7SHIELD

A HOLISTIC FRAMEWORK TO PROTECT GROUND SEGMENTS OF SPACE SYSTEMS AGAINST CYBER, PHYSICAL AND NATURAL COMPLEX THREATS

***Gerasimos Antzoulatos**, Centre for Research and Technology-Hellas (CERTH)*

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

7SHIELD Identity Card

- **WHO: 22 partners** – including **5 Ground Segment operators**
- **WHAT: EC H2020 Grant** under the call **SU-INFRA-2019**
- **WHEN:** September 2020 → February 2023 (30 months)
- **WHY:** In response to topic: **SU-INFRA01-2018-2019-2020** "Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe"
- **HOW:** H2020 Innovation Action

Title: **S**afety and **S**ecurity **S**tandards of **S**pace **S**ystems, ground **S**egments and **S**atellite data assets, via prevention, detection, response and mitigation of physical and cyber threats

Mission: to provide a flexible and holistic **security framework** covering all the macro-stages of crisis management (prevention, detection, response and mitigation) to protect EU Space Ground Segment Infrastructure against cyber, physical and C/P threats.

7SHIELD consortium

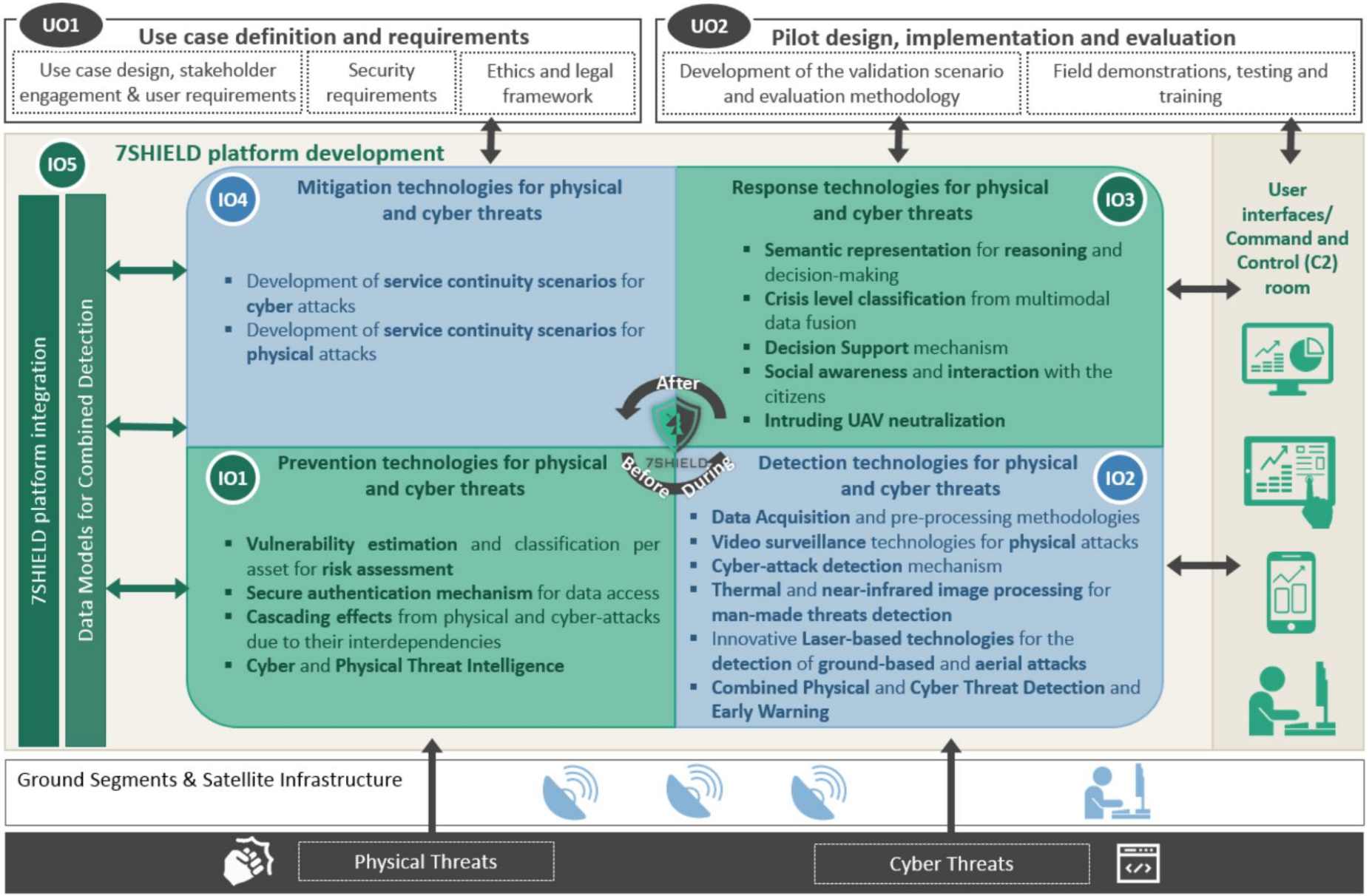
22 Partners from 12 European countries including

- ✓ 5 GSSS infrastructure owners and operators
- ✓ 3 first responder and policy organizations
- ✓ 3 academic/research institutes
- ✓ 11 industrials and technical SMEs

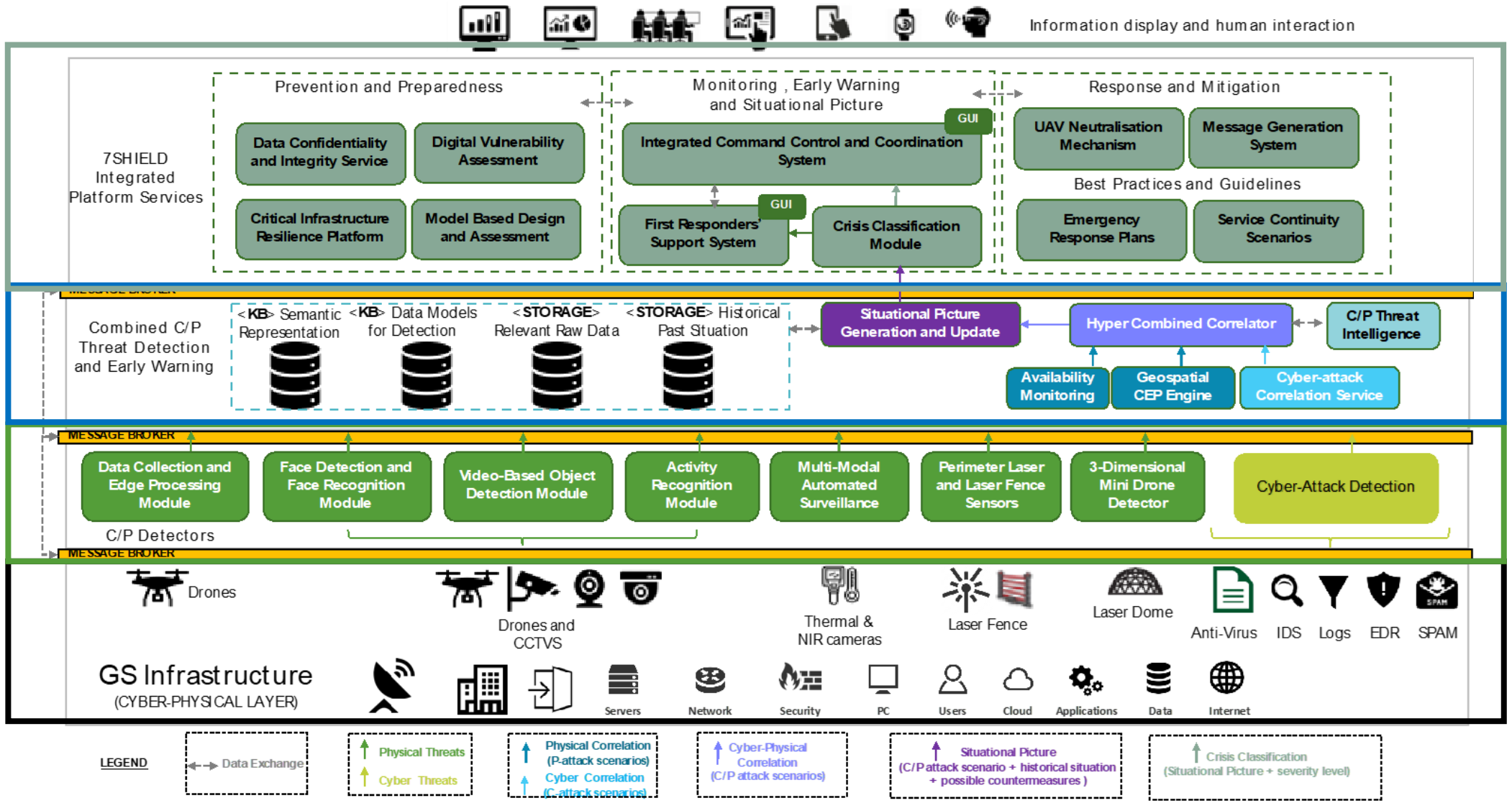
7SHIELD Landscape

- Ground segments increasingly appear as potential “new targets” for “new threats”, especially the hybrid ones (e.g. cyber-physical).
- A physical/cyber-attack would cause debilitating impact on public safety and security of European citizens and affect also other European critical infrastructure.
- Current approaches are inadequate to provide a high-level of protection/resilience of EU Ground Segments
  - do not fully exploit the recent advances in surveillance mechanisms with robotic technologies and AI
  - standards are considered outdated
  - development of a transparent user-oriented resilience-driven decision support system

7SHIELD Objectives



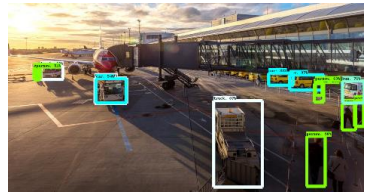
7SHIELD High-Level Architecture



7SHIELD PHYSICAL DETECTORS

- **Data collection from UAVs and processing at the edge**
  - Fully customized UAV to perform on-board image processing for object detection and identification, making use of machine learning-based techniques (e.g. DNN and CNN)

- **Face Detection & Recognition**
  - Detection of criminal suspects, or generally unwanted persons inside designated secure locations of ground stations.



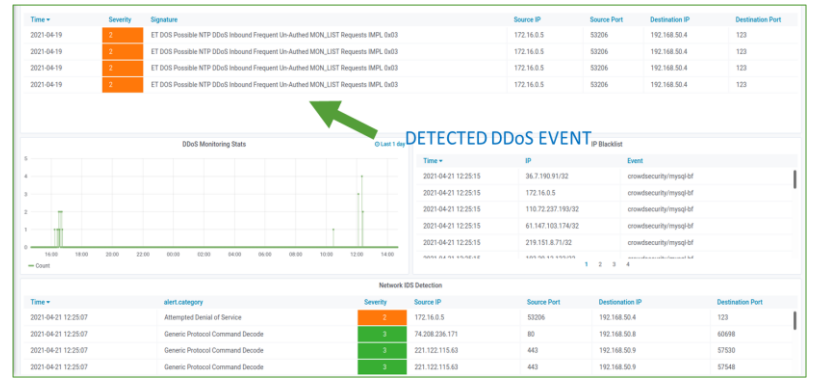
- **Video-Based Object Detection**
  - Video streams processing in order to locate and recognize objects of interest in the provided sources. The main purpose of the module is the accurate and efficient visual interpretation of the surroundings of the surveillance area

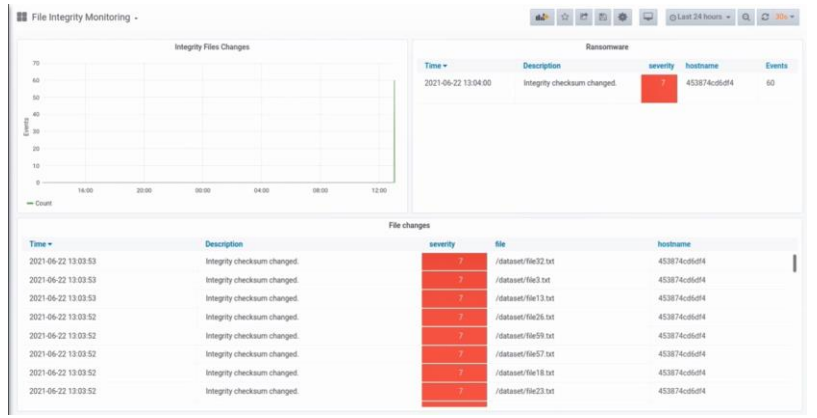
- **Human Intrusion Detection**
  - Using PTZ Camera, Perimeter Laser Sensors and Laser Fence Sensors are the only sensors able of smooth tracking by Pan, Tilt and Zoom, without any need for external PC. 3D MND for drone detection.

- **Man-Made Threats Detection**
  - Thermal and Visible Near-InfraRed (V-NIR) image processing to detect man malicious activities near the infrastructure or the surrounding grounds like detection moving objects and people during the night.

7SHIELD CYBER DETECTORS

- **Cyber-Attack Detection**
  - ➢ Combination of a **Trusted Execution Environment (TEE)** based privacy aware **Security Information and Event Management (SIEM)** solution and a set of properly selected cyber-security related probes.
- **Availability Detection**
  - Performance and **availability monitoring**, e.g., source status monitoring, correlation, metrology to **check if all sensors used by the C/P detectors are working correctly** through ping requests so as to **detect possible cyber-physical attacks to the 7SHIELD physical sources**



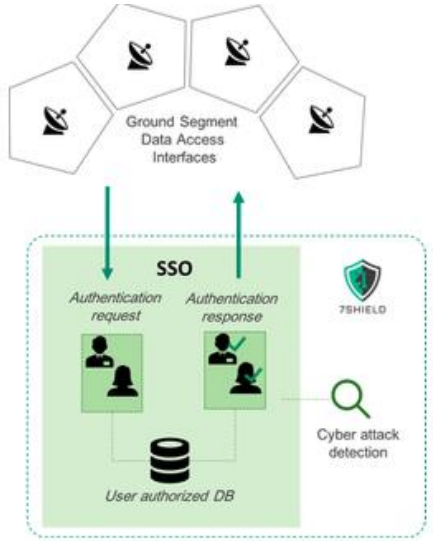


7SHIELD C/P CORRELATORS

- GEOSPATIAL CEP ENGINE
- CYBER-ATTACK CORRELATION SERVICE
- HYPER COMBINBED C/P CORRELATOR
- C/P THREAT INTELLIGENCE TOOL
- SITUATIONAL PICTURE GENERATION AND UPDATE

7SHIELD C/P PROTECTION SERVICES

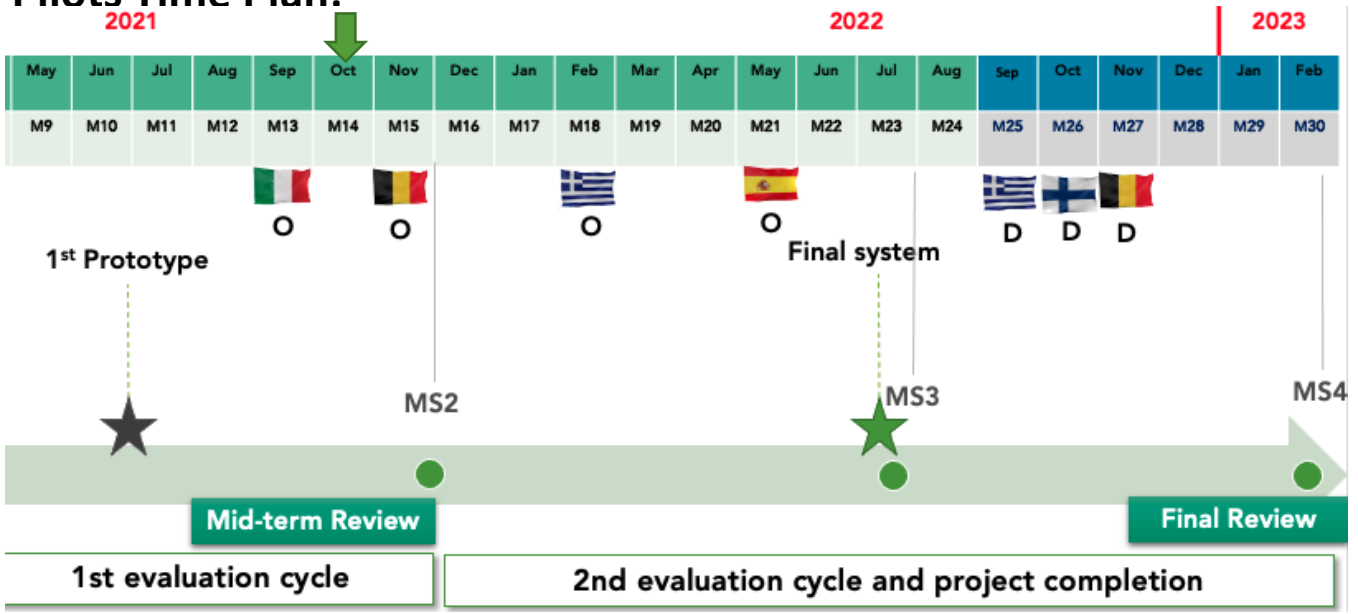
- **PREVENTION AND PREPAREDNESS**
  - Data Confidentiality and Integrity Service
  - Digital Vulnerability Assessment
  - Critical Infrastructure Resilience Platform
  - Model Based Design and Assessment
- **MONITORING AND EARLY WARNING**
  - Integrated Command Control and Coordination System
  - First Responders' Support System
  - Crisis Classification Module
- **RESPONSE AND MITIGATION**
  - UAV Neutralisation
  - Message Generation System
  - Emergency Response Plans
  - Service Continuity Scenarios



PILOTS IMPLEMENTATION and EVALUATION

- **Main Objectives:**
  - Manage all preparatory actions for actual implementation of the pilot use cases
  - Describe the application-specific and comprehensive validation framework of 7SHIELD workflow and platform
  - Present the end-users training processes

Pilots Time Plan:



Pilot	Country	Scenario Type of attack
PUC#1 FMI	Finland	Physical
PUC#2 Deimos	Spain	Physical and Cyber
PUC#3 NOA	Greece	Physical and Cyber
PUC#4 ICE Cubes	Belgium	Cyber
PUC#5 ONDA DIAS	Italy	Cyber

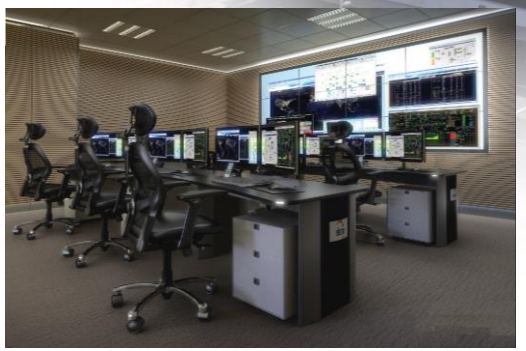
PUC#1 – FMI Arctic Space Centre (ARC)

- Location: 67°22 N, 26°39 E
- 3 satellite reception systems in operations, 1 under construction
- Server rooms with computation and storage capacity, operations room
- Over 500 instrument wide in-situ network to support satellite data calibration and validation
- Pilot story
  - Activist against governmental policy have targeted several critical infrastructures run by authorities like ARC
  - Unauthorized person enters the restricted area, and a UAV enters the premises of ARC without permission, carrying potentially harmful material on-board

PUC#2 – DEIMOS GS & Satellite infrastructure

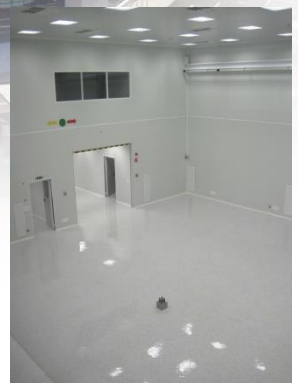
Ground station

Deimos Sky Survey
SST System



Satellite control center

Offices



Clean room (ISO 7)

Situational Factors

- Download classified or sensitive data (National, EU Restricted, NATO…..)
- Facilities in unpopulated area → Easier unauthorized access
- Facilities including expensive materials → claim for thieves
- Ground Segment Services exposed to the internet → potentially attractive to cyber attacks

Type of hazard to be mitigated

- Physical
  - Unauthorised access to DEIMOS premises: control room, data centre, ground station perimeter
  - Damage or theft of equipment
- Cyber
  - Cyber-attacks on exposed GS functions
  - Unauthorised access to GS functions
  - Disruption of critical operational functions
  - Loss or unauthorized disclosure of mission critical data

7SHIELD

PUC#3 – NOA Ground Segment in Penteli, Attica

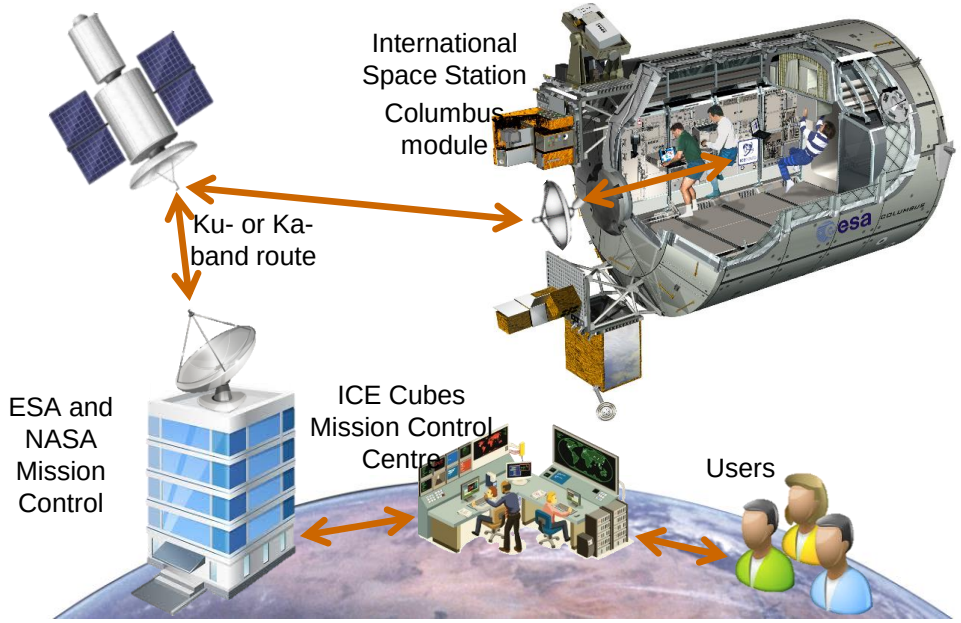
- ✓ NOA offers robust, validated services **based on EO** to the Greek government and regional, public, civil protection authorities, especially to what concerns **natural and manmade disasters early warning**, **monitoring** & **damage assessment**
- ✓ NOA provides access to raw Copernicus Sentinel satellite data from Greek, European and International users, including the industry

7SHIELD

PUC#4 – 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**



- Payload operations from ground, i.e. near real-time telemetry and telecommand -> Internet protocols: TCP/IP, UDP
- Data reception and distribution directly to the various user home bases

PUC#5 – ONDA DIAS

ONDA is a DIAS

(Data and Information Access Services)

an initiative funded by the EC and managed by ESA.

A **Cloud-based platform** with **direct access** to geospatial data – from Copernicus satellite missions and not only – enabling users to build **their applications.**

Data

- Free access to Catalogue for browsing and downloading (almost 40M datasets available)
- On request, Very High Resolution data (up-to-30 cm resolution)
- Data Access services:
  - Advanced API to allow access without full download
  - Jupyter Notebooks to help users manipulate and visualise data

Cloud Resources

- Several options available (from entry level machines, to high performance platforms, to processing clusters)
- Flexible and scalable infrastructure
- Guaranteed performance
- Availability of pre-installed Software tools for data processing or development
- Dedicated engineering support and data hosting

7SHIELD

7SHIELD

https://www.7shield.eu/

Thank You

Gerasimos Antzoulatos
(CERTH)
gantzoulatos@iti.gr