



7SHIELD

D8.13 Final brochure and InfoBoard

Work Package:	WP8 Dissemination, Impact Creation and Exploitation Plan		
Lead partner:	CS GROUP (CS)		
Author(s):	Yasmine Boulfani (CS) and Mathias Paulet (CS)		
Due date:	M30		
Version number:	1.0	Status:	Final
Dissemination level:	Public		

Project Number:	883284	Project Acronym:	7SHIELD
Project Title:	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats		
Start date:	September 1 st , 2020		
Duration:	30 months		
Call identifier:	H2020-SU-INFRA-2019		
Topic:	SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe		
Instrument:	IA		

Revision History

Revision	Date	Who	Description
0.1	15/02/2023	CS	First release of the document
0.2	20/02/2023	RG, CLS	Internal peer review feedback
1.0	20/02/2023	CS, ENG	Final release of the document after internal peer review

Quality Control

Role	Date	Who	Approved/Comment
Internal review	19/02/2023	RG	Approved
Internal review	20/02/2023	CLS	Approved

Disclaimer

This document has been produced in the context of the 7SHIELD Project. The 7SHIELD project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided 'as is' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Executive Summary

7SHIELD brochure and infoboard aim to present the benefits and expected impact of the project to the general public in easy-to-read content for non-specialists, including brief information on key 7SHIELD results and progress.

The first version of the 7SHIELD brochure and infoboard were already designed and presented in deliverable D8.5. It was showcased and distributed during the past events where 7SHIELD was presented.

The object of this document is to present the final version of the 7SHIELD brochure and infoboard, intended to present the results of the project and to continue to disseminate and communicate about the project and its sustained visibility after its closure.

Table of Contents

Executive Summary	4
1. Brochure	7
2. Infoboard	9

List of figures

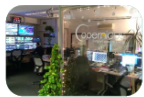
Figure 1: Back side of the final 7SHIELD trifold brochure.....	7
Figure 2: Inner side of the final 7SHIELD trifold brochure	8
Figure 3: Final 7SHIELD Infoboard.....	9

1. Brochure

The final 7SHIELD brochure is a trifold, to be easily showcased and distributed during events. It also helps to structure the information displayed.

PILOT OPERATIONAL TESTS AND DEMONSTRATIONS

The 7SHIELD framework was tested and demonstrated in five substantial pilot use cases.



ONDA DIAS platform (SERCO, Italy) in October 2021 (1st operational trial) - Simulation of three types of cyber attacks on the ONDA DIAS.



ICE Cubes Service onboard the ISS (SPACEAPPS, Belgium) in November 2021 (2nd operational trial) and December 2022 (3rd final demo) - Simulation of threat detection and mitigation on Ice Cubes Service.



National Observatory of Athens Ground Segment (NOA, Greece) in March 2022 (3rd operational trial) and September 2022 (1st final demo) - Simulation of cyber and hybrid (cyber physical) attacks on the Ground Segment assets operated by NOA's Institute for Astronomy, Astrophysics, Space Applications and Remote Sensing.



DEIMOS Ground Segment (DEIMOS, Spain) in May 2022 (4th operational trial) - Simulation of a cyber and physical attacks on DEIMOS's Ground Segment.



Arctic Space Centre (FMI, Finland) in November 2022 (2nd final demo) - Simulation of physical and hybrid (cyber physical) attacks on the Ground Segment assets of the Arctic Space Centre operated by the Finnish Meteorological Institute.



TECHNOLOGIES AGAINST PHYSICAL AND CYBER THREATS



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



www.7shield.eu



contact@7shield.eu



Follow us on

Figure 1: Back side of the final 7SHIELD trifold brochure

What is 7SHIELD ?

7SHIELD provides to the European Ground Segments of Space Systems a holistic framework that enables to confront complex cyber and physical threats against their critical infrastructure

7SHIELD FRAMEWORK

The 7SHIELD framework integrates several cutting-edge technologies from multidisciplinary and complementary fields which might be classified through the following seven (7) main thematic categories:



7SHIELD KEY RESULTS

7SHIELD framework integrates 20 key results (technology bricks) that have been developed and refined during the project according to the evaluations performed in the pilot operational tests and demos.

PREVENTION TECHNOLOGIES

Risk Assessment Tools	Secure Authentication Mechanism	Combined Threat Assessment Tool	Cyber and Physical Threat Intelligence
-----------------------	---------------------------------	---------------------------------	--

DETECTION TECHNOLOGIES

Data Collection and Edge Processing Module	Face Detection and Face Recognition Module	Video-based Object and Activity Recognition	Cyber Attack Detection Framework
Thermal and Near-infrared Image Processing for Man-made Threats Detection	Detection of Ground Based and Aerial Intruders	Combined C/P-Threat Detection and Early Warning Module	Data Models for Combined Detection

RESPONSE TECHNOLOGIES

7SHIELD Knowledge Base	Crisis Classification Module	Tactical Decision Support System
Social Awareness and Warning Message Generation	UAV Neutralisation Mechanism	

MITIGATION TECHNOLOGIES

Potential Impact from C/P Attacks and Countermeasures Knowledge Base
--

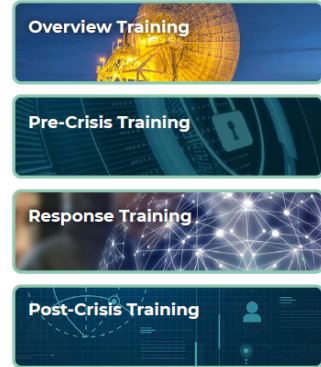
7SHIELD PLATFORM

User Interface-Common and Control	7SHIELD Integrated Platform
-----------------------------------	-----------------------------

7SHIELD TRAINING PLATFORM

The 7SHIELD Training Platform is intended to explain to end-users and other stakeholders the objectives and benefits of the 7SHIELD framework and to provide the Ground Segment Operators with technical information on the integration and use of the 7SHIELD modules.

The 7SHIELD Training Platform is operated by Space Applications Services.



7shieldtraining@spaceapplications.com

Figure 2: Inner side of the final 7SHIELD trifold brochure

2. Infoboard

The final 7SHIELD Infoboard is designed following the shape of a Kakemono, in order to be showcased during physical events.

7SHIELD
Safety and Security Standards of Space Systems, ground Segments and Satellite data assets

WHAT IS 7SHIELD ?
7SHIELD provides to the European Ground Segments of Space Systems a holistic framework that enables to confront complex cyber and physical threats against their critical infrastructure

7SHIELD FRAMEWORK
The 7SHIELD framework integrates several cutting-edge technologies from multidisciplinary and complementary fields which might be classified through the following seven (7) main thematic categories:

- Crisis Management
- Decision Support Systems
- High-level Analytics
- IoT
- Semantic Reasoning
- Sensors Technologies
- Situational Awareness

PREVENTION

DETECTION

RESPONSE

MITIGATION

TECHNOLOGIES AGAINST PHYSICAL AND CYBER THREATS

PILOT OPERATIONAL TESTS AND DEMONSTRATIONS

The 7SHIELD framework was tested and demonstrated in five substantial pilot use cases.

- ONDA DIAS platform** (SERCO, Italy) - Simulation of three types of cyber attacks on the ONDA DIAS.
- ICE Cubes Service onboard the ISS** (SPACEAPPS, Belgium) - Simulation of threat detection and mitigation on Ice Cubes Service.
- National Observatory of Athens Ground Segment (NOA, Greece)** - Simulation of cyber and hybrid (cyber physical) attacks on the Ground Segment assets operated by NOA's Institute for Astronomy, Astrophysics, Space Applications and Remote Sensing.
- DEIMOS Ground Segment** (DEIMOS, Spain) - Simulation of a cyber and physical attacks on DEIMOS's Ground Segment.
- Arctic Space Centre** (FMI, Finland) - Simulation of physical and hybrid (cyber physical) attacks on the Ground Segment assets of the Arctic Space Centre operated by the Finnish Meteorological Institute.

7SHIELD TRAINING PLATFORM

The 7SHIELD Training Platform is intended to explain to end-users and other stakeholders the objectives and benefits of the 7SHIELD framework and to provide the Ground Segment Operators with technical information on the integration and use of the 7SHIELD modules.

- Overview Training
- Pre-Crisis Training
- Response training
- Post-Crisis Training

7ShieldTraining@spaceapplications.com

7SHIELD KEY RESULTS

PREVENTION TECHNOLOGIES

- Risk Assessment Tools
- Secure Authentication Mechanism
- Combined Threat Assessment Tool
- Cyber and Physical Threat Intelligence

DETECTION TECHNOLOGIES

- Data Collection and Edge Processing Module
- Face Detection and Face Recognition Module
- Video-based Object and Activity Recognition
- Cyber Attack Detection Framework
- Thermal and Near-Infrared Image Processing for Man-made Threats Detection
- Detection of Ground Based and Aerial Intruders
- Combined C/P Threat Detection and Early Warning Module
- Data Models for Combined Detection

RESPONSE TECHNOLOGIES

- 7SHIELD Knowledge Base
- Crisis Classification Module
- Tactical Decision Support System
- Social Awareness and Warning Message Generation
- LIUV Neutralisation Mechanism

MITIGATION TECHNOLOGIES

- Potential Impact from C/P Attacks and Countermeasures Knowledge Base

7SHIELD PLATFORM

- User Interface-Common and Control
- 7SHIELD Integrated Platform

www.7shield.eu contact@7shield.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 885284.

Figure 3: Final 7SHIELD Infoboard



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