7SHIELD

D1.5 - Public final activity report

Work Package:	WP1		
Lead partner:	ENG		
Author(s):	Gabriele Giunta (ENG), Emilia Gugliandolo (ENG)		
Due date:	February 2023		
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 1st, 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		

Horizon 2020
European Union Funding
for Research & Innovation

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

Revision History

Revision	Date	Who	Description
0.1	06/02/2023	ENG	First release of the template
0.2	16/02/2023	ENG, ALL	First round of contribution
0.3	23/02/2023	ENG, ALL	Second round of contribution
0.4	27/02/2023	ENG, CERTH	Version ready for internal peer review
1.0.	10/03/2023	ENG	Final version

Quality Control

Role	Date	Who	Approved/Comment
Internal reviewer	09/03/2023	CERTH	Document accepted, only minor changes suggested

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

This deliverable provides an overview of the 7SHIELD project progress carried out by the project consortium during the last period, namely from January 2022 (M17) to February 2023 (M30), starting from the content of **D1.3 – Mid-term review and progress report**, which was submitted in April 2022 (revised version), after having received and integrated feedback and recommendationds from EC experts during the mid-term review meeting. Specifically, it documents:

a) The 7SHIELD objectives.
b) A summary of the project's results in terms of scientific and technological achievements.
c) The communication and dissemination actions.
d) A summary of the provided research ethics guidelines and recommendations so as the project's result be compliance with national or EU regulations.

Table of Contents

Definitions and acronyms

3DMND	3-Dimensional Mini drone
ADM	Availability Detection Monitoring
AC	Availability Correlation
AP	Average Precision
AR	Activity Recognition
AUC	Area Under Curve
C2	Command and Control Center
CA	Consortium Agreement
CAC	Cyber-Attack Correlation
CAD	Cyber-Attack Detection
CTID	Cyber-Threat Intelligence Detector
CC	Control Center
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CNN	Convolutional Neural Network
CPTI	Cyber-Physical Threat Intelligence
C/P	Cyber/Physical
DIAS	Data and Information Access Service
DiVA	Digital Vulnerability Assessment
DNN	Deep Neural Network
DoA	Description of Action
DPIA	Data Protection Impact Assessment
EC	European Commission
ECSCI	European Cluster for Securing Critical Infrastructures
EU	European Union
FDR	Face Detection and Recognition
FH	Flying Hunter
FoV	Field of View
FPR	False Positive Rate
FPS	Frames per second
FRSS	First Responders Support System
GA	Grant Agreement
G-CEP	Geospatial Complex Event Processor
GUI	Graphical User Interface
HCC	Hyper-Correlation Component
IA	Innovation Activity
IC3	Integrated Command Control and Coordination
IMA	Impact-making Activity
IMO	Impact-making Objective
IO	Innovation Objective
IR	Infrared
LFS	Laser Fence Sensor
KPI	Key Performance Indicator
KR	Key Result
MBDA	Model-based Design Assessment

MMAS	MultiModal Automated Surveillance
NIR	Near-InfraRed
ODE	Object Detection at the Edge
PC	Project Coordinator
PLS	Perimeter Laser Sensor
PTZ	Pan-Tilt-Zoom
PUC	Pilot Use Case
ROS	Robot Operating System
SC	Scientific Coordinator
SGS	Satellite Ground Station
SPGU	Situational Picture Generation & Update
TDSS	Tactical Decision Support System
TM	Technical Manager
TPR	True Positive Rate
UA	User-oriented Activity
UAF	Unified Alert Format
UAV	Unmanned Aerial Vehicle
UI	User Interface
ULS	Universal Local Server
UO	User-oriented Objective
UTD	Universal Tactical Display
VNIR	Visible Near-InfraRed
VOD	Video-based Object Detection
WP	Work Package

1. Introduction

This deliverable provides an overview of the 7SHIELD project progress carried out by the project consortium in the second period, namely from from January 2022 (M17) to February 2023 (M30), starting from the content of ***D1.3 – Mid-term review and progress repo*rt**, which was submitted in April 2022 (revised version), after having received and integrated feedback and recommendationds from EC experts during the mid-term review meeting.

The deliverable is structured in the following main sections:

- Section 1 contains the document introduction.
- Section 2 describes the project objectives achieved in the first period with respect to the overall 7SHIELD objectives, as stated in the Grant Agreement. Moreover, a description of the project's results for each of the three areas of interest, namely Pre-Crisis Management, Crisis Management and Post-Crisis Management, is provided.
- Section 3 reports communication and dissemination actions during the first period, including meetings and all the relevant events.
- Section 4 provides a summary of the provided research ethics guidelines and recommendations so as be compliance with national or EU regulations.
- Finally, section 5 presents the conclusion.

2. Overview of the project objectives for the period

2.1. Project objectives

2.1.1. *Innovation objectives (IOs) and innovation activities (IAs)*

Innovation Objectives	Innovation Activities	KPIs
IO1. Prevention technologies for physical and cyber threats	**IA1.1** Vulnerability estimation and classification per asset for risk assessment (KR01)	**KPI 1.1.1** Integrated Scientific Models; **KPI 1.1.2** Ingested datasets size.
	IA1.2 Secure authentication mechanism for data access (KR02)	**KPI 1.2.1** Success in authentication/authorisation attempts according to the different user identity profiles.
	IA1.3 Cascading effects from physical and cyber-attacks due to their interdependencies (KR03)	**KPI 1.3.1** Number of identified threats due to cascading effects identified in pilot sites.
	IA1.4 Cyber and Physical Threat Intelligence (KR04)	**KPI 1.4.1** Accuracy, Error rate.

Achievements
IA1.1 – Details on those activities were provided in D1.3, due at M20. Target value related to KPIs 1.1.1 and KPI 1.1.2 was fully achieved (100%) within the first period. In addition, the cyber risk assessment tool (DiVA) was successfully integrated within the 7SHIELD framework and fully validated during ALL the Operational Test (besides NOA) and Demo pilots. Regarding the physical (and natural hazards) risk assessment tool (CIRP-RAT), it was successfully integrated within the 7SHIELD framework and fully validated during the FMI Demo Pilot.
IA1.2 – Details on those activities were provided in D1.3, due at M20. Target value related to KPIs 1.2.1 was fully achieved (100%) within the first period. In addition, the secure authentication mechanism was successfully integrated within the 7SHIELD framework and fully validated during ALL the Operational Tests and Demo Pilots.
IA1.3 – Details on those activities were provided in D1.3, due at M20. The cascading effects tool (MBDA) was successfully integrated within the 7SHIELD framework and fully validated during ALL the Operational Tests and Demo Pilots. The final release of the functionality for the analysis of cascading effects was tested during the demo pilots: a graph of cascading effects from threats was provided in the tool user interface. Thus, the percentage of achievement of the KPI 1.3.1 is 100% (fully achieved).
IA1.4 – Details on the activities done in the first period were provided in D1.3, due at M20. In the last period, implementation of the threat intelligence core was developed and a first prototype of the Threat Intelligence service was evaluated in the SERCO Operational Tests as well as in FMI and SPACEAPPS Demo Pilots. These two pilots helped in the collection of some feedbacks to improve the performances of the tool. In fact, a refinement of the Deep learning NLP algorithm for text analysis was performed and the support to another source was implemented (Reddit). The latest version was used to evaluate the performances of the CPTI framework against state-of-the-art results, it was applied the following protocol: each class of the Twitter Dataset (used to train the Threat Intelligence service) was split in training and testing according to the number of samples reported in the original paper (Simran, K., Prathiksha, B., Vinayakumar, R., Soman, K. P. - Deep Learning Approach for Enhanced Cyber Threat Indicators in Twitter Stream. SSCC, 2020). The training and the testing split of the original paper are not publicly available. For this reason, it was decided to report only the accuracy without considering other metrics. However, the entire procedure was repeated 5 times to have a stronger evaluation of the proposed solution in terms of accuracy results. The proposed CPTI framework raised an

overall improvement of 1% in terms of accuracy with respect to the best result proposed in the paper and around 5% with respect to the baseline. The obtained results confirm the effectiveness of the TI tool achieving the KPI related target (100%).

Innovation Objectives	Innovation Activities	KPIs
IO2. Detection technologies for physical and cyber threats	**IA2.1** Data acquisition and pre-processing methodologies at the edge (KR05)	**KPI 2.1.1** Duration of continuous inspection operation of each type of agent (UAV edge processor) in one battery charge; **KPI 2.1.2** Improvement of autonomous offline operation (no communication with IC3 systems); **KPI 2.1.3** Amount of time needed to perform surveillance coverage mission, examining cooperative (with other 7SHIELD components) navigation and control scenarios; **KPI 2.1.4**: Size of monitored area per agent (for multi-agent mission) during 24h (10 missions – 2.5km^2 per mission); **KPI 2.1.5** Accuracy and detection latency of on-board object detection and identification algorithms (process to the edge).
	IA2.2 Video surveillance technologies for physical attacks (KR06-KR07)	**KPI 2.2.1**: Accuracy and detection latency. For detection accuracy: False Positive Rate (FPR), True Positive Rate (TPR) and Area Under Curve (AUC); For detection latency: Frames per seconds (FPS).
	IA2.3 Cyber-attack detection mechanism (KR08)	**KPI 2.3.1**: # of cyber-attacks with high impact (based on technical/scientific literature) detected; **KPI 2.3.2**: # of misuse cases with high impact

		(based on technical/scientific literature) detected; **KPI 2.3.3**: Performance penalty of TE technology.
	IA2.4 Thermal and near-infrared image processing for man-made threats detection (KR09)	**KPI 2.4.1**: Classical detection measures (Recall, Precision, F1-Measure) and tracking measures (Stiefelhagen et al., 2006) and real-time performance measures.
	IA2.5 Innovative Laser-based technologies for the detection of ground-based and aerial threats detection (KR10)	**KPI 2.5.1**: Taking pictures of intruders (human, vehicle and drone), using slaved PTZ camera, and following up throughout the track.
	IA2.6 Combined Physical and Cyber Threat Detection and Early Warning (KR11)	**KPI 2.6.1**: Detection of the artificially added threat data in the "normal" logs. **KPI 2.6.2:** Accuracy and correlation latency for physical events.

Achievements

IA2.1 – Details on those activities were provided in D1.3, due at M20. ALL the KPIs, apart from KPI 2.1.5, were successfully achieved during the first period. Regarding the second period, the main activities includes:

- Preparation for pilot in DEIMOS (Spain).
- Pilot execution in DEIMOS (Spain).
- Evaluation of pilot flights in DEIMOS & evaluation of the communication protocols.
- Communication tests with the 7SHIELD control room.
- Final integration tests between ODE & DCEP components.
- Drone wire connection improvements (Hardware).
- Finalisation of the integration between cameras gimbal and Drone stick.
- Finalisation of the communication test between DCEP and control room
- Integration Tests with updated AI and object detection (real data)
- Updates on Hovering operation
- Adjustment of parameters based on experiments' feedback, for both the localization algorithm and the PID controller for tracking
- Integration of FLIR's gimbal operations into RC transmitter
- Extension of RC transmitter's range using new module (protocol)
- Preparation for pilot in FMI (Finland).
- Pilot execution and final demonstration in FMI (Finland).

Finally, during the pilot activity in FMI (November 2022), we demonstrated a fully operational version of KR05. The object detection and identification algorithms (KR07) deployed in the embedded processor of the 7SHIELD UAV. After a number of validation trials (laboratory and field), and during the PUC 1 demonstration we achieve the real time thread detection and identification of an intruder and the corresponding alert transmitted to the 7SHIELD control room. The KPI 2.1.5 was successfully achieved (100%) and approved.

IA2.2 – The main achievements in the reporting period [M17-M23] were the following:

- Development of the final version of the Face Detection and Recognition (FDR) module. The system is initialized with a video stream, but it also can support on-demand analysis of video files in an offline processing scenario. Enabled through state-of-the-art deep learning facial recognition models, the FDR module can monitor critical infrastructure areas, where the human faces captured by CCTV cameras will be first detected by the Face Detection component and then further processed by the Face Recognition component in order to verify authorized matches with an authorised personnel database. In order to create the gallery specific requirements have to be met when capturing the photos. To achieve maximum performance and robustness to pose variations several photos of the known individuals' faces must be collected, thus, specific guidelines were given to the pilot owners in order to prepare the sets. In online video stream Input, a large number of instances that belong to the same person may appear multiple times in an input video segment through sequential video frames. In addition, recognizing each detected instance of a person's face separately provides no means of information aggregation, is non-intuitive and is sensitive to outliers. To solve the problem of the added overhead of FR and to lessen the impact of outliers the final version of the component is equipped with a facial clustering mechanism, in order to cluster similar faces together and base decisions on clusters instead of single samples. The processing pipeline of FR has been adapted accordingly to support clustering and now consists of four main functions: (a) facial feature extraction, (b) feature clustering, (c) cluster matching and (d) distance thresholding. The experimental evaluations of the FDR module in terms of its performance to detect faces reached 95.5% (mean Average Precision - mAP) while the recognition of human faces persons has climbed to 99.4% (mean accuracy). Regarding the detection speed, the FDR succeed to analyse 30 Frames per Second (FPS). The FDR component was also evaluated outside of the lab in two operational tests and two demonstrations that simulated physical attacks on ground stations. Therefore, for the FDR module the KPIs have been fulfilled.
- Development of the final Video-based Object Detection (VOD) and Activity Recognition (AR) modules. The VOD module processes the video input at a frame level and identifies and localizes every object of interest depicted inside every frame. The models being used are Yolov4[1] and EfficientDet[2] which are both deep learning algorithms. The detection results which are related to human presence are further propagated to the AR module. The AR module is responsible to identify any suspicious and potentially harmful activity being taken upon the detected person(s) in a sequence of frames. The AR included 3 classes of interest (running, walking and standing). The main objective of these modules is to visually interpret the surrounding area in a fast, reliable and automatic approach in order to assist the personnel of the premises in detecting and reporting dangerous situations. Object Detection at the Edge (ODE) module is tightly connected to the previous modules and more specifically to the VOD, with the main difference from the latter being the necessity to function in a resource limited environment of the embedded GPU of the project's UAV. We evaluated the efficiency performance of the VOD module when deployed at the edge in order to examine whether the same model could be used or the specific restrictions at the edge imposed the use of a different, lighter model. At the end, it was decided that the same model can be deployed at the edge as well as in workstations with varying efficiency.
- Regarding the VOD module 2 models have been trained and deployed to cover all possible use cases. Custom dataset were compliled so as to encompass the user and project's requirements. The first model included all object of interest at an outdoor environment, which included 5 objects, while the other one included objects found indoors, with 2 objects being including. Both models were evaluated using the mean Average Precision (mAP) metric. The first model achieved a mAP of 69.57% for 5 classes while the later model achieved a mAP of 85.73%. The AR included 3 classes of interest and used heuristic methods to decipher the action being performed by each detected person. Finally, ODE utilized the same model as the VOD but was adjusted to the embedded GPU environment. The speed of the VOD models was 25 and 30 fps for the Yolov4

[1] Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). Yolov4: Optimal speed and accuracy of object detection. arXiv preprint arXiv:2004.10934.

[2] Tan, M., Pang, R., & Le, Q. V. (2020). Efficientdet: Scalable and efficient object detection. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 10781-10790).

(outdoor) and EfficientDet (indoor) respectively when tested on an average Nvidia GeForce RTX 3090 card, while the Yolov4 model ported to the embedded system (Jetson AGX Xavier) dropped to 8.4 fps. AR was extremely fast and contributed minimally to the whole pipeline processing time. The KPIs for mAP and FPS for the indoor detection modules has been achieved their target value (≥80% and ≥ 20 FPS). However, for VOD and ODE outdoor detection seem that the mAP KPI was not met its target. The reason for this was that the custom-compiled dataset that was used for the models training, was too challenging, as it included many small object instances. However, this low mAP detection did not affect the generalisation ability of the VOD and ODE modules to accurately detect unknown objects of interest during their evaluation in the demonstrations of the pilot sites. Further details on those activities were provided in D1.3, due at M20.

IA2.3 –The main achievement in the reporting period was the improvement of the Cyber-Attack Detection framework (CADF) which consists of three main components: a) the Cyber-Attack Detection Layer; b) the Cyber-Attack Correlation Layer and c) the Graphical User Interface. The Cyber-attack dashboards were successfully integrated with the SERCO SSO. In order to meet the use cases requirements, ad hoc correlation rules were defined and successfully tested during the Operational Tests and Demo Pilots. In particular, within the SPACEAPPS pilots, a novel mechanism for combination of proactive and reactive mechanisms was tested to push security enforcement at the edge and to protect sensitive information.

Regarding KPI 2.3.1, as shown in the following table, the CADF was successfully tested against 10 high impact attacks (100% achieved). To satisfy KPI 2.3.1, a set-test case of well-known high-impact attacks, which were detected through the 7SHIELD project, was used.

High Impact Attack	Status
DoS/DDoS	Detected
Unauthorized Access	Detected
Malware	Detected
0-Day Ransomware	Detected
Targeted Ransomware	Detected
Packet Sniffing	Detected
Privilege Escalation	Detected
File Integrity Alteration	Detected
Brute Force Attack	Detected
Jamming/Spoofing	Detected

Regarding KPI 2.2.2, as shown in the following table, the CADF was successfully deployed and tested in the Pilot Use Cases: SERCO, SPACEAPPS, NOA, DEIMOS and FMI, for a total of 10 misuse cases (100% achieved).

Misuse Case	Status
PUC5 - Operational Test Scenario 2 – Detection of Ransomware attack	Completed
PUC5 - Operational Test Scenario 3 – Detection of network level DDoS attack + IP blacklist	Completed
PUC4 - Operational Test Scenario 3 – Privilege Escalation	Completed
PUC4 - Demo Scenario C – Privilege abuse prevention and detection	Completed
PUC3 - Operational Test Scenario 1 – Detection of application level DDoS attack	Completed
PUC3 - Operational Test Scenario 2 - Unauthorized access to the network	Completed
PUC3 - Demo Scenario 3 – RF Interference	Completed
PUC2 - Operational Test Scenario 2c – Login from unexpected location	Completed
PUC2 - Operational Test Scenario 2a – Brute Force Attack	Completed
PUC1 - Demo Scenario 2b – Jamming detection	Completed

Finally, as for KPI 2.3.3 (Performance penalty of TE technology) to fulfil the KPI, we measured the execution time of a procedure that detects a malicious string (a SQL query) in logs. We fixed the length of the string to 10k bytes and compared a native solution with a TE-enabled solution. Results showed an overhead of 8.7%.

IA2.4 – Further details on those activities were provided in D1.3, due at M20.
The GA required a classification minimum threshold of 0.5 F1-score, with the data set produced during the 7SHIELD project was achieved a F1-score of 0.724, the values of Multiple Object Tracking Accuracy (MOTA) achieved also supplanted the requested value of 30% with a value of 68% as such the KPI 2.4.1 were successfully achieved (100%). The MultiModal Automated Surveillance (MMAS) system was successfully integrated with the 7SHIELD and tested during the PUC1 in Finland.

IA2.5 – The main achievements in the reporting period are the deployment of the final prototypes of the Perimeter Laser Sensor V3.0 (PLS), the Laser Fence Sensor V3.0 (LFS) and the 3-Dimensional Mini drone detectors V3.0 (3D-MND). Since in the first reporting period, development and implementation work on all sensors were completed, and in-house field trials commenced. Pilot trials were carried out at PUC2 (DEIMOS) in Spain and PUC1 (FMI) in Finland during the second reporting period. All trials were successful and KPI 2.5.1 was fully achieved (100%).

IA2.6 – the main achievements in the reporting period are the following:

- ADM and AC are fully developed, and SSL secure connections are developed and integrated. ADM has been successfully evaluated during ALL the Operational Tests and Demo pilots while AC was tested in DEIMOS operational test, as well as in NOA, FMI, and SPACEAPPS demonstrations.
- Development of a first (test) correlation rule for the Hyper-Correlation Component (HCC) that mixes cyber security alerts from the Cyber-Attack Correlation (CAC) and Availability alerts from the Availability Detection Module (ADM), the Geospatial Complex Event Processor G-CEP and itself too (HCC). The HCC module was integrated into the 7SHIELD framework and tested in NOA, FMI, and SPACEAPPS Demo Pilots.
- During the reporting period, the Geospatial Complex Event Processor (G-CEP) component was further enhanced in order to support the receiving and correlation of the events that will be detected by the physical sensors. In this direction, the number of functionalities that have been designed, were implemented and fine tunned. In more detail, the support of the format of the messages that will be produced by the physical sensors was finalized. The correlation rules/patterns that were identified in the previous period have been implemented, enhanced and finally tested and validated through the pilots conducted.
- Finalisation of functional specifications of the Radio Frequency Interference Detection and Identification (RFIDI) module. The aim of the RFIDI module is to generate events indicating anomalies in the reception of the Ground Station antenna related to frequency Interference. Development of RFIDI as a (simulated) event detector under the 7SHIELD Cyber-Attack Detection Framework. The RFIDI functionality and integration in the 7SHIELD framework were tested during NOA and FMI pilots. The RFIDI module successfully detected 100% of the simulated frequency interference events used in both Pilot Use Cases. The events generated by RFIDI were further correllated by the CAC and HCC resulting in alerts in the 7SHIELD user screens.
- In the 1st period, the effort focused on the development of the 1st prototype of the Situational Picture Generation & Update (SPGU) module which aims to provide an enhanced Situational Picture for the protected Satellite Ground Segments. The main sources of information exploited by the SPGU are represented by the 7SHIELD correlation/detection modules (e.g. cyber, physical and cyber-physical) and by any 7SHIELD tool able to provide useful information that can contribute to the generation of the Situational Picture. The SPGU correlates the information provided by all the correlators (e.g. CADF, G-CEP, ADM/AC, HCC) with those coming from the prevention and preparedness tools, such as MBDA, DiVA, CIRP. SPGU is also able to heuristically correlate geographical and networking information to detect the assets impacted by a specific event and to calculate some new risk assessment data. The quality of middleware also updates the status of events (e.g. new, mitigating, managed), to have the tools always aligned within the framework. From M17 – January 2022 up to M30 – February 2023, all the 7SHIELD detectors and correlators have been integrated with SPGU. Furthermore, even risk/resilience assessment and mitigation tools have been integrated. Added hazards support for communication with ENGAGE and an alignment component to ensure tools are always up to date with each other. The management (conversion and calibration) of geospatial coordinates has been

improved while support for heuristic detection of assets impacted by events both in geospatial and networking terms has been added. Functions have also been added for calculating risk assessment data which are updated over time with each event reception. Support for automatic management of certificates for communication with SSL/TLS protocols has been added and all third-party services have been wrapped to have a Single Entry Point (API Gateway). The Knowledge Base from the post-crisis management layer was also integrated. The interactions with DiVA and MBDA for the management of risk assessment data such as weaknesses and cascading effects graphs and the management of assets/areas have been correctly integrated. The technology stack used is Spring Framework for JAVA, Tomcat Web Container, PostGIS for data persistence, Docker for containerization. SPGU correlates 100% of assets and events if the assets are correctly configured with latency less than 2 sec.

Summarizing:

- KPI 2.6.1 partially achieved. Detection on scenarios fully achieved (100%) while on machine learning partially achieved (50%). Model needs to be tested (difficulty to found a cyber-physical dataset).
- KPI 2.6.2: fully achieved. During pilot implementation all alerts were identified, analyzed and correlated on time, turned into events with high success rate (low false alarm), feeding on time the HCC module for further correlation (if applicable) with the cyber alerts. The whole process was implemented in (near) real time (<1sec), informing the user for further activities/decisions. .

Innovation Objectives	Innovation Activities	KPIs
IO3. Response technologies for physical and cyber threats.	**IA3.1** Semantic representation and linking for reasoning and decision-making (KR12)	**KPI 3.1.1**: Quality (e.g. Content Quality Metric, Structural Quality Metric (Raad & Cruz, 2015) and completeness metrics will be applied in the ontology. Response time will be computed in the population tool. Accuracy and precision will be calculated in the reasoning process.
	IA3.2 Crisis level classification from multimodal data fusion (KR13)	**KPI 3.2.1**: Precision and accuracy in the crisis level estimation.
	IA3.3 Decision Support mechanism (KR14)	**KPI 3.3.1**: Quickness and quality of information provided and calculated in the reasoning process.
	IA3.4 Social awareness and interaction with the citizens (KR15)	**KPI 3.4.1**: user acceptance rating during pilot testing and debriefing. Increase engagement with messages (likes, shares, comments, replies, link follows, etc.).
	IA3.5 Intruding UAV neutralisation (KR16)	**KPI 3.5.1**: Flying Hunter flies to the intruding drone on the command of the operator, homing on to the drone,

<table>
<tr><td></td><td></td><td>catching the drone and bringing it back to designated ground area.</td></tr>
<tr><td colspan="3"><b>Achievements</b></td></tr>
<tr><td colspan="3"><b>IA3.1 –</b> Regarding the reporting period, the effort was focused on the integration between the 7SHIELD Knowledge Base (KB) and the other modules, which will gain valuable knowledge, by the exploitation of the historical crisis events stored data. To this, a rest API service has been developed to facilitate the knowledge retrieval from the 7SHIELD KB. Specific endpoints for different SPARQl rules were structured to filter the data based on spatio-temporal criteria such as dates, locations and event IDs. The response messages are formed as reports that contain details for each specific events that were observed (severity, type of threat, information of interest, analysers and locations). These reports are forwarded to the SPGU (IA2.6) for further elaboration and visualisation in the CPTMD dashboard provided to the operators. The process was successfully demonstrated and evaluated through the NOA and DEIMOS Operational Test pilots as well as in all the Demo pilots (NOA, FMI and SPACEAPPS). Additionally, the historical stored data would be useful to re-train machine learning models that are able to assess the severity level of a P/C crisis event. Therefore, to cover this need for communication between KB and CRCL (IA3.2), minor updates took place both in the JSON to RDF converter and to the ontological structure. Hence, by using a rest API service, the stored information can be acquired and employed for the machine learning re-training process.
The 7SHIELD KB is capable to answer almost all CQs, by satisfying 89%, which exceeds the minimum targeted value (75%). Additionally, using OOPS (pitfall scanner) to enhance quality evaluation, we corrected all the important and critical pitfalls that we detected. Although, it is hard to set a specific baseline to the Quantitative criteria, however, using a tool (Ontometrics) we can evaluate some of the core metrics of the ontology. The metrics include the axioms (615 in our ontology with 261 logical acioms), the classes (100) and both object (37) and data (22) properties. The description logic expressivity follows the ALCHI(D) type. Combining these metrics we have the following analytical results regarding the attribute richness (0.25: explained because this is a lightweight ontology) the iheritance richness (0.85: the knowledge is well grouped in several categories and subcategories) and the realationship richness (0.34: mainly class-subclass relations). Therefore, the KPIs have been achieved.</td></tr>
<tr><td colspan="3"><b>IA3.2</b> – In the reporting period (M17-M23) the efforts were focused on the fusion of information from other detectors, such as Availability Detection Monitoring which provides information about the status of the sensors, or information concerning the vulnerabilities of the assets of the SGS that are exposed to particular attacks. Therefore, the Crisis Classification module was enhanced with a decision fusion logic in order to support decision-making process during the crisis and be customised efficiently in the specific pilot use cases. Moreover, the Annotation Tool was upgraded and equipped with the functionality to acquire information from historical crisis events (P/C attacks) that are stored in the 7SHIELD Knowledge Base. The aim is to reinforce learning of the machine learning models by exploiting the stored knowledge of the classified past P/C extreme events in terms of their severity level.
In total 1088 cyber-attack scenarios and 762 physical attack scenarios were annotated by the experts in the 5 pilot sites of SGS. The experimental evaluations exhibit that the accuracy of the ML models to classify the cyber-attacks in terms of their severity fluctuates between 69.56% to 95% depending on the pilot use case and the classifier. In the case of physical attacks, the accuracy of the models fluctuates between 65.38% (Random Forest) to 80.76% (SVM). Hence, in the case of the cyber-attack scenarios, the accuracy of the baseline approach is approximately 61% while in the case of the physical attacks scenarios it reaches 68.85%. Hence, the KPI 3.2.1 was achieved. Finally, during the pilot demonstrations the performance of the Crisis Classification module can be considered very satisfactory as its performance reached 95% exceeding the target value (90%).</td></tr>
<tr><td colspan="3"><b>IA3.3 –</b> Following on the system's lab prototype and during the reporting period, the TDSS system final prototype components were assembled on their final configuration, implementing all the hardware/software planned functionalities. The system was later involved in the test scenarios during PUC1 and PUC3 demonstrations, where it was possible to verify the final system in the field, where its functionalities, integration capability and readiness where successfully demonstrated.
During the reporting period after the several deployments which involved the integration with different C2's and where the system was subjected to diverse test scenarios, it was conclude that the KPI 3.3.1 was 100% achieved in all PUCs (produces and makes available > 75% of relevant information) and the TDSS is validated.</td></tr>
</table>

IA3.4 – social interaction and awareness raising with the citizens takes a fourphases approach to developing appropriate message content to warn citizens and persons present onsite in the event of a local incident that affects their safety and security. The first phase conducted a wide-ranging analysis of the current state of the art in warning messages and public alerting. This validated the use of a templated approach to message generation and the identification of the common alerting protocol (CAP) as a standardised framework on which to base the template messages. Furthermore, valuable takeaways such as the use of broadcast and social media to support message dissemination, regularity and timeliness of communications is important. Meanwhile message content should include several key pieces of information including severity, type, time, and location, preferable supplemented by current impact, mitigation measures and response plans. Use of additional media can also be beneficial in improving message visibility.

The second phases analyses messages relating the end users of the consortium to understand their current communication strategy. These were analysed according to the core content and levels of engagement with these messages. Specific messaging focusing on public alerting were extracted for a deeper analysis to analyse the actual content compared to current best practices. However, it was noted that most communication is currently uni-directional and that greater engagement with affected users could be beneficial when dealing with an incident.

The third phase looked at several case studies related to crisis communication for critical infrastructure operators. Unfortunately, there were limited examples directly from the space-sector; however, a range of physical and cyber incidents were examined. In the events that were managed most successfully it was important for the affected organisation to lead the public narrative and to do so early – an information vacuum creates the opportunity for misinformation to spread, while coordinating communication with partner organisations is essential to prevent sharing conflicting information.

The final phase developed a standardised warning message generation framework to support rapid and clear communication with citizens across multiple languages. A standardise message structure, adaptable into multiple languages was created and based on each of the common fields – several pre-selected options were identified utilising the 7SHIELD pilot use cases and demonstrations. The framework is flexible and allows for easy update of standardised fields as well as in-place overrides to communicate particular information whilst still adhering to a standard format. As the KPI 3.4.1 is related to user acceptance testing during piloting activity, IA3.4 was evaluated during the final three DEMO pilots, namely NOA, FMI and SPACEAPPS pilots. Across the three parameters – user friendliness, adaptability and compatibility, user ratings were at 80% for PUC1 (FMI), 100% for PUC3 (NOA) and 87% for PUC4 (SPACEAPPS) demonstration activities meeting or exceeding the target value of 80% in each case.

IA3.5 – The main achievement for the period was the conclusion of the development of the FH,the flight tests done with it to validate the method and detect solve problems that arise during the tests and the final prototype participation in the PUC1 (FMI). The KPI 3.5.1 defined for the UAV neutralisation is flying to the target drone and "catching" it, and bringing it back to pre-determined location. Pilot trials were carried out at PUC1 (FMI) in Finland during the second reporting period. However, Flying Hunter trials were carried out in Israel with online demonstration. All trials were successful and KPI 3.5.1 was 100% achieved.

Innovation Objectives	Innovation Activities	KPIs
IO4. Mitigation technologies for physical and cyber threats (including novel installation designs)	**IA4.1** Development of service continuity scenarios for cyber-attacks (KR17)	**KPI 4.1.1**: Downtime of critical services.
	IA4.2 Development of service continuity scenarios for physical attacks (KR17)	**KPI 4.2.1**: 7SHIELD service continuity planning will focus on ensuring that the critical services, as will be defined by the Ground Space Segment Operators (WP5, T5.4), will be delivered throughout the physical crisis under discussion (WP5,7), and that the

<table>
<tr><td></td><td></td><td>minimum Acceptable Downtime of critical services is achieved.</td></tr>
<tr><td colspan="3"><b><i>Achievements</i></b></td></tr>
<tr><td colspan="3"><b>IA4.1 –</b> During the last reporting period, an operational model has been generated to simulate the effect of various cyber and/or physical perils on the critical processes of modern Ground Segments (GSs). The model follows economic theory input-output concepts, employing network connectivity and product added value to offer a dynamic idealization of daily operations. The impacts to specific sectors of each company can thus be readily simulated, and the effects propagated to quantify the overall consequences to operability.
During the last reporting period, the implementation of the Service Continuity Module (SCM) has been finalized for all PUCs and it was succesfully integrated with the User Interface of the ENGAGE platform. The tool showcased excellent performance in terms of efficiency, as it was capable of executing the requested hazard scenarios and display the results to the user in near real-time. During the SPACEAPPS DEMO pilot, SCM was used by the GS operators in two out of the three cyber-attack scenarios as a decision support tool, by simulating the impact of the attacks to the operability of the organization. While in all scenarios the threats were mitigated before any actual disruptions started to propagate, the pilot users confirmed that (a) the downtime estimates produced by SCM were accurate and (b) the situational awareness offered by the tool can increase the resilience of their organization and consequently reduce downtimes.
Therefore, while at the end of the previous reporting period this KPI was only considered to be 50% fulfilled due to the lack of in vivo testing, it is now considered at 100%.</td></tr>
<tr><td colspan="3"><b>IA4.2 –</b> similarly to IA4.1, a generalized operational model has been generated for representing physical infrastructure of each PUC. The cyber and physical models were interconnected in order to produce a unified view of consequences to cyber-physical operations.
During the last reporting period, the implementation of the SCM tool for physical scenarios was tested in vivo, and it has consistently shown a reduction of downtime to physical attacks thanks to increased awareness and timely quantification of system-level consequences. In particular, the tool was tested in several physical-attack scenarios during the FMI and NOA DEMO pilots, demonstrated good performance in terms of accuracy and robustness. Therefore, while at the end of the previous reporting period this KPI was only considered to be 50% fulfilled due to the lack of in vivo testing, it is now considered at 100%.</td></tr>
<tr><th>Innovation Objectives</th><th>Innovation Activities</th><th>KPIs</th></tr>
<tr><td rowspan="3"><b>IO5.</b> 7SHIELD platform development</td><td><b>IA5.1</b> 7SHIELD platform integration (KR18)</td><td><b>KPI 5.1.1</b>: 7SHIELD modules integrated and deployed in the Framework.</td></tr>
<tr><td><b>IA5.2</b> Data Models for Combined Detection (KR19)</td><td><b>KPI 5.2.1</b>: Semantic concept defined.</td></tr>
<tr><td><b>IA5.3</b> User interfaces/Command and Control (C2) room (KR20)</td><td><b>KPI 5.3.1</b>: Common Operational Picture refresh updates;
<b>KPI 5.3.2:</b> Number of assets depicted on map (without clustering) without flickering;
<b>KPI 5.3.3</b>: Standards supported.</td></tr>
<tr><td colspan="3"><b>Achievements</b></td></tr>
<tr><td colspan="3"><b>IA5.1 –</b> during the last reporting period, the 7SHIELD framework has been expanded and improved until the final release at M23, as reported in D6.5 - Final system. The system architecture is event-driven for a highly scalable system where the Apache Kafka broker allows message exchanging between the framework components following the publish/subscribe pattern. As result, it allows the decoupling of the subsystems which makes service continuity possible even if one of the components should be offline.
Apache Kafka was chosen as the message broker as it offers high throughput and is suitable for messaging systems for massive processing (such as logs, big data analytics and stream processing) and boasts greater</td></tr>
</table>

support and multiple implementations in different languages/language platforms (e.g. (C/C++, JAVA, Sping Boot, Python, Go, NodeJS, PHP, etc.) In addition, Apache Kafka broker was chosen because it can work on a distributed system and for this reason it allows N Topics to be partitioned into N different machines to overcome the performance limit of the single host machine and to do this, the used version of Kafka makes use of Zookeeper which provides synchronization services for large distributed systems. Furthermore, Kafka is properly configured in 7SHIELD to support the correct size of the message but also avoid large bottle cones. Furthermore, the threshold of replicas and requests by producers is configured accordingly. This type of configuration allows the broker to keep its backup copies in the various nodes (in the specific case of the Pilots the number of nodes is 1). The configuration set up typically, without a message key, uses the round-robin strategy on all partitions of the Topic thus maintaining a uniform space but without a precise ordering. However, if the message has a key, the target partition will be computed from a hash of the key. This allows Kafka to ensure that messages with the same key always arrive in the same partition and therefore are always in order. Finally, according to the proposed integration plan (D6.3 – Definition of the integration and validation plan) due at M15, after the Operational Test Pilots carried out in March 2022 (PUC2 – NOA) and May 2022 (PUC3 – DEIMOS) and during the Demo Pilots in September 2022, October 2022 and November 2022 respectively in Greece (NOA), Finland (FMI) and Belgium (SPACEAPPS), all the 20 7SHIELD Key Results (KR) and the 32 modules have been developed and integrated. Therefore, KPI 5.1.1 is fully achieved .
IA5.2 – Despite of KPI 5.2.1 was fully achieved in the first reporting period, during the reporting period, a new version of the Unified Alert Format (UAF), based on IDMEF (Intrusion Detection Message Exchange Format) v2.0.3 was released to be adopted in 7SHIELD for the exchange of information related to alerts, threats, and combined threat scenarios.
IA5.3 – During this final reporting period, the initial version of the 7SHIELD User Interface components was updated and finalised according to the user requirements, objectives of the project and the type of information to be presented to the users/operators of the platform, but also based on the feedback gathered through its demonstration and evaluation, during the Operational Test and Demo pilots. To integrate the 7SHIELD UI elements, the concept of "global dashboard" is established through the Cyber-Physical Threat Monitoring (CPTM) Dashboard which integrates dashboards, UI tools and widgets in a single navigable panel that allows you to have better control over the system. Specifically, the CPTM Dashboard integrates the Cyber-Attack dashboard, MBDA, DiVA and CIRP/RAT UI tools to visualize and manage relevant information, such as risk and resilience assessment data. It also shows in detail all the Situational Picture data, including CI assets, related risk assessment values and all events captured over time. These events are shown both in descriptive (text) and geographical (map) way. The map is implemented with MapBox which supports over hundreds of thousands of assets on the map (where each track supports up to 100 coordinates and each cluster supports up to 100,000 points) for which KPI 5.3.2 is largely achieved. KPI 5.3.1 is also achieved as each event is updated every 100ms. Regarding the KPI 5.3.3 the supported standards are: GeoJSON (RFC 7946), OGC KML (RFC 2806), JSON (RFC 8259), IDMEF v2.0.3 (RFC 4765) and the WebSocket Protocol (RFC 6455). The technology stack used for CPTM Dashboard is ReactJS with Redux/Thunk, Material UI and OpenStreetMap. Taking into consideration the KPIs related to ENGAGE PSIM (Physical Security Information Management) system provided by STWS, further enhanced to ENGAGE CSIM (Convergent Security Information Management), the User Interface should refresh updates in less than 2 seconds (KPIs 5.3.1), assuming sufficient communication bandwidth in the field. This target value is highly dependent by the performance of the overall 7SHIELD system (end-to-end communication). Due to the successful Integration and collaboration between the components was finally completely achieved (100%). Additionally, the User Interface should be able to depict 4000 objects without flickering (KPI 5.3.2). New technology was adapted and developed by the ENGAGE PSIM components for that purpose, achieving the fulfilment of the KPI in the first reporting period. Finally, according to KPI 5.3.3, several interoperability standards should be adapted and supported by the UI/C2 components. Finally, all standards that were initially envisaged (EDXL & OGC standards) have been supported. Additionally, the support of the UAF standard message format has been added to this list.

2.1.2. User-oriented objectives (UO) and user-oriented activities (UA)

User-oriented Objectives	User-oriented Activities	KPIs

<table>
<tr><td rowspan="3"><b>UO1.</b> Use case definition and requirements</td><td><b>UA1.1</b> Use case design, stakeholder engagement and user requirements</td><td><b>KPI 1.1.1</b>: User-defined requirements that are clear and broad enough in order to ensure that all stakeholders' needs are met. At least 15 questionnaires are answered by ground stations professionals from at least 5 independent organizations. At least 3 focus groups are implemented and at least 15 user scenarios are proposed.</td></tr>
<tr><td><b>UA1.2</b> Security requirements</td><td><b>KPI 1.2.1:</b> Secure access to the system, secure communications.</td></tr>
<tr><td><b>UA1.3</b> Ethics and legal framework</td><td><b>KPI 1.3.1</b>: Demonstrate that research activities and expected results respect and promote the European Convention on Human Rights and the EU's Charter of Fundamental Rights and enhance European and local values, in accordance with the public sense of fairness.</td></tr>
<tr><th colspan="3">Achievements</th></tr>
<tr><td colspan="3"><b>UA1.1 –</b> KPI 1.1.1 was fully achieved in the first reporting period as follows:
• 250 functional and non-functional user requirements were collected.
• 16 questionnaires were completed by 8 different organizations.
• 5 main focus groups and additional follow up meetings were organized, 19 use case scenarios were proposed).</td></tr>
<tr><td colspan="3"><b>UA1.2 –</b> During the second period, the identification of security requirements in order to limit the risks of data breach, and to secure data exchange and storage procedures was accomplished. The aim of the work conducted was to examine both the hardware/software security and the security and protection of generated information within the 7SHIELD solution and to finally introduce a list of security requirements and organize various aspects of security into a hierarchy of concepts based on existing standards, policies, guidelines, and the needs of the 7SHIELD operators. The identified security requirements from both the literature review and the operators' contribution were elicited through the 7SHIELD components, as well as the 7SHIELD specific use cases. These requirements were mapped to several main categories covering cyber and physical security fields such as access control, system development, data protection, etc. The KPI 1.2.1 achievement during the second reporting period is 100% completed with the advancement of the demos and operational tests scheduled within the project.</td></tr>
<tr><td colspan="3"><b>UA1.3</b> – In the second period, further analysis including updates on the forthcoming AI act and its implications for 7SHIELD and the CER directive were included. The substantive update was the undertaking of a Data Protection Impact Assessment (DPIA) for the 7SHIELD system to document the full scope of personal data processing within the system as well as set out the appropriate risks and mitigation measures for an operational version. These further analysis and assessments allow for KPI 1.3.1 to be fully achieved within the project period.</td></tr>
<tr><th>User-oriented Objectives</th><th>User-oriented Activities</th><th>KPIs</th></tr>
<tr><td rowspan="2"><b>UO2.</b> Pilot design, implementation and evaluation</td><td><b>UA2.1</b> Development of the validation scenario and evaluation methodology</td><td><b>KPI 2.1.1:</b> Evaluation metrics, User satisfaction metrics, user feedback, system usability metrics.</td></tr>
<tr><td><b>UA2.2</b> Field demonstrations, testing and training</td><td><b>KPI 2.2.1</b>: User satisfaction metrics, user feedback, system usability metrics.</td></tr>
<tr><th colspan="3">Achievements</th></tr>
</table>

UA2.1 – The KPI 2.1.1 was 100% achieved within the first reporting period. Furthere details are in D1.3, due at M20.

UA2.2 – During the reporting period, the last two (four in total) Operational Test pilots of the 7SHIELD prototype, namely in NOA and DEIMOS Ground Segments, were conducted, following the evaluation methodology of UA2.1. The Operational Tests were performed on the PUC3 (NOA) and on the PUC2 (DEIMOS), following physical and cyber-attack scenarios in realistic and heterogeneous operational environments.

Furthermore, the three Demonstration pilots of the final 7SHIELD framework were also performed. The Demonstrations were organised in PUC3 (NOA), PUC1 (FMI) and PUC4 (SPACEAPPS), respectively in September, November and December 2022.

Before each Operational Test and Demonstration pilot, training sessions were organized with the participation of the technical partners, to familiarize the end-users of the PUC to the 7SHIELD framework. After each Operational Test and Demonstration pilot, an evaluation of the 7SHIELD framework was performed by the pilots' users, including collection of user feedback on user interfaces & user friendliness, system adaptability and system compatibility.

The full report on the evaluation of the final 7SHIELD framework is available in the report D7.3.

As a short summary, the evaluation results show the following figures:

- A total of 170 Acceptance Criteria from 20 KRs was evaluated.
- There were 155 Acceptance Criteria that were fulfilled and 6 that were partially fulfilled and only 9 that were not fulfilled.
- The percentage of end-user Acceptance Criteria fulfilment excluding partial fulfilments was 91.2 % and including also the partially fulfilled as high as 94.7 %. These values show that 7SHIELD framework has met the user requirements well and been able to adopt the request and definitions coming from different users.
- 31 Key Performance Indicators (KPI) under five different Innovation Objective category, defined in the Grant Agreement (GA), were tested at least in one PUC but many of them in several, when applicable. The KPIs covered 19 Key Results of which had one to four KPIs each. All KPIs based on GA were fulfilled and their target values reached or surpassed.

User satisfaction of 7SHIELD framework was measured using 5-point Likert Scale in three different categories: user friendliness, adaptability, and compatibility, for each Key Result. The feedback was collected from end users, i.e., operators and personnel who provided their subjective view of the system. To be able to compare the different use cases and calculate the averages, the final evaluation of user satisfaction took into account only the last three Demonstration pilots where the final 7SHIELD framework was used.

The averages of Key Results' user friendliness varied between 3.7 and 5.0, adaptability between 3.0 and 5.0 and compatibility between 3.0 and 5.0. The total averages of each category were 4.3, 4.3 and 4.4., respectively. Each Key Results' overall user satisfaction was calculated averaging the three categories resulting user satisfaction varying between 3.3 and 5.0. The overall user satisfaction of the 7SHIELD system that take into account three PUCs, all Key Results and three user satisfaction categories was 4.3. The majority of users satisfactions were High or Very High, and even at lowest Medium, that can be considered as a success and great achievement for a complicated multi-module framework from the users' perspective.

2.1.3. Impact-making objectives (IMO) and impact-making activities (IMA)

Impact-making Objectives	Impact-making Activities	KPIs
IMO1. Dissemination and collaboration	**IMA1.1** Dissemination and communication of the project results	**KPI 1.1.1**: At least two domain-specific communities for dissemination and clustering.
	IMA1.2 Collaboration and clustering with other SU-INFRA-01 projects	**KPI 1.1.2**: At least two domain-specific communities for

		dissemination and clustering.

Achievements

IMA1.1 – the main activities implemented during the second project period to support the communication of the project were as summarised as follows:

- Continue the update of the website and social media (LinkedIn)
- Preparation and distribution of the 2nd project newsletter issue
- Preparation of the 2nd version of the brochure and infoboard
- Preparation of 19 KR leaflets
- Preparation of the project video
- Participation in conferences, workshops and other events as described below
- Publication of 5 scientific papers
- Organisation of the Info Days

During the reporting period, 7SHIELD became a member of the European Cluster for Securing Critical Infrastructures (ECSCI – https://www.finsec-project.eu/ecsci) for dissemination of the main outcomes and clustering. In the same period, 7SHIELD consortium carried out the following dissemination activities:

- 5 publications
- participation in 42 conferences including International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP), Space Tech Expo Europe , EU-HYBNET and ESA's Phi-Week 2021.

In addition, SERCO organized a tailored info day in Bruxelles on 14 December 2022. 104 persons were registered to the 7SHIELD info day, including 38 external stakeholders (relying on networks already established and inviting external stakeholders mostly belonging to public section or agencies).
Additionally, 19 KR leaflets were produced and published on the website and advertised on the 7SHIELD LinkedIn page. The KR leaflets have been created in conjunction with the various partners responsible of the project KR. As a result, the KPI 1.1.1 has been achieved (100%).

IMA1.2 – The fulfilment of KPI 1.1.2 has been achieved being involved in 3 domain-specific communities for dissemination and clustering:

- ECSCI (European Cluster for Securing Critical Infrastructures)
- SMI2G (The Security Mission Information and Innovative Group)
- CERIS (Community for European Research and Innovation for Security)

In more details, the 7SHIELD consortium, as member of the European Cluster for Securing Critical Infrastructures (ECSCI – https://www.finsec-project.eu/ecsci), actively participated to the clustering and networking activities with other 24 H2020 research projects dealing with security of Critical Infrastructures. Its main objective is to bring about synergetic, emerging disruptive solutions to security issues via cross-projects collaboration and innovation. In this context, we participated and will continue to attend to events organised by other EU projects with activities overlapping 7SHIELD thematics

- EU-HYBNET (https://euhybnet.eu)
- DRONEWISE (https://dronewise-project.eu/)

Moreover, the "Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience" (https://www.steinbeis-edition.de/shop/out/pictures/media/9783956632853.pdf) has been published by Steinbies-Edition (https://www.steinbeis-edition.de/shop/Tagungsbaende/Tagungen-Symposien/Consolidated-Proceedings-of-theSecond-ECSCI-Workshop-on-Critical-Infrastructure-Protection-and-Resilience.html) as open access.

SMI2G Event 2022, co-organised by EARTO Security & Defence Research Working Group, the SEREN network, EOS, IMG-S, ECSO and supported by ENLETS gathered European-wide innovators and practitioners who are looking for further consortium partners by presenting game-changing ideas and novel technologies addressing the challenges of Horizon Europe's Civil Security for Society 2022 cluster.
This initiative complements the clustering activities of the 7SHIELD project by creating an ecosystem of experts to define the next topics of innovation in the field of the protection of critical sites. The expertise accumulated by 7SHIELD is an important asset that perfectly fuels these reflections, to build on what has been achieved

and provide concrete answers to the question "what's next?", which systematically arises at the end of the projects.

CERIS aims to facilitate interactions within the security research community and users of research output and 7SHIELD participated in 3 events: The CERIS FCT: Protection of Public Space (April 2022), the CERIS INFRA 2022 workshop: How research supports the directive on the resilience of critical entities (July 2022) and to the CERIS Annual Event 2022: Fighting Crime and Terrorism and Resilient Infrastructure (September 2022). In these events, 7SHIELD, presented the overall approach and the objectives of the project.

Impact-making Objectives	Impact-making Activities	KPIs
IMO2. Exploitation and sustainability model	**IMA2.1** Market analysis and existing business models	**KPI 2.1.1:** Demonstrations to at least two other external installations and comparison.
	IMA2.2 Exploitation plan and Intellectual Property (IP) protection for the proposed tools	**KPI 2.2.1:** Demonstrations to at least two other external installations and comparison.

Achievements

IMA2.1 – During this first reporting period, 2 Operational Tests of the 7SHIELD framework were performed (KPI 2.1.1) on 2 external installations:

- The 1st Operational Test was performed on the ONDA DIAS (Copernicus' Data & Information Access Services)
- and the 2nd Operational Test was performed on the ICE Cubes Service (ISS International Commercial Experiment Cubes) in Belgium.

During the second reporting period, a second version of the market analysis was refined and completed by adding information and analysis for all components of the 7SHIELD framework. Collaboration and clustering with similar projects and relevant solutions from other critical infrastructure types (IMA1.2) that were identified in the project's communication and dissemination activities (IMA1.1), helped us to provide a focused market analysis (IMA2.1) and a developed business plan (IMA2.2).

During the second reporting period, the audience of 7SHIELD has gone beyond the project participants. Collaboration and clustering with similar projects and relevant solutions from other types of critical infrastructures have been identified in the project, aiming to deliver a portable solution for quick insertion. Specifically, KPI 2.2.1 is related to the demonstrations to at least two other external installations and comparison. In particular, starting from KER20b – CPTMD and KR11 - SPGU developed within 7SHIELD have been implemented and demonstrated new KRs in another EU-funded project, PRECINCT - Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-physical Threats, funded under H2020-SU-INFRA-2020. In PRECINCT the two 7SHIELD KRs have been adapted according to the users' needs and requirements within 2 PRECINCT Living Labs (LLs): Ljubljana and Bologna. It's worth mentioning that the adoption of these innovative technologies in other installations for safety and security should be approached as a continuous process and not as a one-time event. Regularly reviewing and updating the technology is crucial to ensure it continues to meet the organization's needs and to address any new risks and threats that may arise.

IMA2.2 – During the last reporting period the second and final version of the Exploitation Plan for each 7SHIELD result was provided. The information collected in the first version of the Exploitation Plan was reviewed and integrated during the project life as well as the number of Key Exploitable Results and joint Exploitation Schemes. In the second version of the Exploitation Plan, the number of the individual and joint KERs was modified, and some new results were added. This means that the main KERs have been updated with a further analysis and improvement of their exploitation plan, while some others have been added to enrich the 7SHIELD offering. Specifically, 3 new individual KERs have been added, namely KER17: Emergency Response Plan (ERPs) Model, KER20a: ENGAGE CSIM and KER20b: 7SHIELD CYBER-PHYSICAL THREAT MONITOR DASHBOARD – CPTMD. Furthermore, the same updates are related to the Joint Exploitation Schemes and, in particular, the Joint Exploitation Scheme "UAVs with on-board computer vision and visualisation dashboard" was expanded by incorporating the User Interfaces from ENG. In this way, the 7SHIELD project will offer an aerial detection and response exploitable solution. A larger grouping mechanism "Combined cyber-physical protection" is added to cover a core and an integrated set of functionalities within the 7SHIELD ecosystem and as a whole part to make the commercial proposition more compelling as a whole. The 7SHIELD combined cyber-physical protection covers the combined cyber-physical aspect and provides completed features from the cyber and physical threat detection, correlation of cyber and physical threats, update situational picture along with the mitigation aspect.

The market opportunities envisaged for the 7SHIELD solutions are several and they are increasing day by day. From this point of view, the 7SHIELD market entry strategy was elaborated and presented. The 7SHIELD exploitation strategy includes two complementary exploitation approaches: commercial and community-based exploitation. While the prime objective of the project is to develop new knowledge that can form the basis for marketable products, it is also necessary to acknowledge that there are some 7SHIELD results that come out with the aim of supporting sustainability through community-based and scientific exploitation.

The IPR theme has been also further analysed. An Intellectual Property Rights (IPR) Repository was created for 7SHIELD. It contains information about the intellectual property rights associated with each 7SHIELD result, both individual and joint results. For the latest, a draft Exploitation Agreement for joint Exploitation Schemes have been prepared and provided.

Impact-making Objectives	Impact-making Activities	KPIs
IMO3. Standardisation, strategy and policy-making	**IMA3.1** Policy framework	**KPI 3.1.1:** At least two domain-specific communities for dissemination and clustering.
	IMA3.2 Standardisation, strategy (investment measures) and policy-planning	**KPI 3.2.1**: At least two domain-specific communities for dissemination and clustering

Achievements

IMA3.1 – In the 2nd period, EETT following up on the contact with ENISA that had initially begun in the 1st period, proceeded in actions to communicate information about the project in order to identify together with ENISA the appropriate channel that would allow the dissemination of the project results to stakeholders related to ENISA. The ENISA ECASEC Expert Group was identified as the optimum event where the 7SHIELD experts would have the possibility to present the project objectives and results to security experts from the National Regulatory Authorities of electronic communications from EU Member States. The presentation was held during the ENISA ECASEC meeting on the 29th of June in Brussels.

In the 2nd period discussions with organisations such as CEN/CENELEC and conversations with delegates at meetings (see below in IMA3.2) highlighted the value of being aware of policy, namely, what is the overall purpose of the technology being developed in 7SHIELD. We see this as a responsibility to enhance resilience against cyber/physical threats and hence ensure continuity of space ground segment operations. This responsibility is realised through developing technology, solutions and best practices. None-the-less, developers ultimately have to demonstrate they meet requirements and fulfil the accreditation conditions both of which are stipulated by the procuring authority of the ground segment.

Projects such as 7SHIELD can assist in policy making by providing expert knowledge, as 7SHIELD has done when invited by policy makers, and also, in establishing standards and best practices which 7SHIELD also has achieved.

IMA3.2 – In the 2nd period efforts continued to engage with key stakeholders responsible for procuring space ground segments as well as communicating with other projects pursuing cyber/physical policy and standards. This was as planned, but also took into consideration the recommendations given at the Project Review Meeting held 3rd March 2022 in Brussels.

At the Living Planet Symposium held 23-27 May 2022, World Conference Center Bonn, Bonn, Germany 7SHIELD brochures were distributed to participants during the daily poster sessions. Also initial contact was made with EUSPA to discuss policy.

At the invitation of DG-HOME 7SHIELD participated at the 11th EU-US-Canada expert meeting on critical infrastructure resilience hosted by the French Government in Paris 1-2 June 2022. 7SHIELD had a stand with brochures and made a presentation. Discussion with several delegates showed that that subject of Critical Infrastructure Resilience is extremely broad. Security at national government/political level leaning more towards screening of employees of critical infrastructure, anti-terrorism intelligence gathering whereas 7SHIELD is focussing on technology solutions to increase resilience to cyber/physical threats. The opportunity was taken to discuss 7SHIELD with EUSPA on the second day of the meeting.

Through the membership of the European Cluster for Securing Critical Infrastructures contact was made with EU-HYBNET. At their invitation 7SHIELD was presented at the EU-HYBNET, Innovation and Standardization Workshop, The Hague – 15 June 2022. The subject chosen was: Who needs standards? With the intention of being provocative to initiate discussion on the value of standardisation. While there was consensus on the value of standards in support of innovation and promoting solutions there was some concern on the increasing number of standards in the field of hybrid threats.

Following up on the meetings with EUSPA a meeting was organised with EUSPA on the 4th August 2022. Interest was shown in the work performed in 7SHIELD with specific reference to the needs of Galileo from threats of spoofing and intentional interference. The low power of Galileo signals of course being a critical consideration.

A 7SHIELD_presentation was organised and given to SatCen – 23-Aug-2022. The focus of the discussion was the cyber security components of 7SHIELD. SatCen themselves participate in Horizon programmes as users, but as do ESA and EUSPA they acquire there infrastructure through open tendering. The value of 7SHIELD was recognised but exploitation of 7SHIELD will have to be through tendering.

From the discussions with ESA, EUSPA and SatCen is that tenderers to procurements have to demonstrate they can meet legislation and required standards on security when proposing for a contract. While ESA and EUSPA are investing in policy and accreditation it is the tenderer who will have to invest in meeting legislation and standards in delivering the ground segment system.

The demonstrations of 7SHIELD were closely followed together with the training and the establishing of the training platform. The interest being to see how best practices were flowing through to the training.

At part of the process of writing the delivery D8.12 Security Standardisation Strategy and policy-planning the survey first organised in June 2022 was repeated in February 2023 extending the number of questions. The objective of the survey was to understand how the teams in 7SHIELD had been influenced by the standards being applied to their work and how the saw a possible evolution. The response was positive with respect to the influence on their work particularly with respect to establishing a baseline for their work. There was no consensus (50/50 split) on the need for standards to evolve to accommodate the innovations introduced in 7SHIELD. In one case there was a contribution to a standard. Namely the update of IDMEFv1, a cyber intrusion detection format specified to the new version IDMEFv2.

The deliverable D8.12 Security Standardisation Strategy and policy-planning has been delivered.

2.2. Summary of project's results in the last period

The work done in the last period, from M17 (January 2022) to M30 (February 2023) was devoted to the finalisation of the literature review regarding the general **security requirements** and the **privacy by design principles**. In addition, the collected input from both the literature review and the operators' contribution led to a consolidated list of more than 800 security requirements. The security requirements as collected based on the literature review were mapped to the relevant 7SHIELD tools based on their functionality. A questionnaire that aimed to further elicit the security requirements based on the 7SHIELD tools actual compliance with security requirements was circulated to all technical partners. This procedure led to the identification of several general and reusable security requirements, which are grouped in different main categories such as access control, client-server communication, system development and data protection, etc. Finally, and to refine the security requirements through the use case scenarios, a cyber and physical risk analysis was conducted.

In the context of **ethics and legal framework,** a review of newly introduced legislation or upcoming legislation relevant to the project (e.g., CER directive, NIS2, Artificial Intelligence Act) has been conducted.

Regarding the 7SHIELD **pre-crisis and prevention technologies,** the design of the secure authentication mechanism was finalized, including some further subcomponents that allow the module to be compliant to all the user requirements and facilitate the integration with other 7SHIELD modules. Moreover, the **asset and threat taxonomies** were finalized: the first version of the asset taxonomy was improved and extended with more physical assets; the cyber threat taxonomy was finalized, unifying different versions previously defined; a second version of the natural and physical threat taxonomy was developed. Furthermore, the design of the **risk assessment toolchain** was finalized and the final prototype of **MBDA tool** was released with the functionality of analysis of cascading effects and integrated with the components of the platform. This functionality was tested for the first time in the NOA Operational Test pilot, in March 2022.

Several refinements of the Deep learning NLP algorithm for text analysis on the **Threat Intelligence** (TI) tool were performed and a first prototype of the Threat Intelligence service was evaluated in the SERCO Operational Test as well as in FMI and SPACEAPPS Demo Pilots. The latest version was used to evaluate the performances of the CPTI framework against state-of-the-art results.

Regarding the **design of 7SHIELD mission UAV** (included the mechanical, electronical and flight subsystems), numerous test & trial flights were carried out checking software and hardware in different flight stages. 7SHIELD mission UAV's capabilities, such as the communication between DCEP and the control room, were demonstrated in DEIMOS Operational Test pilot (Spain) and in FMI Demo pilot (Finland).

The **Face Detection and Recognition** (FDR) module was implemented and tested for the analysis of real-time video input. The module was further improved by the development of a facial clustering algorithm for video streaming analysis. Additionally, FDR module (offline version) was prepared and participated successfully in NOA (including Operational Test) and FMI Demo pilots. Furthermore, the **Activity Recognition** (AR) module which can distinguish if a person is moving or stationary was released and along with the Video-Object Detection module, was demonstrated in NOA (including Operational Test) and FMI Demo pilots. Activities were done towards the finalisation of the detection and correlation modules, including the preparations for their participation in the Demo pilots. During the Operational Test and Demo pilot in NOA and FMI premises, the detectors for face detection and recognition (FDR), video-based object detection (VOD) and activity recognition (AR) along with the cyber-attack detection framework (CADF) were successfully demonstrated over various use cases.

Activities concerning the data source identification and analysis, the definition of monitoring rules based on Use Cases and the SIEM adaptation/improvement were carried out. Moreover, in the last period, activities focused on the data source, **cyber threats identification and analysis**, the definition of new monitoring rules for attacks detection and correlations. Furthermore, work on the SIEM adaptation/improvement by adopting new monitoring rules for malware detection and new features for port scanning detection feeding the alerting system. Also, the **Rule Designer** was improved. Finally, based on the experience on the previous operational test, the log analyser component was improved.

The User Interface for the **MultiModal Automated Surveillance** (MMAS) operator, namely user functionalities related to visualization of video streaming, positioning of the camera, zooming and setting of alarms and warnings was developed and evaluated. Furthermore, the elaboration of techniques for detection of man-made attacks from thermal and IR data, namely detection of movements, classification and detection based on the level of heat, was elaborated.

Upgradation work on PLS v3.0, LFS v3.0 and 3D MND v3.0 was progressed in terms of hardware and software. The work has also focused on the performing of long test to check the stability of KAFKA server. Further tests were carried out also for the 3D MND detector. After that, the thee detectors were tested, calibrated and installed.

The definition of the UAF message format used to describe **physical, cyber and combined security alerts** was finalized. The **Geospatial Complex Event Processor** (G-CEP), which was enabled to receive, correlate and forward physical events was deployed on the CI/CD environment. The resulting message that is produced by the G-CEP was refined by adding new fields.

The **Situational Picture Generation and Update (SPGU)** was extended to handle the latest format of messages produced by the G-CEP, AC and by the HCC. Also, the interaction with the Crisis Classification module was tested and evaluated. Moreover, different geometric shapes supported by GeoJSON such as multi-location, polygon, line, multi-polygon, multi-point, multi-line, were added to the SPGU features.

Regarding the **Post-Crisis management for response and mitigation** of physical and cyber threats of 7SHIELD, improvements in the RDF conversion service to map information regarding the infrastructure, was carried out. It worked on the upgrades of the reasoning service in order to retrieve the knowledge by queries (geospatial, threat type, temporal, etc.).

The FRSS's architecture and the definition of the hardware wearables were performed, as well as the acquisition of the equipment. The activity continued the integration of the sensors in the FRSS and fine-tuned the scenarios requirements with the end-users. It also made updates in the TDSS, especially in the FRSS, based in the feedbacks from the laboratorial tests. The integration with the 7SHIELD core framework was performed and also with the ENGAGE tool. After the NOA Operatinal Test pilot the results were evaluated and adjustments and corrections were made in the TDSS system.

The design of the **Crisis Classification scenario for annotation tool** was finalised. It was finalised the development of the machine learning models (classifiers) and fine tuning of the parameters of each method to improve the accuracy of the severity level predictions. Experimental evaluations of the Crisis Classification module were carried out. Crisis Classification module was also integrated into the 7SHIELD framework hosted at NOA infrastructure for the execution of the PUC3.

A comprehensive literature review was performed on relevant **emergency response standards**. Based on the above and on widely accepted best practices a model Emergency Response Plan was developed to describe the strategies, techniques, systems and practices widely applied for the effective response during an emergency incident and the containment of its impacts on an organization's assets, property, and people as well as its offered services. Moreover, a series of questionnaires was developed and distributed with the purpose of extracting useful information regarding the 7SHIELD Emergency Response Plans in order to better comprehend the special requirements, needs of end-users, as well as the particular conditions that PUCs will be realized. Based on the feedback collected from the Operational Test and Demo pilots further fine-tuning was done.

A review of **service continuity standards and practices** was undertaken and the generic structure of the business continuity model for the PUCs was finalised. The implementation of the Python module was tested and validated. The definition and setup regarding the integration of the tool within 7SHIELD framework, specifically ENGAGE tool, started.

Regarding the **System Integration,** interoperability was achieved with the Crisis Classification module (CRCL) through which it is possible to update the severity level. The modules of SPGU and CRCL interact with each other through a reciprocal alignment (bilateral update) that allows CRCL to track changes in the Situational Picture and SPGU to track the latest level of severity deduced from new changes and past events. In addition, the interoperability of MBDA with SPGU was implemented to allow a dynamic update of the data relating to assets and areas of the map shown on the CPTM dashboard. Early work on the integration of the DiVA module for risk assessment data relating to the assets shared with MBDA. Interoperability is implemented between ENGAGE and SPGU regarding alarm reporting. The integration of the tools that interact with the detection modules was updated in order to foresee all the possible combinations of data that can be returned by the correlation tools (e.g. CAC, GCEP and HCC) to ensure that the interaction between detection and correlation modules can communicate correctly with the data collector.

The **modelling of pilots** was carried on, analysing vulnerabilities and weaknesses, and identifying security solutions to mitigate the risks. The activities of modelling pilot infrastructure and of threat assessment were completed. Furthermore, the STRIDE analysis of the components of the platform was started and a first draft is available.

An initial version of the **7SHIELD User Interface (UI)** was designed and implemented according to the user requirements, objectives of the project and type of the information to be presented to the users/operators of the platform. The main graphical interface of the 7SHIELD platform was provided to users through a number of GUI elements, namely Cyber Attacks Dashboard provided by CeRICT, Cyber-physical Threat Monitoring Dashboard by ENG and ENGAGE CSIM solution by STWS). These components were separated into two groups, according to the type of operations they support: the UI components that are related to the Preparedness and Detection phase and the UI components that are related to the Response phase. The internal interconnection of the UI components, as well as the interconnection of the UI components with the rest platform, was enhanced and updated.

Finalization of the **validation scenarios and evaluation methodology** for the Operational Test and Demo pilots and KPIs for the evaluation of the modules' performance were also defined.

Planning the validation and demonstration phase, by figuring out a detailed plan with the requested actions to prepare and execute the pilots. Specifically, the validation and demonstration phases, and the demo events, were prepared using a pilot validation and demonstration plan as a general guideline providing all the relevant information. The pilot validation and demonstration plan were prepared for all the pilot sites and provided a detailed description of the pilots' preparation activities. Moreover, this document provides information of the pilots' planning activities, and a plan for the pilot execution activities was presented.

User training sessions were organized for allowing PUCs end-users to get familiar with the technologies and the details of the 7SHIELD system. In parallel to the training sessions for the Operational Test and Demo pilots, the 7SHIELD online training platform was setup, based on the Moodle platform. The 7SHIELD online training platform hosts the training material (presentation, webinar) covering each module of 7SHIELD.

Regarding the **field demonstrations and testing**, preparation activities were done for the planned trials. The activities included testing of interoperability between different Key Results and components as well as logistics and other travel and hosting tasks. During and after the Operational Test and Demo pilots, the Pilot Validation and Demonstration Plan and Validation Scenario and Evaluation Methodology documents were filled.

The **communication and dissemination activities** during the reporting period were successfully conducted. In the context of WP8, particular effort was made to consolidate the network and prepare for Info Day. The consolidation of the network requires the sustained participation of the project partners in conferences to promote the results obtained (keeping in mind the commitment of 2 conferences per partner). As such, the recommendations of the experts during the mid-term review to boost communication were implemented with a reminder sent regularly to partners providing the list of upcoming events where the project brings added value. The objective is to be able to communicate massively with all the consolidated details during the following period.

Regarding the **exploitation** activities, a further analysis and addition of 7SHIELD KERs is an important step because this is a continuous activity. In particular, an **additional Joint Exploitation Schema,** following a **larger grouping mechanism** to cover a core and an integrated set of functionalities within the 7SHIELD ecosystem and as a whole part to make the commercial proposition more compelling was introduced. A structured and in-depth analysis of the exploitable results was conducted in order to structure exploitation planning and ensure a sustainable exploitation.

Standardisation strategy and policy-making objective deals with the 7SHIELD's aims to standardise and demonstrate strategies and policies to prevent, early detect, response and mitigate of amalgamated attacks in physical and cyber manner. Regarding the policy framework, we focused in particular on how the current policies could influence the solutions and what gaps in the policies are present that need to be put in place to make it possible to fully implement the 7SHIELD innovative technologies. Work was performed to understand how the developments in 7SHIELD could possibly influence future policy and understand how requirements arising from existing policies have shaped the requirements on 7SHIELD Key Results. Regarding the standardisation, strategy (investment measures) and policy-planning, we investigated the current standards and practices being used by operators of Ground Segments of Space systems, security authorities, industry, policy makers, and civil protection across the European Union. Further work was focused on re-visiting contacts with the European Space Agency and contacting other organisations such as EUSPA and SatCen as well as the European Standards Organizations, CEN, CENELEC, and ETSI.

3. Dissemination actions

During the project last period, several communication and dissemination actions took place in line with the structure of the Annex 1 to the Grant Agreement. Besides the Meet-the-partner LinkedIn campaign (https://www.linkedin.com/company/7shield/) and the 7SHIELD website creation (https://www.7shield.eu/) and continuous update, the following main events were actively participated.

3.1. Communication and dissemination events

In the following table are listed all the communication and dissemination events have been participated in the second reporting period.

	Event Title	Type of Event	Event Dates	Location	Type of Participation	Presentation Title	Attendee
1	CERIS Disaster-Resilient Societies (DRS) Event	Conference	23/25-Mar-22	Hybrid	Auditor	N/A	Eftihia Georgiou (KEMEA)
2	Space 4 Critical Infrastructure - Introduction into the EU-Directive on the resilience of critical entities [WEBINAR]	Workshop	29-Mar-22	Virtual	Auditor	N/A	Leslie Gale (SPACEAPPS)
3	EU-HYBNET 2ndAnnual Workshop	Workshop	6-Apr-22	Roma, Italy / Virtual	Speaker	General presentation of 7SHIELD project	Gabriele Giunta (ENG)
4	CYSAT PARIS 2022	Conference	6-Apr-22	Paris, France	Speaker	General presentation of 7SHIELD project	CS
5	CERIS FCT workshop on protection of public spaces	Workshop	7-Apr-22	Brussels, Belgium	Speaker	General presentation of 7SHIELD project	Ilias Gkotsis (STWS)
6	2nd ECSCI workshop on Critical Infrastructure Protection	Workshop	27/29-Apr-22	Hybrid	Speaker	7SHIELD: A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats	Gerasimos Antzoulatos (CERTH)
7	Security Mission Information & Innovation Group (SMI2G) Workshop 2022	Workshop	16/17-May-22	Brussels, Belgium	Poster	General presentation of 7SHIELD project	Salvatore D'Antonio (CeRICT)
8	DroneWISE final conference (ISFP project)	Conference	20-May-22	Šibenik, Croatia	Poster	General presentation of 7SHIELD project	Katerina Kokaliari (ACCELI)
9	Living Planet Symposium 2022	Conference	23/27-May-22	Bonn, Germany	Booth	7SHIELD general presentation shared at the booths	CS, SERCO

10	13th International Conference "days of Corporate Security 2022"	Conference	31-May-22/1-Jul-22	Ljubljana	Speaker, Booth	7SHIELD: A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats	Gabriele Giunta (ENG)
11	11th EU-US-Canada Expert Meeting on Critical Infrastructure Resilience	Workshop	1/2-Jun-22	Paris, France	Speaker	Presentation of 7SHIELD project focused on innovations	Leslie Gale (SPACEAPPS)
12	FIC (International CyberSecurity Forum)	Conference	7/9-Jun-22	Lille, France	Speaker	General presentation of 7SHIELD project	Franck Ranera (SERCO), Yann Van Engelandt (CS), Magdalini Karadimou (HP)
13	CIPRE-EXPO - 2022 Critical Infrastructure Protection and Resilience Europe	Conference	14/16-Jun-22	Bucharest, Romania	Speaker	General presentation of 7SHIELD project	Gerasimos Antzoulatos (CERTH)
14	EU-HYBNET Innovation and Standardisation Workshop	Workshop	15-Jun-22	The Hague, Netherlands	Speaker	7SHIELD - EU-Hybnet - Who needs standards?	Leslie Gale (SPACEAPPS)
15	37th ECASEC EG of Telecom Security Authorities meeting	Conference	28-Jun-22	Brussels, Belgium hybrid	Speaker	7SHIELD projects results to cover risk assessment, service continuity and emergency plan	Gabriele Giunta (ENG)
16	ICONHIC 2022 - 3rd International Conference on Natural Hazards & Infrastructure	Conference	5/7-Jul-22	Athens, Greece	Speaker	A Multihazard Risk analysis Platform	STWS
17	CERIS INFRA event: “How research supports the directive on the resilience of critical entities?”	Workshop	12-Jul-22	Brussels, Belgium	Booth, Speaker	General presentation of 7SHIELD project	STWS
18	ICECET 2022	Conference	20/22 July 2022	Prague, Czech Republic	Speaker	Study on the Application of EfficientDet to Real-Time Classification of Infrared Images from Video Surveillance	Filipe Mendes (INOV)
19	IEEE International Conference on Cyber Security and Resilience	Conference	27/29 July 2022	Virtual	Speaker	Modelling and assessing the risk of cascading effects with ResilBlockly	Enrico Schiavone (RESIL)

20	ARES Conference (PCSCI WORKSHOP 2022)	Conference	23/26-Aug-22	Vienna, Austria	Auditor	N/A	KEMEA
21	IAC 2022 Paris	Conference	18/22-Sep-22	Paris, France	Speaker, Booth	Improving ICE Cubes security resilience with 7SHIELD	Mathieu Schmitt (SPACEAPPS), CS, DES, DEIMOS
22	9th EDEN Conference on Data Protection in Law Enforcement	Conference	19/20-Sep-22	The Hague, Netherlands	Auditor	N/A	CENTRIC
23	3rd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2022) (CPS4CIP 2022)	Conference	26/30-Sep-22	Copenhagen, Denmark	Speaker	Solutions for Protecting the Space Ground Segments: From risk assessment to emergency response	STWS, KEMEA
24	CERIS FCT/INFRA annual event	Workshop	27/28-Sep-22	Brussels, Belgium	Speaker	General presentation of 7SHIELD project	STWS
25	Space Tech Expo Europe 2022	Conference	15/17-Nov-22	Bremen, Germany	Booth	7SHIELD brochure and infoboard at booth	DES, DEIMOS
26	International Exhibition BEYOND 2022	Workshop	29-Sep-22/1-Oct-22	Thessaloniki, Greece	Booth	General presentation of 7SHIELD project at booth	STWS
27	CERIS event on "Innovation Uptake of EU-funded Security Research outcomes"	Workshop	1-Dec-22	Brussels, Belgium	Speaker	General presentation of 7SHIELD project	STWS
28	Finnish Satellite Workshop with Finnish Remote Sensing Days	Conference	18/19-Jan-23	Espoo Dipoli, Finland	Speaker	7SHIELD framework for Ground Station cyber-physical security solutions	Timo Ryyppö, Tapani Mikkola (FMI)

At the time of writing this deliverable, 7SHIELD has been invited to be presented at the second meeting of the Critical Entities Resilience Group (CERG), 20 March 2023, Conference Centre Albert Borschette, Brussels.

3.1.1. Scientific publications

In the following table are listed all the scientific publications have been submitted in the second reporting period.

Date	Title	Author(s)	Type of publication
18/02/2023	Solutions for Protecting the Space Ground Segments: From risk assessment to emergency response	Ilias Gkotsis, Leonidas Perlepes, Aggelos Aggelis, Katerina Valouma, Antonis Kostaridis, Eftichia Georgiou, Nikolaos Lalazisis, Vasiliki Mantzana	Workshop (Springer Book)

15/02/2023	Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience	Habtamu Abie, Ilias Gkotsis, Manos Athanatos, Rita Ugarelli, Denis Caleta, Lorenzo Lodi, Fabrizio Di Peppo, Aleksandar Jovanovic	Virtual Workshop (Steinbies-Edition)
28/07/2022	Modelling and assessing the risk of cascading effects with ResilBlockly	Irene Bicchierai, Enrico Schiavone, Francesco Brancati	Conference
22/07/2022	*Study on the Application of EfficientDet to Real-Time Classification of Infrared Images from Video Surveillance*	Filipe Mendes, Armando M. Fernandes, Luis Fernandes, Fernando Piedade and Paulo Chaves	Conference
01/04/2022	*A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants*	Luigi Coppolino, Salvatore D'Antonio, Vincenzo Giuliano, Giovanni Mazzeo, Luigi Romano	Journal

3.2. Collaboration and networking activities

- 3rd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021) [08/10/2021 and 26-30/09/2022], supported by the European Cluster for Securing Critical Infrastructures (ECSCI). Two works were presented: Severity level assessment from semantically fused video content analysis for physical threat detection in ground segments of space systems (also published) and A holistic framework to protect Ground Segments of Space Systems against cyber, physical and natural complex threats. The paper presented during the 3rd annual workshop, entitled "Solutions for Protecting the Space Ground Segments: From risk assessment to emergency response", emphasizes cyber security tools developed within the framework of 7SHIELD (CIRP-RAT, ENGAGE CSIM and ERP solutions).
- Final conference of H2020 DroneWISE project - Sibenik, Croatia on May 20th, 2022
- The annual workshop of the EU-HYBNET project, empowering a Pan-European Network to Counter Hybrid Threats, (No. 883054) on April 2022.
- 7SHIELD participated in 3 events supported by CERIS (Community for European Research and Innovation for Security):
    - The CERIS FCT: Protection of Public Space (April 2022),
    - the CERIS INFRA 2022 workshop: How research supports the directive on the resilience of critical entities (July 2022) and
    - CERIS Annual Event 2022: Fighting Crime and Terrorism and Resilient Infrastructure (September 2022).
- SMI2G Event 2022, co-organised by EARTO Security & Defence Research Working Group, the SEREN network, EOS, IMG-S, ECSO and supported by ENLETS, on 16-17 May 2022 in Brussels.

3.3. Hands-on plenary board meetings

- 5th Plenary Meeting [28.02.2022]
- 6th Plenary Meeting [12-14.07.2022]

3.4. Phone calls and virtual meetings

- WP and TMC telcos - Every month

- First operational test of 7SHIELD tools on the Cyber-physical attack in the Ground Segment of NOA (Athens, Greece) [03.2022]
- 2nd EU-HYBNET Annual Workshop [06.05.2022]
- 2nd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop [27-29-04.2022]
- First operational test of 7SHIELD tools on the Cyber-physical attack in Deimos Ground Segment (Spain) [05.2022]
- Demonstration of 7SHIELD tools on the Cyber-physical attack in the Ground Segment of NOA (Athens, Greece) [09.2022]
- Demonstration of 7SHIELD tools on the Physical attack in Arctic Space Centre of FMI (Sodankylä, Finland) [10.2022]
- Demonstration of 7SHIELD tools on the Threat detection and mitigation in the ICE Cubes Service of SPACEAPPS (Brussels) [11.2022]
- 7SHIELD Info day preparation activities calls involving all the partners:
    - Plenary calls [03/10/2022 and 17/11/2022]
    - co-design days [03-04-05-16/11/2022]
    - KR interviews: 20 calls in October and November 2022 involving the KR owners for the production of KR leaftlets
    - Rehearsal of the infoday sessions [30/11/2022 - 01/12/2022 - 02/12/2022]

3.5. Other important outcoming events

- Meeting of the Critical Entities Resilience Group [20/3/2023]

4. Research ethics guidelines and recommendations

During the last period the consortium followed closely the required legal and ethical requirements as set out in WP9 – Ethics requirements; this is in addition to the legal and ethical safeguards considered as part of T2.4 – Ethics and legal framework.

The top-level outcomes from D2.3 were the following, these will be updated in D2.6.

- Identification for fundamental frameworks on human rights (i.e., European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the Charter of Fundamental Rights of the European Union (CFR)) and data protection (i.e., GDPR).
- Frameworks for the protection of National/European Critical Infrastructure, Space-related legislation and cybersecurity (i.e. NIS Directive) and their translation into national regulations
- System-based guidance including cyber-physical protection of ECI sites and UAV requirements and legislation (European and National)
- Legal and ethical considerations for data acquisition and use of artificial intelligence covering datasets, availability of open-source and online data, privacy, copyright, terms of service, video surveillance, facial recognition and wearable technologies for the 7SHIELD technologies.

In respect of WP9, the following deliverables were reported under the scope of the ethics requirements:

- **D9.1 H - Requirement No. 1** sets out the steps that 7SHIELD uses to identify and recruit research participants and a template for the informed consent and participant information sheets required for any activities involving humans as research participants. Specifically, 7SHIELD embeds the following principles for humans involved in research: voluntary and consent-based participation; consent-based processing of personal data; no provisions of inducement for participation; freely withdrawable consent; acknowledgement and mitigation against employer-employee power imbalance in cases where research volunteers are from consortium members; full rights of the data subjects; no involvement of vulnerable groups; authorizations through local ethics committees and ethical conduct for all partners.
- **D9.2 H - Requirement No. 2** provides the incidental findings policy for 7SHIELD research that requires informing the Project Coordinator, Internal Ethics Board and the Project Officer.
- **D9.3 H - Requirement No. 3** provides statements of ethics compliance from the end-user partners in relation to their piloting activities. The statements are provided from: DEIMOS; DES; FMI; NOA; SERCO and SPACEAPPS.
- **D9.4 POPD - Requirement No. 4** provides the names of the data protection officers for each organisation within the project; and the technical and organisational safeguards put in place for engaging with human participants; face and activity detection and recognition; the analysis of social awareness; and the piloting activities.
- **D9.5 POPD - Requirement No. 5** evaluates the ethical risks within 7SHIELD in terms of data processing activities; and a conclusion on the need for a data protection impact assessment (DPIA). The analysis concluded that D9.8 will include a DPIA for 7SHIELD as a holistic solution as well as individual DPIAs for the activities of CENTRIC and SERCO in relation to their tasks.
- **D9.6 EPQ - Requirement No. 7** demonstrates the safety procedures put in place by 7SHIELD to manage the UAV flights required within the project's piloting phase and the associated permissions for undertaking research at the pilot locations and the approvals (from ACCELLIGENCE) for UAV flights have been obtained.

- **D9.7 DU - Requirement No. 8** confirmed that no partners will use tools that could be subject to dual use implications and therefore no export control licences are required.
- **D9.8 M - Requirement No. 9** provides a DPIA assessment for the previously identified partners (CENTRIC and SERCO)
- **D9.9 GEN - Requirement No. 12** establishes the Ethics Board which is comprised of Kirsi Aaltola (external ethics advisor); Helen Gibson (internal ethics member from CENTRIC); and Ioana Cotoi (internal ethics member from ENG).
- **D9.10 GEN - Requirement No. 13** provides an Ethics Board report about guidelines on how to address ethics issues within the pilot demonstrations at the critical infrastructure sites.

In April 2021, the draft proposed AI regulation was published by the European Commission, D2.5 will include a section that fully considers how 7SHIELD will be compatible with the requirements in the proposed regulation with respect to the use and potential future deployment of 7SHIELD technologies.

5. Conclusion

This document constitutes the final project progress report outlines the activities carried out by the project consortium during the following period: January 2022 (M17) - February 2023 (M30). As a result, it is an updated version of D1.3 - Mid-term review & progress report, which was submitted in April 2022 (M20). In this document, an overview of the achieved 7SHIELD objectives and project's results in terms of scientific and technological outcomes is provided. In addition, a summary of the main communication and dissemination actions as well as the provided research ethics guidelines and recommendations so as to be compliant with national or EU regulations is also reported with regard to the first period.

Horizon 2020
European Union Funding
for Research & Innovation

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