SDLS Monitoring & Control
  - How to manage the cryptographic keys used for security operations → Key Management
- New TM OCF Type 2 for security status reporting
- Currently under agency review, publication expected for 2018



SDLS Extended Procedures Cloud Testing



First Use Case: SDLS Extended Procedures

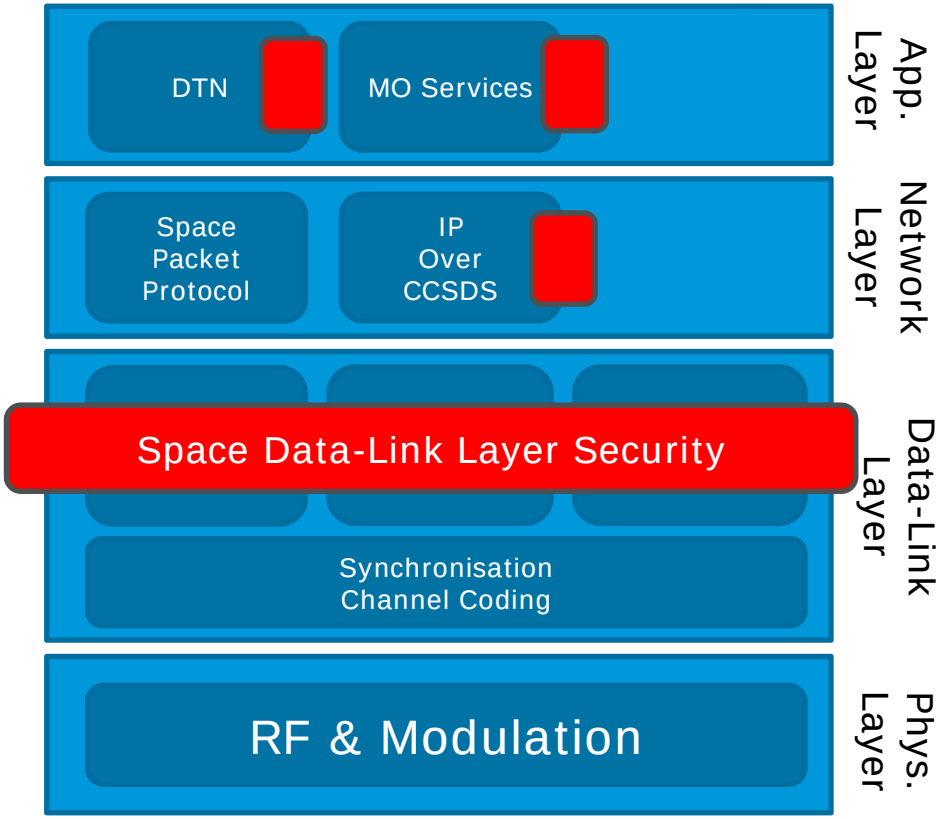
- SLDS Extended Procedures testing was a full success
  - Setup of the cloud environment took less than a day
  - SLE set up took some time but ultimately was not an issue
  - Much more extensive testing as with the previous setup was possible

- What did the new modular and flexible design actually add?
  - Easier transition into the cloud (VM can just be cloned)
  - Modularity allows easy switching of roles (space / ground)
  - Other space-link security protocols (e.g. network layer security, or bundle security) can easily be added

The Way Ahead - Secure Communications Testing

- Validation of emerging space-link security standards
  - IpSec over CCSDS IP Encapsulation
  - DTN Bundle Security Protocol
  - Mission Operations Services Security

- Security Performance Testing Campaigns
  - Performance Trade-Off for crypto algorithms and algorithm configurations
  - Testing of various security services approaches e.g. for key management



The Way Ahead – Secure Systems Engineering

- Exploitation of engineering development lab capabilities for security testing
  - ➢ Use of the sophisticated automation technologies
  - ➢ Security testing for all lab components

  → Enabling of automated security and security performance testing for future mission ground segments

- Contribution to Security Education and Training

- Use of secure systems engineering security services

A Modular Ground Segment Environment for Effective Space-Link Security Protocol Validation

Daniel Fischer, Mariella Spada
European Space Agency

Ground System Architecture Workshop 2018

Thank You for your Time!