7SHIELD

#3 - Demo pilots

Partners involved in piloting the 7SHIELD framework tell their stories: methodology used for approaching the security of a Ground Segment and benefit in adopting the 7SHIELD modules

Barbara Scarda (SERCO Italia SPA)

Communication manager

7SHIELD Pilots

Physical Attack in Arctic Space Centre in Sodankylä, Finland

Cyber-physical attack in the ground segment of NOA, Athens

Cyber-physical attack in Deimos Ground Segment in Spain

Threat detection and mitigation on the ICE Cubes Service

Cyber-attack on the ONDA DIAS platform

7SHIELD

Pilot Demonstration at the National Observatory of Athens

Souzana Touloumtzi (NOA)

Project manager

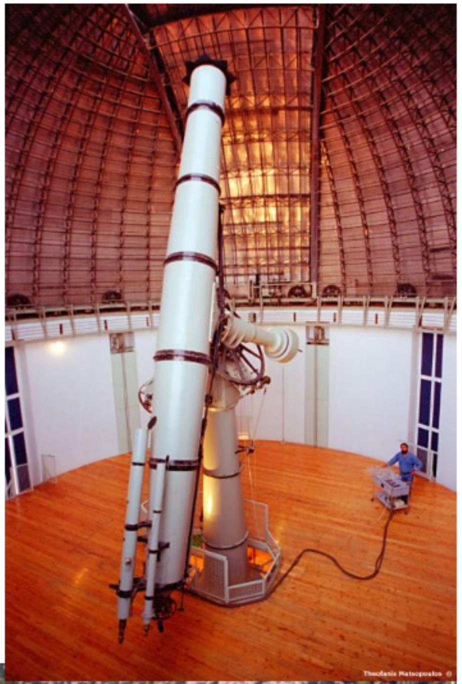
National Observatory of Athens

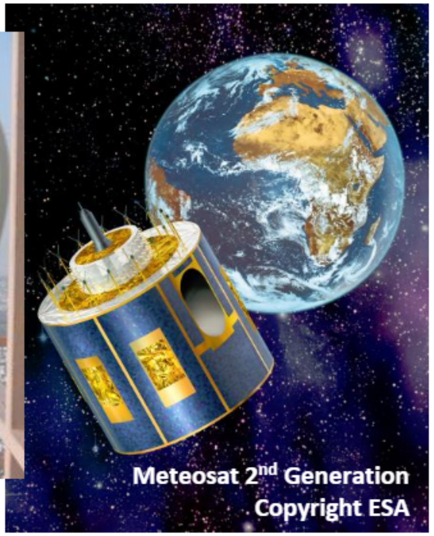
- Founded 1842, nominated by the Greek government as the sole research institution in charge of natural disasters monitoring.
- 3 research institutes
  - Institute for Astronomy, Astrophysics, Space Applications & Remote Sensing (IAASARS)
  - Institute for Environmental Research & Sustainable Development (IERSD)
  - Institute of Geodynamics (GEIN)
- IAASARS exploits satellite assets to develop operational EO-based services, to assist decision making of stakeholders in charge of crisis management.

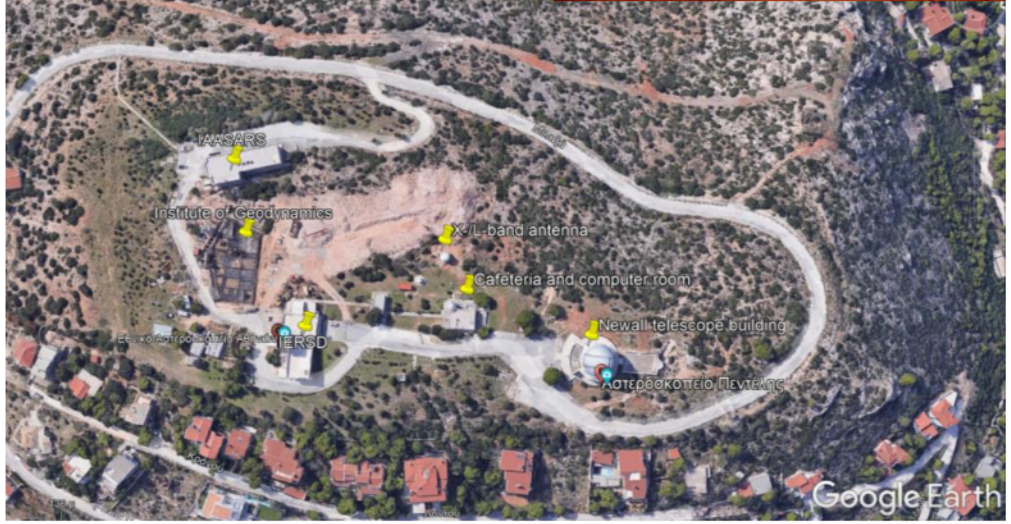
Theofanis Matsopoulos ©

Ground Station & Astronomical Station in Penteli

- Newall telescope
- X-/L-band antenna: acquisition/processing of data from NASA's MODIS, Suomi NPP, NPOESS, NOAA, MetOp missions – covers SE Europe, N. Africa, Black Sea, Balkans, Middle East.
- Meteosat 2nd Generation SEVIRI antenna & archiving facility for reception of EUMETSAT data
- Data centres, cloud & computing infrastructure
- Collaborative Ground Segment for management & dissemination of Sentinel data.




Meteosat 2nd Generation
Copyright ESA

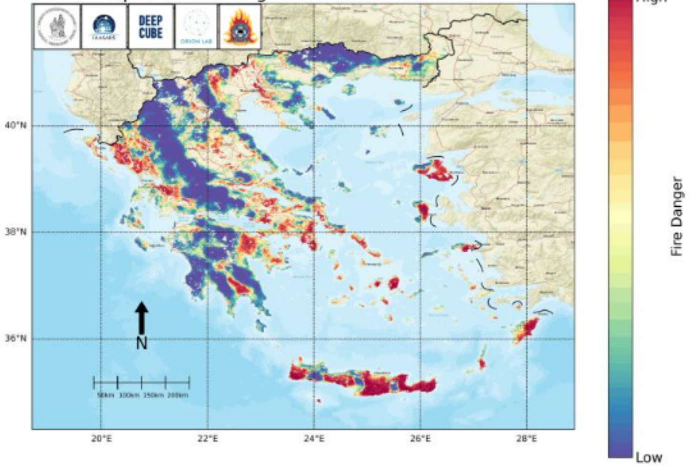


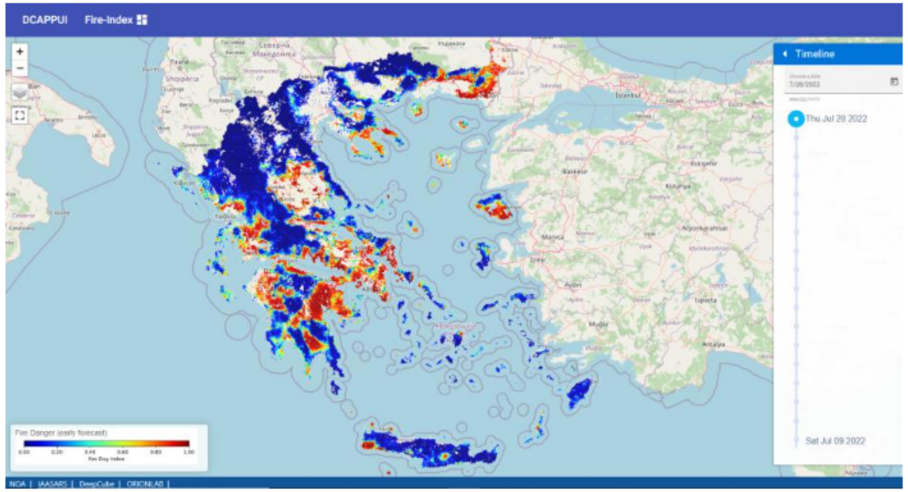
Indicative operational EO-based services supported by the Ground Station & data centres

- Satellite data access service: raw Copernicus Sentinel satellite data to Greek, European, International users & industrial stakeholders
- Single point of access for all user communities of Sentinel-5P mission
- Data collection, archiving & access from national seismological network and other national ground-based sensor networks

- Fire danger forecasting provided to Hellenic Fire Service on 24/7 basis
- Flood extent monitoring
- Volcanic unrest monitoring
- Earthquake monitoring
- Solar energy forecasting

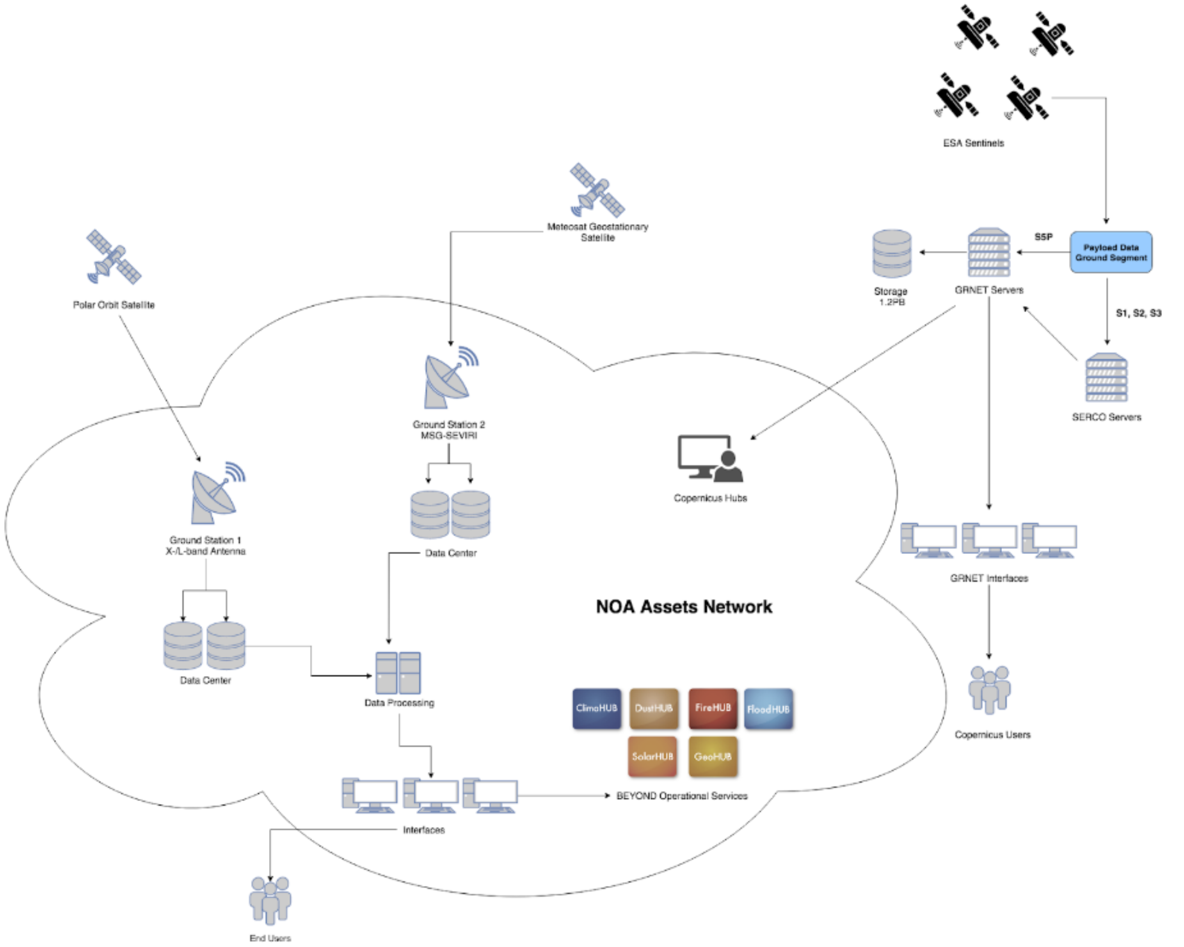
Updated fire danger forecast for 07-07-2022



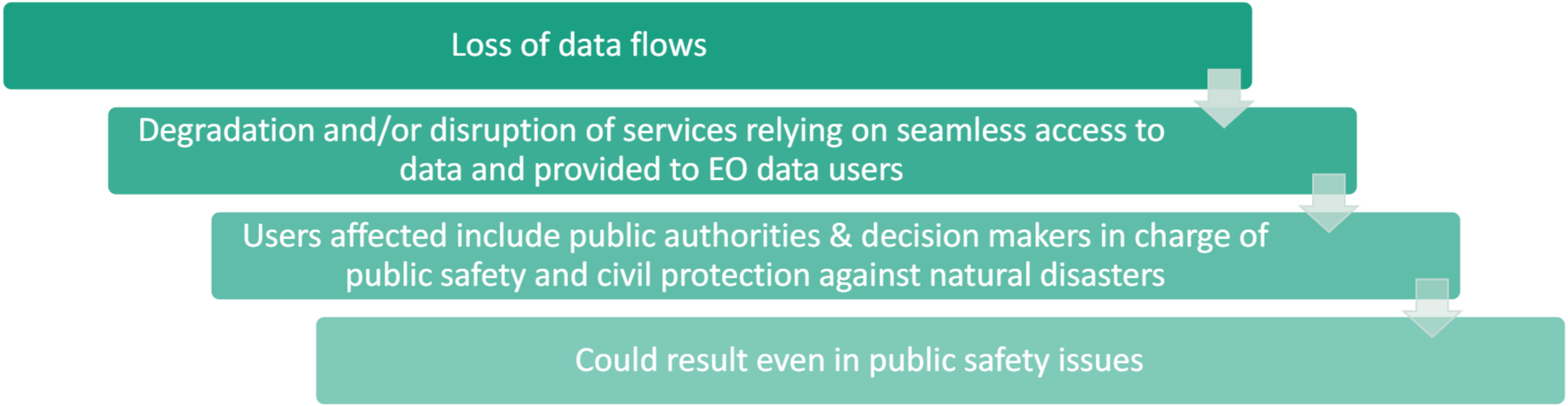


Importance of NOA’s Critical Infrastructure security

- Penteli site is *physical terminal point for all CI operated by NOA:* optical fibers, telecommunication networks, wireless networks & all main assets of the GS (antennas, meteorological stations, servers etc.)
- Combination of multiple single points of failure, which would result in disruption of operations
- Operational services to stakeholders rely on seamless access to satellite data and must never go offline



Cascading effects in case of disruption of service



Loss of data flows

Degradation and/or disruption of services relying on seamless access to data and provided to EO data users

Users affected include public authorities & decision makers in charge of public safety and civil protection against natural disasters

Could result even in public safety issues

- Assets include SOTA equipment → damage would result in high financial losses
- Time required for procurement of new equipment + possible lack of components, integration issues with existing infrastructure etc.

Advantage of using 7SHIELD technologies

✓ Enhance resilience of NOA's IT infrastructure against cyber-attacks with SOTA cybersecurity technologies

✓ Address physical vulnerability associated with the Visitor Center

✓ Help NOA, as CI operator in the space industry, comply with current standards for Ground Segments & be prepared for ***emerging hybrid threats***

✓ Research Support Directorate responsible for NOA's infrastructure is also in charge of security issues → need accurate detection technologies, user-friendly threat monitoring dashboards & support to make informed decisions and timely contact First Responders in case of emergency

Scenario 1: DDoS attack on NOA's mirror satellite ground station service

https://sentinels.space.noa.gr/dhus/#/home

- Motivation: NOA has suffered high number of (malicious) attempts to disrupt normal traffic of servers and services, resulting in slow or totally unavailable service
- Based on actual urgent needs, quite common & high-impact type of attack

✓ Secure Authentication Mechanism (KR02)

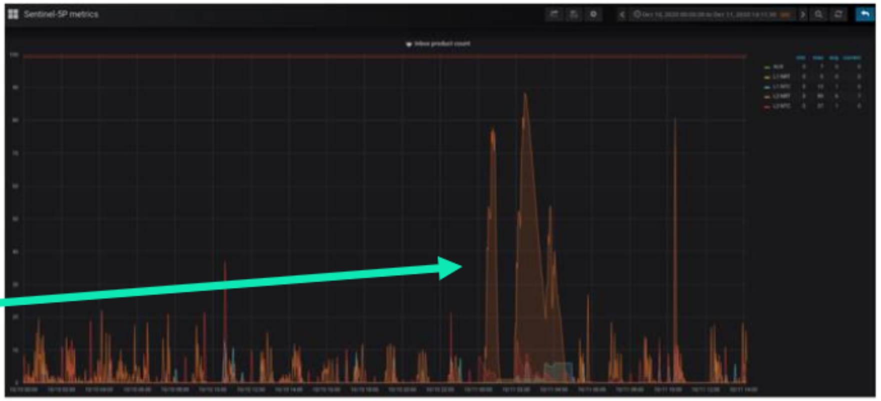
✓ Cyber-Physical Threat Monitoring dashboard (KR20)

✓ ENGAGE platform (KR20)

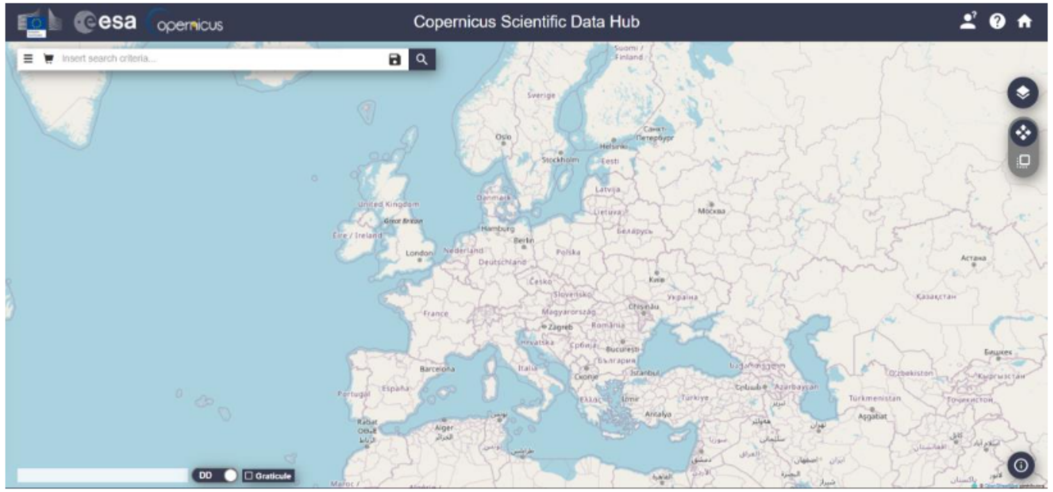
✓ Cyber-Attack Detector & GRAFANA dashboard (KR08)

✓ Emergency Response Plans (KR17)

✓ Business Continuity Scenarios (KR17)

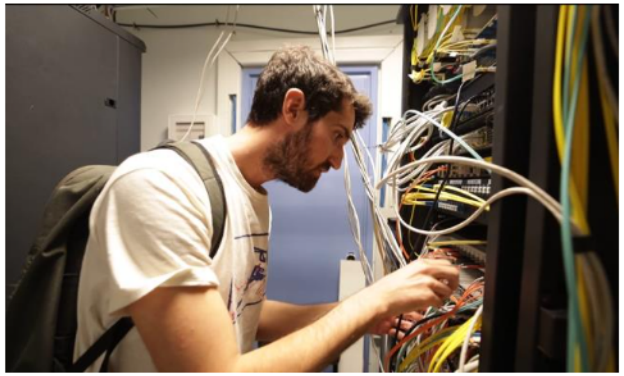


Example of a DDoS attack to Copernicus Hubs in October 2020: a queue of products to be ingested and published to the end users is created



Scenario 2: intrusion at NOA's premises in Penteli combined with cyber-attacks

- 2 intruders entered as visitors at Newall Visitor Center with intention to perform damage to IT infrastructure of IAASARS that supports the GS operations
- Detection of physical & cyber threats → correlation → confirmation of **hybrid attack**
- Intervention of First Responders & successful execution of ERP



- ✓ Geospatial Complex Event Processing Engine, Situational Picture Generation and Update, Hyper Combined Correlator (KR11)
- ✓ Video Object Detection & Activity Recognition (KR07)
- ✓ Face Detection and Recognition (KR06)
- ✓ CPTM & ENGAGE (KR20)
- ✓ Cyber-Attack Detector & Correlator & GRAFANA (KR08)
- ✓ Emergency Response Plans & Business Continuity Scenarios (KR17)
- ✓ Message Generation System (KR15)
- ✓ First Responders Support System (KR14)

Detection & correlation of events

- 2 persons in restricted zone
- 2 persons entering IAASARS building
- Unauthorized PC connected to NOA network
- Unknown face at critical data centre

Scenario 3: RF interference with jamming device & demo of EETT Spectrum Monitoring countermeasures

- Motivation:
  - *RF interference (e.g., from transponders of mobile network companies installed in Ymittos mountain) issue for several years affecting sensing equipment in Penteli*
  - *Can be also malicious in the form of jamming or spoofing*
  - *Leads to corrupted satellite images & service degradation*
  - *Affects critical services such as wildfire monitoring*
- NOA depends on EETT to resolve attack as the competent authority for earth stations at national territory

✓ CPTM and ENGAGE dashboards (KR20)

✓ CADF Rule Designer API & GRAFANA dashboard (KR08)

✓ Tactical Decision Support System (KR14)

✓ Emergency Response Plans, Business Continuity Scenarios (KR17)

Souzana Touloumtzi
stouloumtzi@noa.gr

7SHIELD

Thank You

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883284.

Hybrid scenario from pilot demo on 29 September 2022

Methodology for the user requirements definition

- ✓ Study of situational factors exposing the GS to natural and man-made threats
- ✓ Thorough examination of premises for physical vulnerabilities conducted by the Hellenic Police
- ✓ Confidential detailed vulnerability analysis and security recommendations report prepared for NOA by HP
- ✓ Interviews and focus groups with GS operators from NOA Network Operations Center to collect history of events & needs
- ✓ Meetings with First Responders & CI security experts
- ✓ Mapping of threats based on history of events, frequency, probability & impact
- ✓ Mapping of all critical assets and cyber-physical threats assessment using 7SHIELD pre-crisis tools (e.g., MBDA, CIRP-RAT, CPTI etc.)

7SHIELD

Demonstration pilot at Finnish Meteorological Institute’s Arctic Space Centre

Timo Ryyppo (FMI)

Project manager

Finnish Meteorological Institute’s Arctic Space Centre (FMI-ARC)

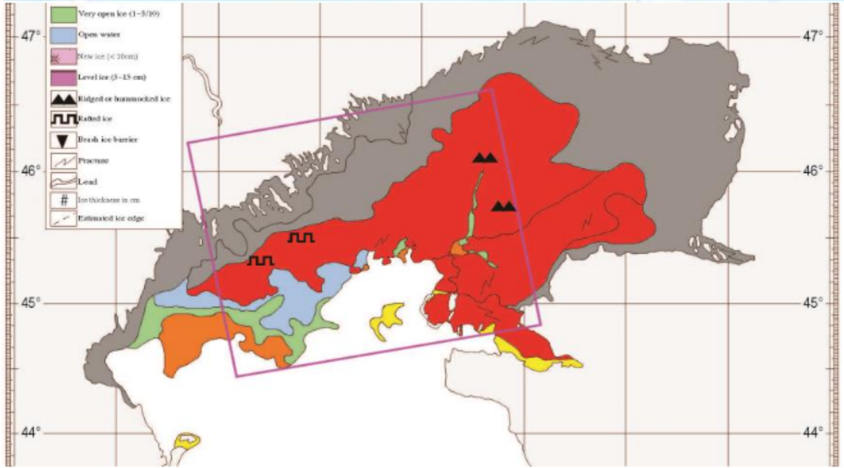
FMI-ARC Ground Segment

- 4 antenna systems
  - 2 x 7.3 m (X-band and S/X-band)
  - 2 x 3.7 m (X/L-band)
- Data center for data processing, dissemination and archiving
- Excellent location for contacting polar orbiting satellites
- Collaboration with ESA, NASA, NOAA, EUMETSAT and partners globally
- Copernicus Sentinel Collaborative Ground Station

Issues in setting up the Ground Segments' security

- Climate and weather
    - Temperature variation between -40 to 30°C
    - Temperature record -50°C
    - Springtime condensation water on surfaces
    - Polar night
- Remoteness
    - Sodankylä municipality has ~9 000 inhabitants, of which ~4 000 lives in Sodankylä town about 7 km from site
    - 130 km to closest bigger city (Rovaniemi)
- Site locates close to Finnish Defence Force's military base (~10 km)

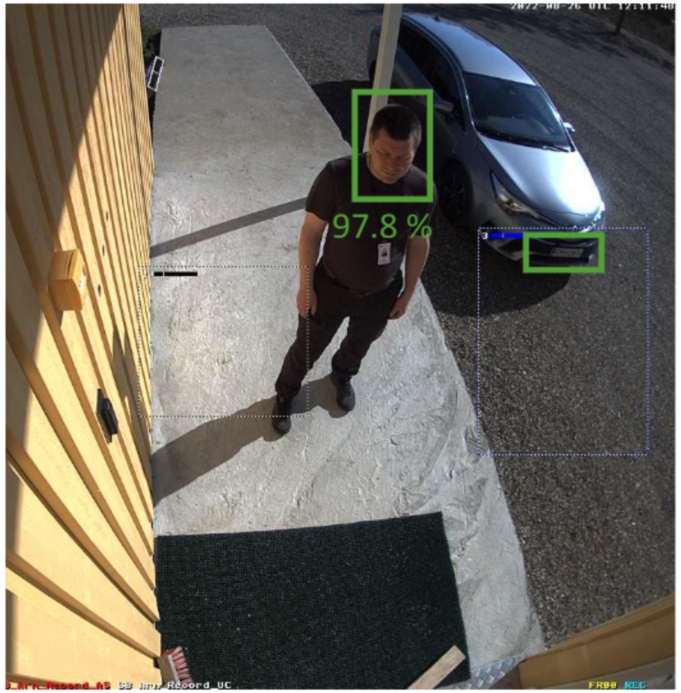
Cascading effects in case of disruption of Ground Station services



Pilot demonstrations through scenarios

- Technical modules for physical detection
    - Video-based object detection (VOD)
    - Activity recognition (AR)
    - Face detection and face recognition (FDR)
    - Object Detection at the Edge (ODE)
    - Multi-Modal Automated Surveillance (MMAS) (thermal and near-infrared
    - First Responders’ Support System (FRSS)
    - Laser Fence Sensor (LFS)
    - Perimeter Laser Sensor (PLS)
    - 3D Mini Drone Detector (3D MND)
    - UAV Neutralization Mechanism (UNM)

Concrete advantage of using 7SHIELD



ILMATIETEEN LAITOS

FMI-ARC satellite handbook

Version 2.0

Physical scenario from pilot demo on 10 November 2022

7SHIELD

https://www.7shield.eu/

Contact name

timo.ryyppo@fmi.fi

ILMATIETEEN LAITOS
METEOROLOGISKA INSTITUTET
FINNISH METEOROLOGICAL INSTITUTE

Thank You

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883284.

7SHIELD

Demonstration pilot in SPACEAPPS

Mathieu Schmitt, Manuela Aguzzi (SPACEAPPS)

Project manager

PILOT USE CASE: ICE Cubes Service

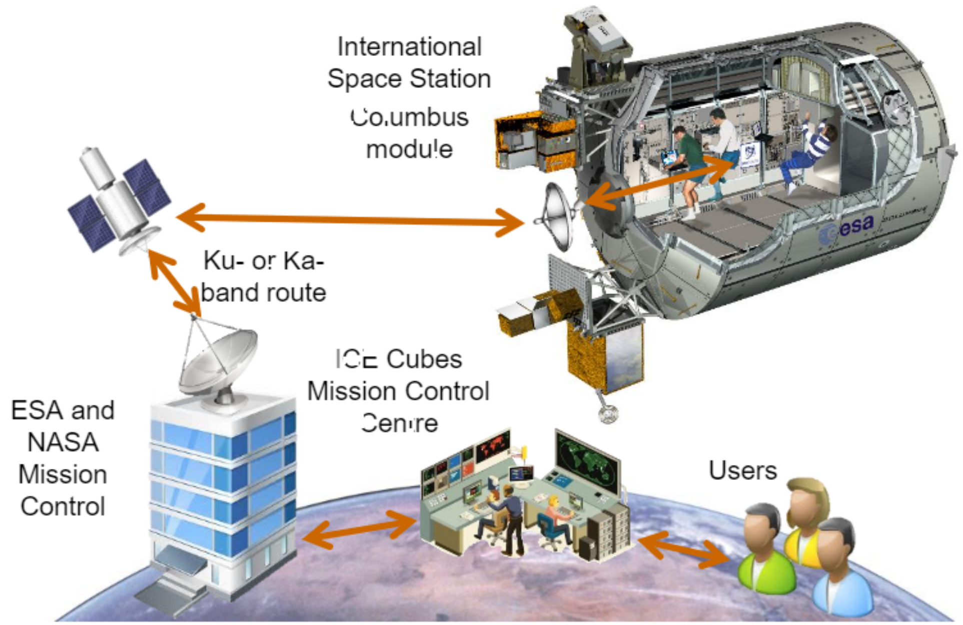
The ICE Cubes service provides:

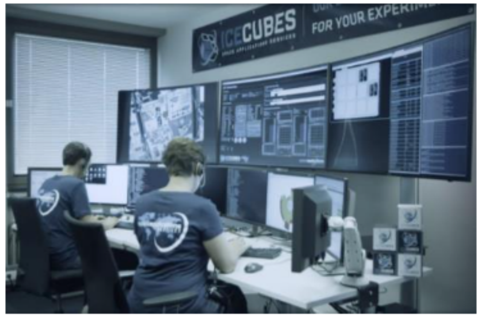
- A permanent multipurpose facility (**ICE Cubes Facility**) on board the ISS allowing for the accommodation and exploitation of **Experiment Cubes** in the fields of science, education and technological readiness (TRL) enhancement

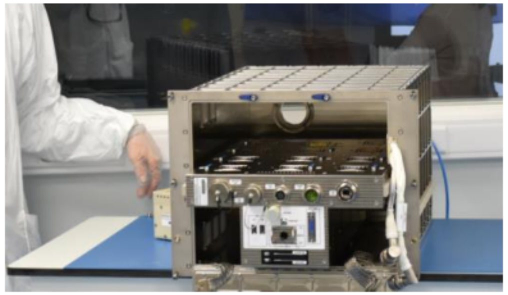
- The ground infrastructure for the management of the ICF and the Experiment Cubes

- The end-to-end commercial service allowing utilization of the **ICE Cubes Facility**

- Data reception and distribution directly to the various user home bases

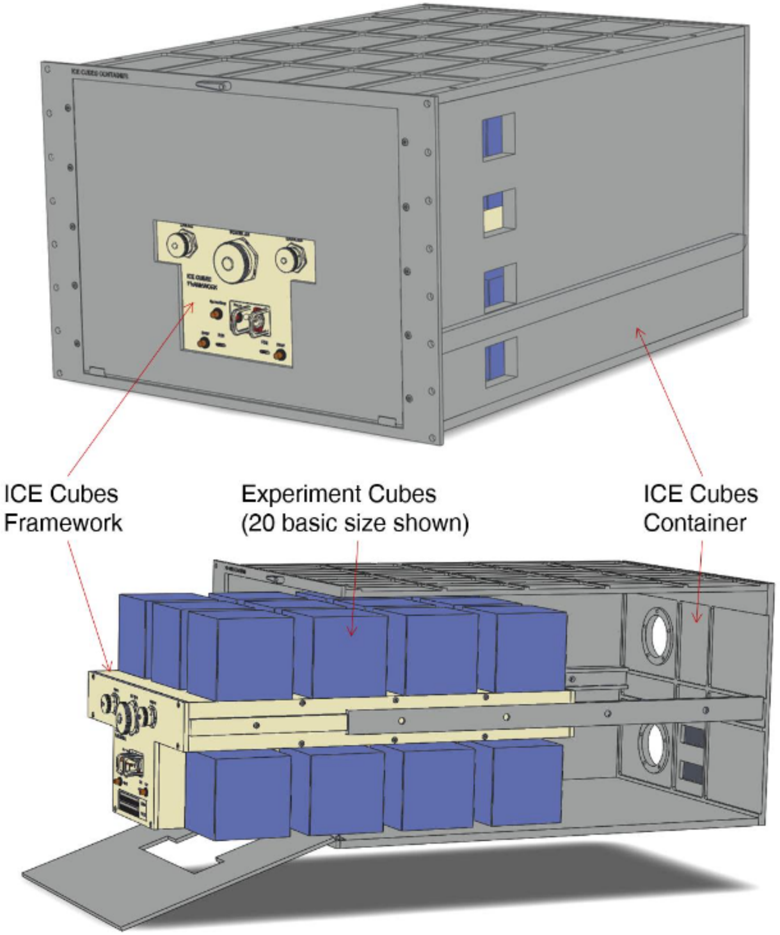

International Space Station
Columbus module
esa
Ku- or Ka-band route
ESA and NASA Mission Control
ICE Cubes Mission Control Centre
Users



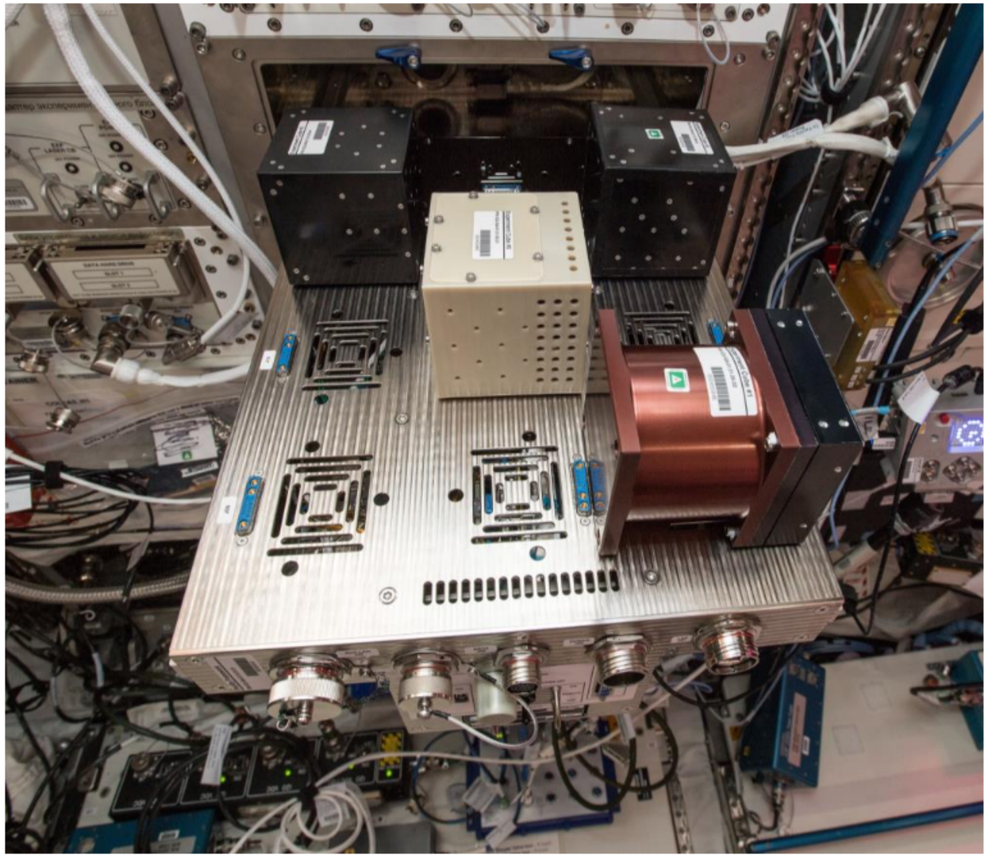


PILOT USE CASE: ICE Cubes Service

ICE Cubes Facility and Experiment Cubes.



ICE Cubes Facility (ICF)



ICE Cubes Facility in Columbus

PILOT USE CASE: ICE Cubes Service

Scientific Opportunities and Possible Uses:

Microgravity

- Fluid science
- Materials science
- Plasma physics
- Human physiology
- Plant biology
- Cell and molecular biology
- Biotechnology
- Microbiology

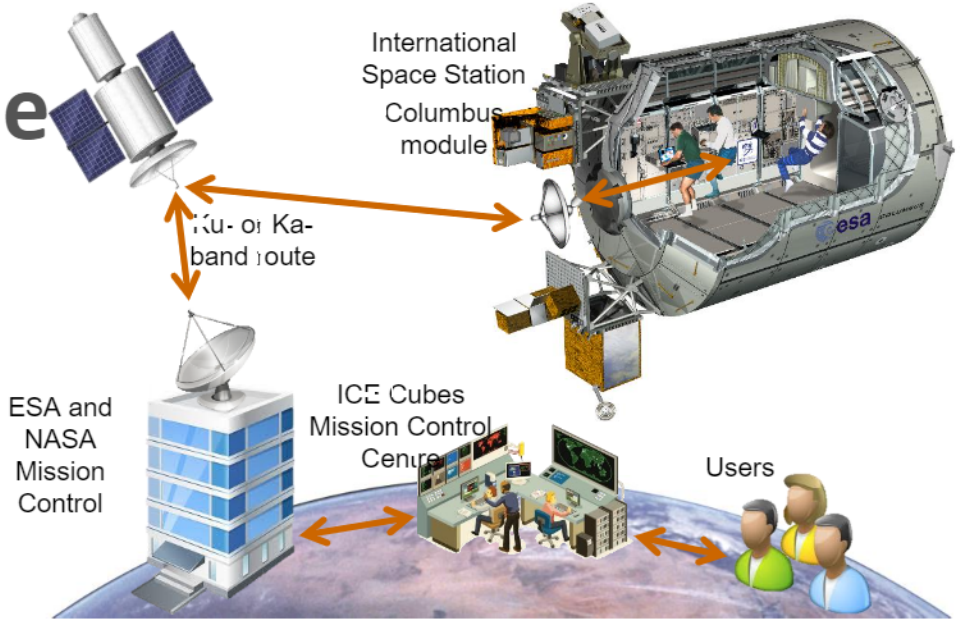
Technology demonstrations

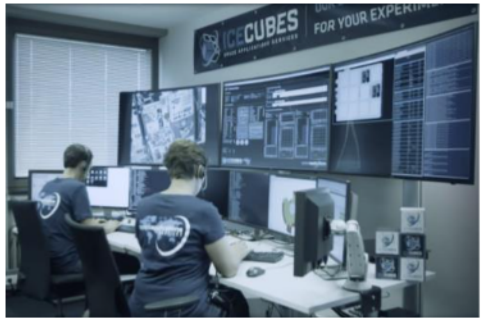
- 3D printing / tools manufacturing
- In-space testing of components
- In-space testing of systems
- Receivers / transmitters
- Sensing / actuating devices
- Robotics
- Chip-scale atomic clock

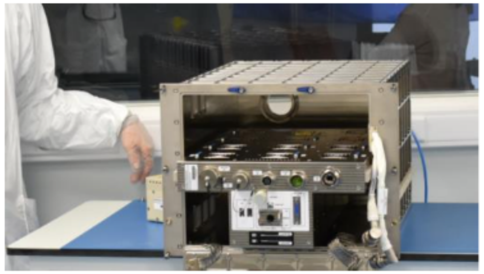
PILOT USE CASE: ICE Cubes Service

Security Aspects:

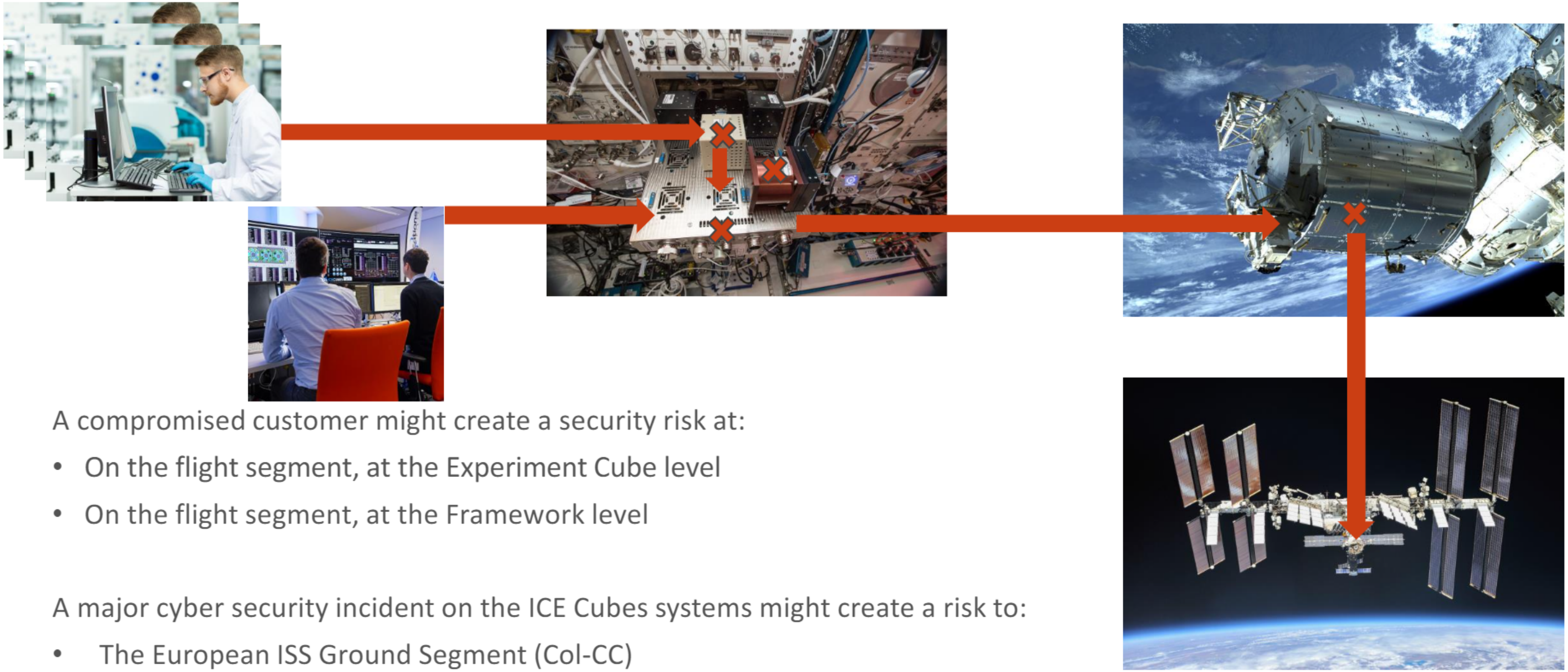
- Payload operations from ground, i.e. near real-time telemetry and telecommand -> Internet protocols: TCP/IP, UDP
- The investigators to monitor and control their Experiment/Cube, from their office to the ISS.
- The security aspect of the service, especially in terms of cyber security is of high priority.
- In terms of prevention, the architecture of services is audited by external parties mandated by ESA.


International Space Station
Columbus module
Ku- or Ka-band route
ESA and NASA Mission Control
ICE Cubes Mission Control Centre
Users





Cascading effects in case of disruption of service



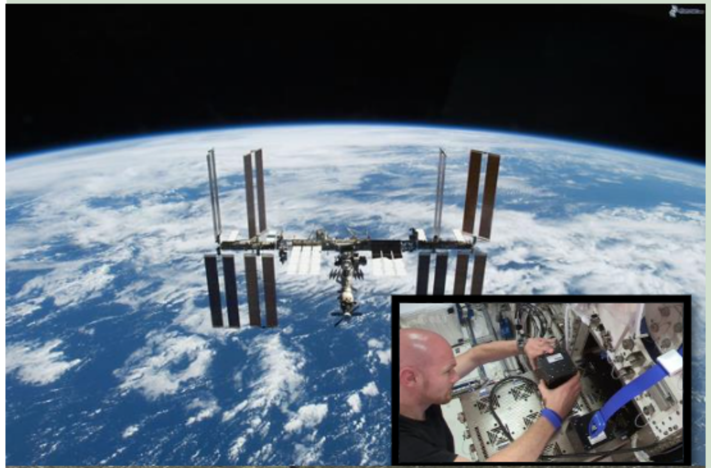
A compromised customer might create a security risk at:

- On the flight segment, at the Experiment Cube level
- On the flight segment, at the Framework level

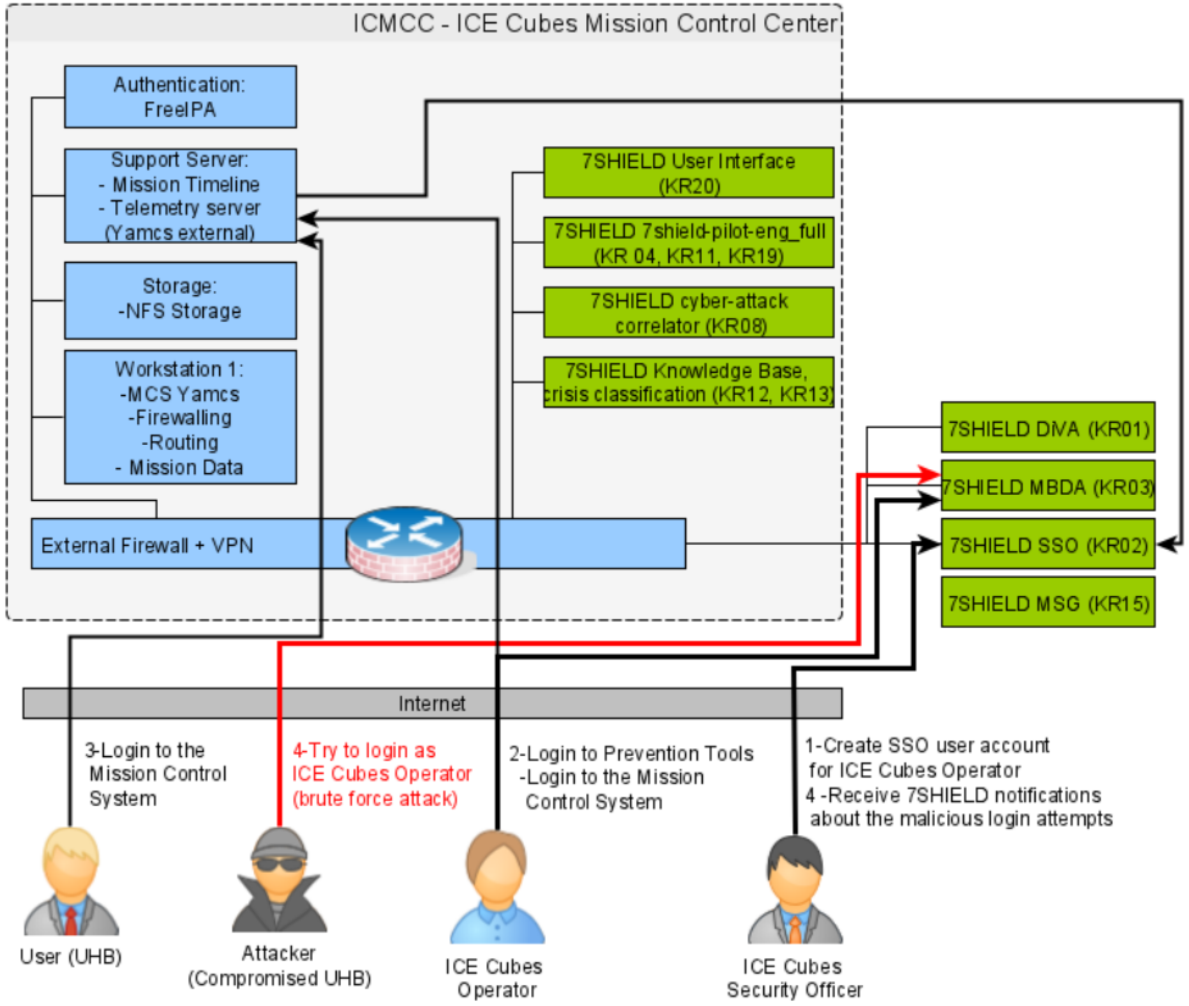
A major cyber security incident on the ICE Cubes systems might create a risk to:

- The European ISS Ground Segment (Col-CC)
- The ICE Cubes Flight Segment at Cubes Level
- The ICE Cubes Flight Segment at Framework level
- The ISS Joint Station LAN.

PUC4 ICE Cubes – Scenarios Overview

Operational Environment		7SHIELD Reference Environment	
	ICE Cubes Flight Model within the ISS		ICE Cubes Engineering Model within the SpaceApps Cleanroom
	Space to ground: via TDRS->NASA White Sands->ESA Col-CC		Space to ground: simulated
	Operations from the ICMCC in Brussels		Operations from the ICMCC in Brussels Duplicated environment

PUC4 ICE Cubes – Scenario 4A – User Login Protection


ICMCC - ICE Cubes Mission Control Center
Authentication: FreeIPA
Support Server: - Mission Timeline - Telemetry server (Yamcs external)
Storage: -NFS Storage
Workstation 1: -MCS Yamcs -Firewalling -Routing - Mission Data
External Firewall + VPN
7SHIELD User Interface (KR20)
7SHIELD 7shield-pilot-eng_full (KR 04, KR11, KR19)
7SHIELD cyber-attack correlator (KR08)
7SHIELD Knowledge Base, crisis classification (KR12, KR13)
7SHIELD DIVA (KR01)
7SHIELD MBDA (KR03)
7SHIELD SSO (KR02)
7SHIELD MSG (KR15)
Internet
3-Login to the Mission Control System
4-Try to login as ICE Cubes Operator (brute force attack)
2-Login to Prevention Tools -Login to the Mission Control System
1-Create SSO user account for ICE Cubes Operator
4 -Receive 7SHIELD notifications about the malicious login attempts
User (UHB)
Attacker (Compromised UHB)
ICE Cubes Operator
ICE Cubes Security Officer

Setup

- The Security Officer checks the security assessment with the 7SHIELD integrated prevention tools (MBDA, CIRP, Diva)
- The Security Officer registers a new user account for the ICE Cubes Operator and two users UHB
- The ICE Cubes operator uses its login to access the 7SHIELD tools (MBDA) and the Mission Control Systems (Yamcs)

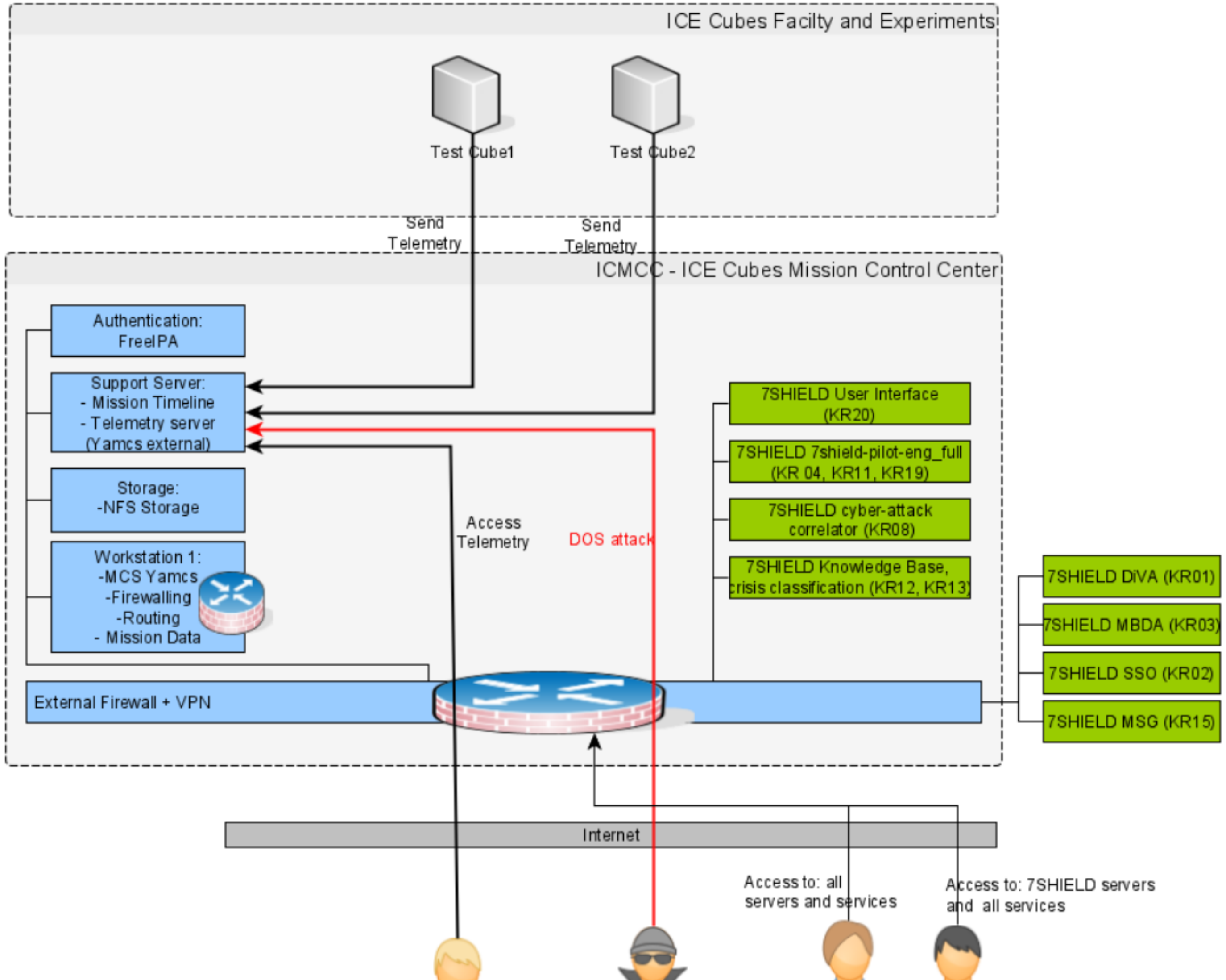
Attack

- An attacker attempt to login as the ICE Cubes operator. With Repeated malicious attempts / brute force login

Detection and Mitigation

- The 7SHIELD cyber detectors detect the brute force attack.
- The Security Officer receives notification (7SHIELD interface, emails, message) and follows the 7SHIELD mitigation tools: Emergency procedure, Impact Assessment

PUC4 ICE Cubes – Scenario 4B – DoS on Telemetry Server


ICE Cubes Facilty and Experiments
Test Cube1
Test Cube2
Send Telemetry
Send Telemetry
ICMCC - ICE Cubes Mission Control Center
Authentication: FreeIPA
Support Server: - Mission Timeline - Telemetry server (Yamcs external)
Storage: -NFS Storage
Workstation 1: -MCS Yamcs -Firewalling -Routing - Mission Data
Access Telemetry
DOS attack
7SHIELD User Interface (KR20)
7SHIELD 7shield-pilot-eng_full (KR 04, KR11, KR19)
7SHIELD cyber-attack correlator (KR08)
7SHIELD Knowledge Base, crisis classification (KR12, KR13)
7SHIELD DiVA (KR01)
7SHIELD MBDA (KR03)
7SHIELD SSO (KR02)
7SHIELD MSG (KR15)
External Firewall + VPN
Internet
Access to: all servers and services
Access to: 7SHIELD servers and all services

Setup

- Test Cubes are assigned to two users and produce telemetry, store in the ICE Cubes Telemetry servers
- Users access their Telemetry, via the ICE Cubes service "Telemetry Server Yamcs External"

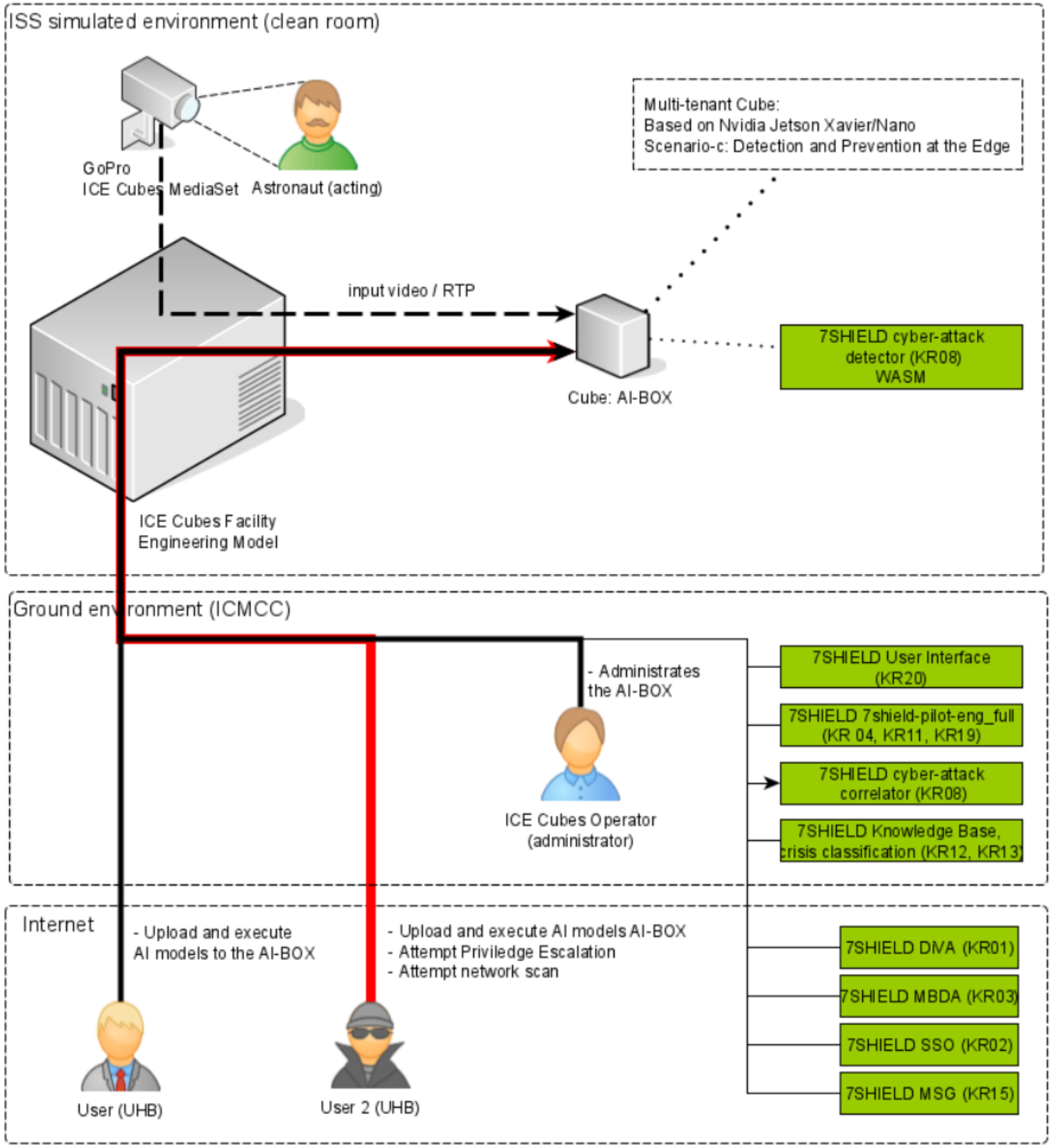
Attack

- One of the user starts a DoS attack on the Telemetry server
- Service availability is disrupted

Detection and mitigation

- The attack is detected by the CAD
- The ICE Cubes operator follow to the ERP procedures to mitigate the attack.
- The 7SHIELD MSG system alerts operators and users
- The impact assessment is provided to the security officer

ICE Cubes Scenario C overview: Detection and Prevention at the Edge


ISS simulated environment (clean room)
GoPro
ICE Cubes MediaSet
Astronaut (acting)
Multi-tenant Cube:
Based on Nvidia Jetson Xavier/Nano
Scenario-c: Detection and Prevention at the Edge
input video / RTP
Cube: AI-BOX
7SHIELD cyber-attack detector (KR08) WASM
ICE Cubes Facility Engineering Model
Ground environment (ICMCC)
- Administrates the AI-BOX
ICE Cubes Operator (administrator)
7SHIELD User Interface (KR20)
7SHIELD 7shield-pilot-eng_full (KR 04, KR11, KR19)
7SHIELD cyber-attack correlator (KR08)
7SHIELD Knowledge Base, crisis classification (KR12, KR13)
Internet
- Upload and execute AI models to the AI-BOX
- Upload and execute AI models AI-BOX
- Attempt Priviledge Escalation
- Attempt network scan
7SHIELD DVA (KR01)
7SHIELD MBDA (KR03)
7SHIELD SSO (KR02)
7SHIELD MSG (KR15)
User (UHB)
User 2 (UHB)

Setup

- Two users share a Test Cube: the AI-BOX
- The ICE Cubes operator is administrator of the Cube
- Users are allowed to a defined number of operations
- Nominal user AI operations: a webcam is streaming video to the AI-Box, the users' AI model identifies astronauts in the video and streams back the result to ground

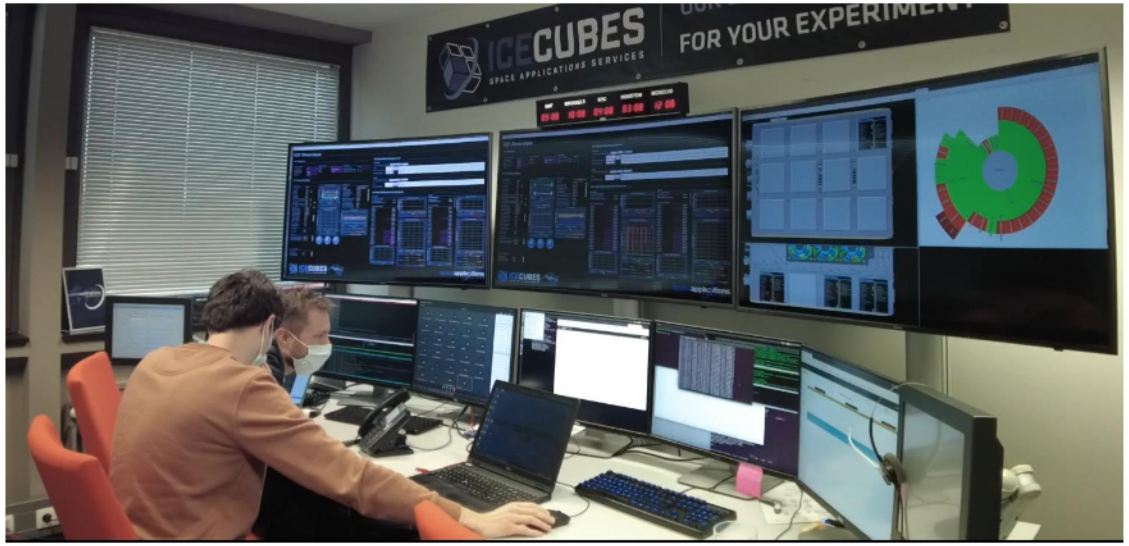
Attack

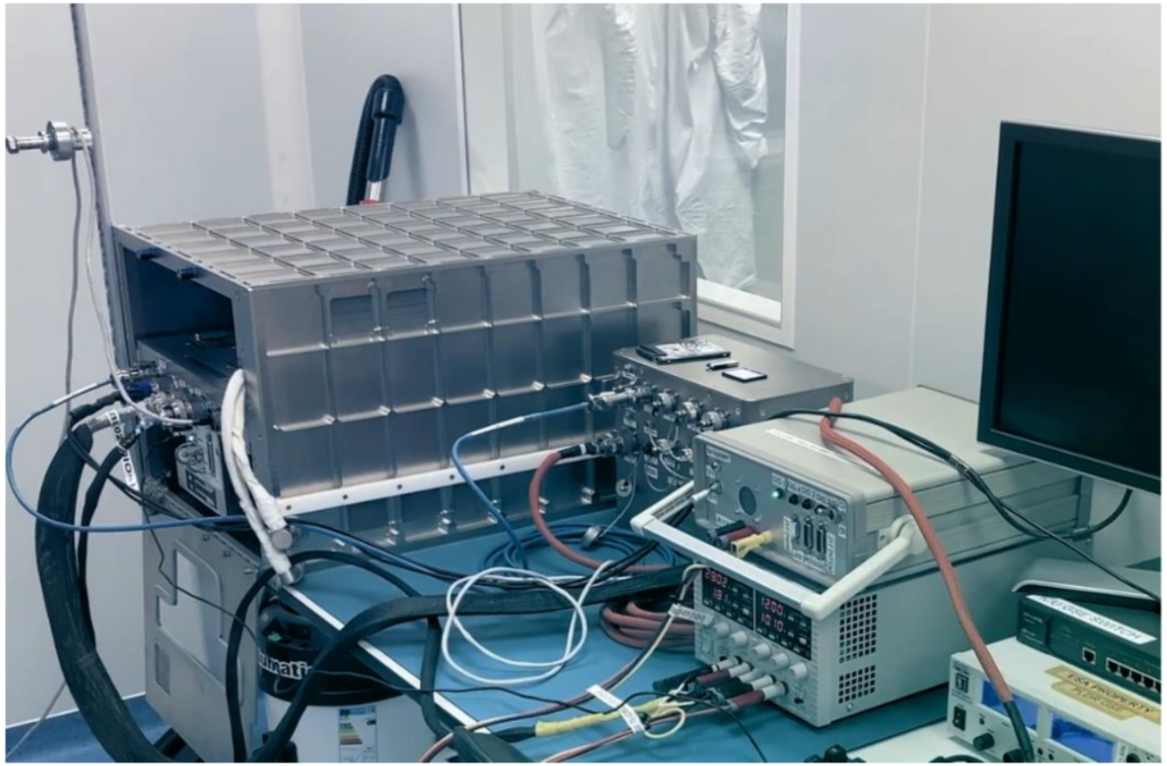
- A malicious user connects and attempts unauthorized operations:
- scan the LAN networks for devices and open services
- attempt privilege escalation within the AI-BOX

Detection and Mitigation

- Attempt 1: no 7SHIELD edge protection (WASM) is installed. Both attack (network scan, privilege escalation) succeed
- Attempt 2: the 7SHIELD edge protection (WASM) detects and prevent the unauthorized operations. The detections are communicated to the 7SHIELD correlator, and further processed by the 7SHIELD framework

ICE Cubes Pilot Achievement





- The ICE Cubes Pilot demonstration took place in the period from 15th November to 29th November 2021.
- 9 partners (SERCO, ENG, NOA, SATWAYS, CERICT, KEMEA, RESIL, SPACEAPPS, CSNOV) have been actively involved in the test’s execution
- more than 50 peoples attended to the real exercise for demonstration organized by SpaceApps on the 17 and 29 November

Result - Test Scenario Evaluation

The evaluation results show the following figures:

95% of the KPIs were effectively tested and fulfilled.

Two thirds of the Acceptance Criteria related to Key Results were effectively tested and all of them were fulfilled.

All KPIs effectively tested were fulfilled.

Further enhancement that can be taken into future versions of the 7shield framework:

Auto mitigation of the security events

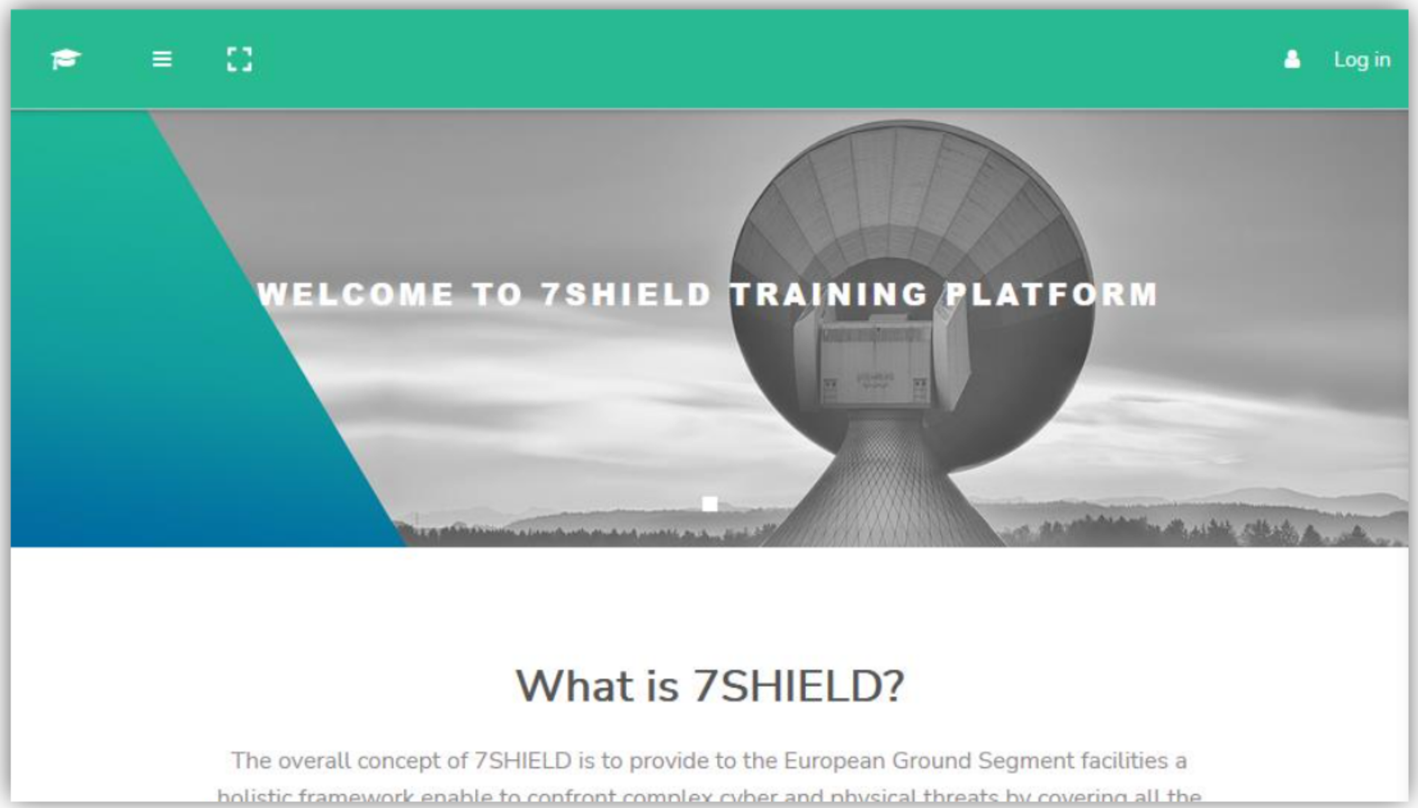
Concrete advantage of using 7SHIELD

- A unique location with dashboards centralizing the security status of the service: service status and reports, attack detections, crisis responses;
- An improved threats detection, in particular, cyber-attack detections
- Extend cyber security coverage to they system at the edge, onboard the International Space Station.
- Tracking and reporting of previous attacks, responses, updates and lessons learned;
- Remote notifications to the operators and security officer.

=> Overall an holistic framework allowing to control all the aspects of the cyber security of the ICE Cubes service

Introduction of the training platform used during the Demos

- Live access to the training platform: https://7shield.spaceapplications.com/



WELCOME TO 7SHIELD TRAINING PLATFORM

What is 7SHIELD?

The overall concept of 7SHIELD is to provide to the European Ground Segment facilities a holistic framework enable to confront complex cyber and physical threats by covering all the

For courses enrolment contact: manuela.aguzzi@spaceapplications.com

Introduction of the training platform

Overview

Pre-Crisis

During Crisis

Post-Crisis

- Focus on explaining the capabilities of 7SHIELD to targeted groups: Operators, Decision Maker, Stakeholders
- Organize training sessions for the operators surrogate in view of each Pilot demonstration scenario, performed during the execution of the project;
- Provide a comprehensive on-line manual for the final users on a public e-learning platform.
- Deliver webinars for the decision makers and stakeholders

Cyber attack scenario from pilot demo 13 December 2022

7SHIELD

https://www.7shield.eu/

Thank You

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883284.