7SHIELD

D1.3 - Mid-term review & progress report

Work Package:	WP1
Lead partner:	ENG
Author(s):	Gabriele Giunta, Emilia Gugliandolo, Giuseppe Li Calsi (ENG)
Due date:	31/12/2021
Version number:	2.0 **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	13/11/2021	ENG	First release of the template
0.2	17/12/2021	ENG	First round of contribution
0.3	23/12/2021	ENG	Second round of contribution
0.4	27/12/2021	ENG	Version ready for peer review
1.0	30/12/2021	ENG	Final version
2.0	30/04/2022	ENG	Revised version after mid-term review recommendations

Quality Control

Role	Date	Who	Approved/Comment
Internal reviewer	29/12/2021	CERTH	Document accepted, only minor changes suggested

Disclaimer

Executive Summary

This report provides an overview of the 7SHIELD project progress carried out by the project consortium during the first period, namely from September 2020 (M1) to December 2021 (M16). 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 first period, namely from September 2020 (M1), to December 2021 (M16).

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 and future outlook.

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 – The baseline for the impact & risk assessment model development is the Critical Infrastructure Resilience Platform (CIRP) capitalizing on the results of the previous EU Research project entitled EU-CIRCLE. CIRP allows the integration of various risk and impact models, analyses what-if scenarios and calculates vulnerability and impact for several threats in a unified environment. The main achievement in the reporting period was the release of an integrated prototype of the multi-hazard risk assessment tools (KR1) implements a scenario-based approach focusing on the analysis of the impact that is produced on the assets by their exposure to various hazards. The integration among cyber, physical and natural hazard risk assessment tools was clearly defined. Functionalities related to the risk assessment of cyber threats were already implemented, demonstrated and evaluated during the first two Pilot Use Cases (i.e. PCU4 and PCU5). The risk assessment process of natural and physical threats will be demonstrated and evaluated during the next period in PCU1, PCU2 and PCU3. Within 7SHIELD it is expected for the risk assessment functionality to integrate more than five (5) risk and impact assessment models and ingests an unlimited size of datasets. In 7SHIELD, the target value related to KPIs 1.1.1 and KPI 1.1.2 is fully achieved (100%).		
IA1.2 – The baseline for the operational solutions implemented for the Access Control Systems, including the federated identity management that spans across different organizational or services boundaries, is defined according to the targets for the service performance that includes the monitoring of the percentage of logins with regard to the user identity profiles. Usually, the range of 95%-97% of successful logins according to the user identity profiles is considered an 'acceptable' performance indicator while 97%-98% is 'good'. In 7SHIELD, we achieved the target value of 100%. To evaluate the successful authentication/authorization of end users in the secure authentication mechanism, an instance of the open-source identity and access management solution, Keycloak, enabling the two endpoints (i.e. OpenID endpoint configuration and SAML 2.0 identity provider metadata) has been deployed on the OVHcloud environment.		

Keycloak provides customizable user interfaces for login, registration, administration, and account management. The user identity profiles are defined within the realms by using different groups or roles. Realms are isolated from one another and can only manage and authenticate the users that they control.
The Keycloak instance was interfaced with the SERCO reference environment in order to enable the self-user registration on the ONDA-DIAS catalogue validated during the SERCO PUC took place in October 2021. In addition, two 7SHIELD modules (MBDA and DiVA) were successfully interfaced with the secure authentication mechanism validated during SPACEAPPS pilot in November 2021.

IA1.3 – in the reporting period, a study on existing research projects, methods and tools of analysis of cascading effects and interdependencies was accomplished. Analysis methods can be divided into four groups: empirical, economic-based, agent-based and system dynamic-based.
Then, a methodology for the assessment of cascading risk due to complex threats has been defined. The method has been chosen is a mixed method between network based and empirical; it uses the graph theory in order to obtain metrics to assess the cascading effects. This method does not need a large amount of data, in fact for the analysis it is sufficient to define the assets and the various dependencies between assets. This method allows assessing the cascading risk due to *nth-order* dependencies and it permits the detection of high impacts that would otherwise not appear if only the immediate risk caused by a threat were to be considered. The analysis result allows the decision maker to have a more accurate view of how threats can affect infrastructures, data and assets.
Finally, the chosen methodology has been implemented in the MBDA tool. First, the functionality of the MBDA for the analysis of cascading effects was designed through mockups. In the Model Designer, a new tab was inserted, dedicated to the analysis of cascading effects which in turn consists of three different inner tabs: Asset dependencies, Initiating Threat and Cascading Graph. Once inserted information about definition of dependencies between assets and information about the risk associated to an initiating threat, the tool produces a table of the cascading effects generated by that initiating threat, showing the various paths in the graph of dependencies, ordered by the Cumulative Dependency Risk.
The baseline has been defined considering the tool Blockly4SoS developed by ResilTech in order to provide a low complexity still rigorous solution for system of system modelling and early prototyping. In the MBDA tool existing features of Blockly4SoS have been refactored and new ones have been introduced such as, for instance, the assessment of risk due to cascading effects. Thus, we consider as the performance indicator KPI 1.3.1 the number of identified threats due to cascading effects and as target value, a value greater than zero, since this functionality was not present in the previous tool. Regarding the progress, the implementation of the cascading effects analysis functionality will be finalized in the second period, so in the first period the percentage of achievement of the KPI 1.3.1 is 0% (not achieved). We can add that the percentage of completion of the implementation of the cascading effects analysis functionality is 75%. When the implementation will be finalized, the functionality will be tested in the incoming pilots

IA1.4 – To evaluate the performances of the CPTI framework against state-of-the-art results, we applied the following protocol: each class of the TwitterDataset (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 performances.		
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 – 25km^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 – the main achievement in the reporting period is the release of the 1st prototype of the 7SHIELD UAV which is fully customised to accommodate the various hardware components (e.g. height/distance sensors, cameras) so as to perform on-board image processing making use of deep learning-based techniques. Visible light sensors (RGB) were embedded in 7SHIELD UAV in order to acquire high-spatial and temporal images that can facilitate the surveillance of a specific area (covering a predetermined distance/radius around the ground stations). 7SHIELD UAV will be able to operate under two different modes, namely the Scheduled mode and Alert mode.

More specifically, the 7SHIELD UAV is an octa-copter with the following characteristics: max thrust (nominal) 22.8 kg; vehicle mass approx. 7.5 kg; vehicle mass (batteries, camera & companion computer included) approx. 10 kg; max takeoff weight (50% of max thrust) 11.4 kg; dimensions (between opposite rotor shafts) 1.26 m; flight time up to 40 min (depends on payload and wind); flight radius with radio control: max 1500 m, with waypoints: it depends on power consumption, payload and weather conditions operating; temperatures -10 to 45 °C. Due to its optimized design, it has an extended flight time of up to 30 minutes, which is a substantial advantage when compared to conventional models currently available in the market, and a high precision localization of 1cm using GPS-RTK2. The experimental results in the laboratory exceed an improvement approximately 30.43% for 30 minutes operation measured from 23 minutes (KPI A2.1.1). The KPI A2.1.1 was already achieved in the lab and we are planning to validate it during 7SHIELD demos. In addition, 7SHIELD UAV is one of the first UAV with a separate onboard computer with an embedded Jetson Xavier processor, running the latest version of Robot Operating System (ROS) in order to host Artificial Intelligence (AI) algorithms for object detection and identification for edge processing. This feature is expected to enhance the surveillance capacity of 7SHIELD UAV reducing the time needed for an inspection mission to no more than 20 minutes. In field validation trials 25 minutes operation measured (KPI A2.1.3 – achieved) and 25 km2 monitored area in one mission assessed (KPI A2.1.4). The KPI A2.1.4 was achieved through simulations and estimations from the field trials as it is impossible to execute no line of sight flights due to the current regulation limitations. Thus, the specific KPI was theoretically achieved.

A fully customized Mission UAV was manufactured in order to execute smart algorithms (e.g., visual object detection and collision avoidance services, algorithms for swarming), and generally to be easily adapted to the current operation by the user.

7SHIELD Mission UAV will be capable to perform on-board image processing, making use of machine learning-based techniques, and more precisely Deep Neural Networks (DeepNN) and

Convolutional Neural Networks (CNN) exploiting the data (e.g., 2D/ 3D images/ point clouds) obtained from the various aforementioned sensory inputs.
Further to this and thanks to the embedded processing power, the proposed module will be able to operate in 'offline' mode, thus it can operate semi-autonomously without any connection with 7SHIELD IC3 system, increasing further the inspection duration, as there is not any power loss due to the telecommunication link between the UAV and the control room. A kafka server installed in GPU for 100% offline operation (KPI A2.1.2). Therefore, KPI A2.1.2 was successfully achieved. Finally there were not any laboratory results for KPI 2.1.5, as it is strongly related with the KR06 and KR07. This KPI will be validated and demonstrated in the secord reporting period following the timeline of the project.

IA2.2 – the main achievements in the reporting period are the following:

- Development of the 1st version of the Face Detection and Recognition (FDR) module. So far, the FDR processes offline video files in order to detect faces that may belong to unauthorized individuals. 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. The accuracy of the adopted Face Detection model (DSFD[1]) was tested against the baseline (TinyFaces[2]) on the Wider Face[3] dataset using the average precision (%) metric. The model's average precision is 95.5%, 4.8% over the baseline (90.7%). The speed of detection is 4.2 frames per second, but the detection can be executed in real-time using frame dropping without sacrifice in performance in the context of a use case scenario. The accuracy of the Face Recognition model (FaceNet[4]) was tested against the baseline (DeepFace[5]) on the LFW[6] dataset using the accuracy (%) metric. The model's accuracy is 99.4%, 0.45% over the baseline (98.95%). The execution time for a single face recognition process increases linearly with the size of the matching gallery. The maximum time reached was 1ms with a gallery size of 100 people which can be considered negligible.
- Development of the 1st version of the Video-based Object Detection (VOD) and Activity Recognition (AR) modules. The VOD module processes still images/frames in order to locate and recognize objects of interest in the provided sources. For the detection, deep learning techniques enabled to visually locate and identify the object of interest in the Critical Infrastructure area are utilised. Additionally, after detecting any human presence in the scene the corresponding results of object detection will be propagated to the AR module to identify suspicious and harmful activities. The main purpose of these modules is the accurate and efficient visual interpretation of the surroundings of the surveillance area. Moreover, a "lighter" version of the aforementioned approaches can be embedded in GPU aiming to process video content at the edge by the Object Detection at the Object Detection at the Edge (ODE) module. This lighter version will run on the autonomous

[1] Li, J., Wang, Y., Wang, C., Tai, Y., Qian, J., Yang, J.,& Huang, F. (2019). DSFD: dual shot face detector. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5060-5069).
[2] Hu, P., & Ramanan, D. (2017). Finding tiny faces. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 951-959).
[3] Yang, S., Luo, P., Loy, C. C., & Tang, X. (2016). Wider face: A face detection benchmark. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 5525-5533).
[4] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).
[5] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition.
[6] Huang, G. B., Mattar, M., Berg, T., & Learned-Miller, E. (2008, October). Labeled faces in the wild: A database forstudying face recognition in unconstrained environments. In Workshop on faces in'Real-Life'Images: detection, alignment, and recognition.

7SHIELD UAV and will be capable of performing on-board image/video processing by focusing on object detection from captured videos by the drone.

- A series of evaluation measurements were utilised in order to estimate the modules' performance. Regarding the VOD module, the model being developed has two custom models involved, which are based on EfficientDet models. The first one being more generic for outdoor detection of objects, which can detect 5 classes, and the second one focusing on indoor object detection which can detect 2 classes of objects. The qualitative results are shown in the four following tables. It must be noted that two (2) models are not comparable as the object instances in the first case are generally smaller and more difficult to be detected and, thus, no comparison can be made between them:

baseline outdoor EfficinetDet phi2 Average Precision (AP)		
51.11% (person)	70.35% (bus)	74.68% (car)
47.97% (motorcycle)	67.82% (truck)	**mAP 62.39%**

Improved model outdoor EfficinetDet phi2 Average Precision (AP)		
52.42% (person)	75.36% (bus)	76.68% (car)
52.94% (motorcycle)	69.22% (truck)	**mAP 65.32%**

baseline indoor EfficinetDet phi1 Average Precision (AP)		
86.26% (person)	83.28% (packpack)	**mAP 84.77%**

improved model indoor EfficinetDet phi1 Average Precision (AP)		
86.40% (person)	85.07% (packpack)	**mAP 85.73%**

Regarding the efficiency of the models, the second one is faster than the former one and achieves more than 35 fps while the first one processes images with a speed of around 30fps.

Concerning the Object Detection at the Edge (ODE) model, preliminary experimental evaluations were carried out attempting to evaluate both the efficiency as well the effectiveness of the model. For the efficiency of the model, we run the same model of Yolo v4 model a) on a machine equipped with a GPU NVIDIA GeForce RTX 3090 and b) on a Jetson AGX257Xavier GPU. As it can be expected there is a great difference in the processing speed, the NVIDIA RTX 3090 has achieved to process 29 frames per second (fps) against 4.8 fps that were processed by the Jetson AGX Xavier. Regarding the effectiveness of our model to detect the 5 classes, namely person, car, truck, bus, motorcycle, the experimental evaluations exhibit that the best precision is achieved for class bus and it's 81.16% while the mAP for all 5 classes reaches 60.93%. Specifically, the per class precision as well as the overall mean Average Precision (mAP) are shown in the following Table:

Yolo v4 effectiveness evaluation - Average Precision (AP)		
70.47% (person)	59.88% (car)	56.22% (truck)
81.16% (bus)	64.2% (motorcycle)	60.93% (mean AP)

We intend to further improve this performance and consider this as a baseline for improved results.

IA2.3 – the main achievement in the reporting period was the development and deployment of the Cyber-Attack Detection (CAD) framework which is capable of collecting security events from end-node sensors, correlating events coming from heterogeneous sources, providing analytics on the status of the system and raising alerts in case of dangerous scenarios. The framework consists of three main components: a) the Cyber-Attack Detection Layer; b) the Cyber-Attack Correlation Layer and c) the Graphical User Interface. The CAD was successfully deployed and tested in the first two Pilot Use Cases, in SERCO and SPACEAPPS, over a total of 4 misuse cases (KPI2.3.2 = 5). The KPI2 achievement during the reporting period was around 40%. It will be 100% completed with the advancement of the demos and operational tests scheduled within the project. The CAD framework has been already successfully tested against 5 high impact attacks (KPI2.3.1 = 5) with a percentage of achievement around 50%. Additional attacks leading to 100% achievement for KP1 will be considered by the end of CADF component validation that is going to be documented as part of *D4.4 – Cyber-attack detection methods* due at M21 (May 2022).
As for KPI2.3.3 (Performance penalty of TE technology), we have not yet evaluated the impact of TE technology. Past experiments conducted in our laboratory, also reported in the paper *VISE*[7]*: Combining Intel SGX and Homomorphic Encryption for Cloud Industrial Control Systems*, demonstrated that the target of less than 10% of overhead is plausible when limiting the adoption of Homomorphic Encryption. At the moment, we are featuring Trusted Execution in the context of the SpaceApp pilot. Once the setup will be ready, we will be able to provide an evaluation of the KPI and thus to consolidate our results and confirm our expectations.

IA2.4 – the main achievements in the reporting period are the development of the MultiModal Automated Surveillance (MMAS) system which is capable to detect possible threats through the use of video images that are within a Field of View (FoV) of a thermal camera. The MMAS system is based on a network of Near-InfraRed (NIR) and Thermal EO sensors that are supported by multiple processing servers, which process the video images from cameras, by employing Convolutional Neural Networks (CNN) to classify three kinds of entities: reindeers, vehicles and persons. The MMAS sends the alarms to the 7SHIELD platform where multiple correlators will determine if the alarms are real threats. The MMAS is composed also by a User Interface (UI) that

[7] [VISE] L. Coppolino, S. D'Antonio, V. Formicola, G. Mazzeo and L. Romano, "VISE: Combining Intel SGX and Homomorphic Encryption for Cloud Industrial Control Systems," in IEEE Transactions on Computers, vol. 70, no. 5, pp. 711-724, 1 May 2021, doi: 10.1109/TC.2020.2995638.

permits an operator to monitor the area under surveillance, configure and set the alarms. The MMAS is ready to be integrated with the 7SHIELD and perform the first integration tests.
The KPI for the MMAS was chosen having as a baseline the performance of other automated surveillance systems. The KPI is normally used to evaluate the performance of machine learning algorithms and tracking algorithms, namely the classification of vehicles, persons and animals (deers) and tracking of objects. These require the existence of data taken from real situations. The first iteration was tuned with the use of public data sets, with thermal images available from a internet data set. The second iteration is being made with a data set based on video images taken from the thermal camera chosen for the 7SHIELD. At the time of this report, there were available only results from the Internet data set and due to the dispersion of the quality of the images, unfortunately the KPI was not yet fully achieved even though the percentage of achievement is about 80%. During the next reporting period the integration with the core system will be concluded. A new evaluation will be done with the use of images taken from the 7SHIELD camera in several situations and using improved algorithms.

IA2.5 – the main achievements in the reporting period are the deployment of the 1st prototypes of the Perimeter Laser Sensor (PLS), the Laser Fence Sensor (LFS) and the 3-Dimensional Mini drone (3D-MND) detectors. The PLS and LFS are two DFSL's innovative 2-dimensional laser-based detection systems with slaved PTZ cameras, to be incorporated with dedicated software and DFSL proprietary algorithm – for detection of human and vehicular intrusion on the ground level, and connectivity to state-of-the-art nodes and modern technologies. The 3D-MND is the DFSL's innovative 3D laser-based detection system with a slaved camera, to be incorporated with specially developed DFSL software – for detection of drones over the sky of the pilots against aerial threats from drones. For integration purposes with the 7SHIELD platform, a customised Universal Local Server (ULS) was also developed and its communication with the platform will be tested and evaluated. KPIs are detection and tracking of intruders (human, vehicle and drone) using Laser Sensors with slaved PTZ camera and following up through the track capability. Since in the first reporting period, development and implementation work on all sensors were completed, and in-house foeld trials commenced, the KPI was partially covered (60%). Finalisation of field trials and on-site trails at pilots will be followed during second reporting period.

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

- Development of the Availability Detection Monitoring (ADM) module which aims to monitor the availability of configured components and servers and generates alerts in case a status change is detected. It has been deployed on two Pilot Use Cases, in SERCO and SPACEAPPS. The ADM module successfully detected 100% of the simulated malfunctions used in both Pilot Use Cases' testing phases. ADM is fully developed and SSL secure connection developed ready to be integrated.
- Development of the Availability Correlation (AC) module which takes availability alerts generated by the ADM module and aggregates alerts related to the same incident together. The module is currently being integrated into the 7SHIELD framework but not yet deployed at any Pilot Use Case. AC fully developed and tested SSL secure connection developed ready to be integrated.
- Development of the Cyber-Threat Intelligence Detector (CTID) module which adds cyber-threat intelligence data to the cybersecurity alerts generated by the Cyber-Attack Detection (CAD) and Cyber-Attack Correlation (CAC) modules. The module is currently being integrated into the 7SHIELD framework but not yet deployed at any Pilot Use Case. CTID fully developed still need to develop the SSL secure connection but tested successfully on internal platform
- 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 HCC module is currently being integrated

into the 7SHIELD framework but not yet deployed at any Pilot Use Case. HCC will be tested during NOA pilot.

- During the reporting period, the Geospatial Complex Event Processor (G-CEP) component was enhanced in order to support the receiving and correlation of the events that will be detected by the physical sensors. In order to support that operation, a number of functionalities have been designed and implemented. In more detail, the support of the format of the messages that will be produced by the physical sensors was implemented. The correlation of these events is based on a number of correlation rules/patterns that were identified during that period. Enhancement of these rules will be implemented during the upcoming monthsIt will be tested during NOA pilot.
- Development of the 1st prototype of the Situational Picture Generation & Update (SPGU) module which aims to provide a clear Situational Picture of the SGS the 7SHIELD system is monitoring. The main sources of information exploited by the SPGU are represented by the 7SHIELD correlation modules (e.g. cyber, physical and cyber-physical) and by any 7SHIELD tool able to provide useful information that can contribute to the creation of the Situational Picture. Currently, the SPGU correlates the information with those coming from the tools included in the prevention and preparedness phase, such as MBDA, DiVA, CIRP and in the response and mitigation phase, such as the 7SHIELD correlation modules (CAD, G-CEP, ADM).

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: not yet achieved.

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, catching the drone and bringing it back to designated ground area.

Achievements

IA3.1 – the 7SHIELD Knowledge Base (KB) or 7SHIELD ontology is a knowledge representation model for semantically representing concepts relevant to the cyber-physical threats. In the reporting period, the KB framework has been developed that encompasses technologies for semantic content and sensor input modeling and integration. The models that were created constitute the reasoning mechanisms taking into account the ontology vocabulary and infrastructure for capturing and storing information related to the 7SHIELD application domain. The KB can be populated automatically with semantic information provided by the correlators of the 7SHIELD. For this purpose, a dedicated component has been created that enables the conversion of JSON format to RDF and upload the information to the 7SHIELD database (GraphDB). Moreover, all stored data can be retrieved from GraphDB with specific SparQL queries. About metrics on the current version of the 7SHIELD ontology was used qualitative and quantitative criteria.

Qualitative: For measuring the qualitative value we used as criteria the percentage of the answered Competency Questions that were formulated during the ontology requirements elicitation process.

Competency Question

1. Observations
   - 1.1. What is the severity of the observation [X]?
   - 1.2. What is the confidence of the observation [X]?
   - 1.3. What is the analyser category that made the observation [X]?
   - 1.4. What is the detection/creation time of the observation [X]?
   - 1.5. Which analyser made the observation [X]?
   - 1.6. Which is the GeoLocation of the analyser[X]?
   - 1.7. Which is the UnLocation of the analyser[X]?
   - 1.8. Which is the Location of the analyser[X]?
   - 1.9. Which is the method used by the analyser[X]?
   - 1.10. What is the data used by the analyser[X]?
   - 1.11. In which infrastructure does the observation [X] take place?
   - 1.12. Which is the most/least severe observation?
   - 1.13. Which agents where detecting between time intervals []-[]?
   - 1.14. Which observations occurred after time []?
   - 1.15. How many physical vectors were detected between time intervals []-[]?
   - 1.16. How many physical vectors were detected between time intervals []-[]?
   - 1.17. What is the Location of the target in the observation [X]?
   - 1.18. What is the IP of the source in the observation [X]?

2. Threats
   - 2.1. What is the category of the threat [X]?
   - 2.2. What is the source/target IP in a cyber threat [X]?

2.3. What is the type of intruding object [X]?
2.4. What is the type of the recognised activity [X]?
2.5. Who is the recognised face[X]?
2.6. How many Incidents[X] were recorded?
2.7. What type of threats are detected between time intervals []-[]?
2.8. Which is the manifestation of threat [X]?
2.9. Which infrastructure is targeted the most?
2.10. Which is the most/least common threat [X]?
2.11. Which observation led to the threat [X]?

3. Risk Assessment & Mitigation Plan
   3.1. What is the location of the FR [X]?
   3.2. Who is the leader of the FR [X]?
   3.3. What is the current mitigation plan of the FR [X]?
   3.4. For which incident is the mitigation plan?
   3.5. What is the location of the FlyingHunter?
   3.6. What is the Impact on the Critical Infrastructure [X]?
   3.7. What is the Likelihood on the Critical Infrastructure [X]?
   3.8. What is the Vulnerability on the Critical Infrastructure [X]?
   3.9. What is the Condition of the FR [X]?

From these CQ the 7SHIELD KB is capable to answer almost all, with an exception of the 3.1, 3.2, 3.5, 3.9 because we lack of the specific data, satisfying 89% that exceeds the minimum targeted value. Additional using OOPS (pitfall scanner) to enhance quality evaluation, we corrected all the important and critical pitfalls that we detected

Quantitative: The nature of the 7SHEILED KB makes it so specific that it is hard to set an specific baseline to the Quantitative criteria. However, using a tool (Ontometrics) we can evaluate some of the core metrics of the ontology like the attribute, inheritance and relationship richness as well as some ratios between classes and axioms. The metrics may differ from the ones presented in the D5.1 because of some modifications and extension to the ontology

Axioms	615
Logical axioms count	261
Class count	100
Total classes count	100
Object property count	37
Total object properties count	37
Data property count	22
Total data properties count	22
Properties count	59
Description Logic expressivity	ALCHI(D)

IA3.2 – the main achievement in the reporting period is the development of the 1st version of the Crisis Classification module that provides real-time assessments of the severity level of an ongoing physical, cyber, or a combination of the two (C/P) attacks, in critical satellite and ground segments. In order to achieve this goal, machine learning methods have been developed that are able to fuse the information of the various modalities, namely the 7SHIELD correlators/detectors. The utilisation of machine learning methods needs annotated datasets to fit the models. Hence, a web-based application was developed, called Annotation Tool, which enables to capture the

domain knowledge and experience of the experts by characterising in terms of the severity level hypothetical scenarios of physical and/or cyber-attacks in specific locations/assets in the Satellite Ground Stations (SGS). So far, in total 1088 cyber-attack scenarios and 762 physical attack scenarios were annotated by the experts in the 5 pilot sites of SGS. The preliminary experimental evaluations exhibit that the accuracy (F1-score) of the models to classify the cyber-attacks in terms of their severity fluctuates between 60% (SVM) to 74.25% (Random Forest). In the case of physical attacks, the accuracy of the models fluctuates between 65.38% (Random Forest) to 78.9% (SVM). In a previous project (beAWARE[8]) where the Crisis Classification module was applied, a rule-based approach based on linear formula was utilised for the severity assessment of natural hazardous events. Although the application domain is quite different, however, we can consider that approach as a baseline and estimate the severity level of the hypothetical scenarios of physical and/or cyber-attacks using the linear approach. 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%.

IA3.3 – the TDSS (Tactical Decision Support System), is a complex system, which is based on a pro-security vest, embedded with wearables sensors, communication transceivers and an UTD (Universal Tactical Display) for action team leader. The first responder teams once equipped with the FRSS (First Responders Support System) will become self-aware and have more information to support effective decision making in the field with or without an infrastructure or C2 support. At the same time, the C2 will also receive real-time information about the team on the field, crucial to improve the awareness of the mission rollout and taking last-minute decisions.

The main achievement during this report period is the build of the first lab prototype with all hardware components and the successful migration of all software components developed for the TDSS from the simulation platform to the final hardware of the TDSS.

Regarding the KPI 3.3.1, defined for the TDSS, related to the speed and quality of the information provided, it is based on the knowledge of similar systems, not necessarily for the same type of application, that follow some kind of rule model and also apply inference algorithms, with regard to the communication with C2, the definition and assignment of missions and the preparation and availability of information to the team leader in the field.

To date, the TDSS system has been established as the 1st lab prototype and has already been subjected to several tests in a controlled environment, in which some systems belonging to C2 are simulated, while others, which are already at a more advanced stage of development "the final ones" are already integrated (e.g. the connection to 7SHIELD's KafKa broker).

This way and based on the results already obtained in laboratory, which are fully in line with expectations. At the moment, the KPI achievement is around 70%, with the remainder depending on the future validation of the TDSS, fully integrated into 7SHIELD, after performing real environment tests, and the introduction of optimizations to the prototype, namely at the level of user interfaces (UTD). With the data available and results obtained so far, everything points for the objective defined for the TDSS being fully achieved and in which it produces and makes available 75% of relevant information.

In the next reporting period the development will be concluded, the final integration will performed with the 7SHIELD core system and the pilots will be done.

IA3.4 – social interaction and awareness raising with the citizens takes a three phases approach to developing appropriate message content to warn citizens in the event of a local incident that affects their safety and security. The first phase analyses messages relating similar physical and cyber-attacks on critical infrastructure and the core content and levels of engagement with these messages; the second phase analyses pilot partners existing communications activity to understand the gaps and capabilities in their communication processes; while the third phase

[8] https://beaware-project.eu/

develops a standardised warning message generation framework to support rapid and clear communication with citizens across multiple languages. The first reporting period has focused mainly on the first phase of this approach. As the KPI 3.4.1 is related to user acceptance testing during piloting activity, IA3.4 is due to be evaluated during the final three demonstration activities, namely NOA, FMI and SPACEAPPS demos to be reported in the second period.

IA3.5 – the UAV neutralizing an intruding drone tool is a green technique non-destructive. Is a specially designed and assembled drone (Flying Hunter – FH) developed by DFSL which will be used for capturing/catching the intruder drone while it is in flight. This FH will be fitted with under-belly net which will be used for "catching" the intruder drone. Initial phase of FH flight will be based on coordinates of intruding drone received from 3D MND, whereas final phase of "catching" would be done manually by a skilled operator. The intruder drone can be analysed to obtain complete information about its payload and uploaded waypoint. The main achievements for the period were the development of the FH and the flight tests done with it to validate the method and detect solve problems that arise during the tests. KPI for UAV neutralisation is flying to the target drone and "catching" it, and bringing it back to pre-determined location. In the first reporting period, development and implementation works have been completed, and in-house flight trials are being conducted. KPI was partially achieved (55%) During the second reporting period, in-house trials would be completed and on-site trials would be undertaken.

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 minimum Acceptable Downtime of critical services is achieved.

Achievements

IA4.1 – the aim of the activity is to develop various service continuity scenarios for assessing the efficiency of the actions that need to be taken in response to physical and/or cyber stressors of different severity. The service continuity scenarios to be developed will account for different (a) single/multiple attacks and severity levels, (b) critical infrastructure vulnerability levels (link to Task 3.1) (c) local/national security regulations and (d) relevant international standards, namely ISO22301.

During the reporting period, a generalized physical operations model has been generated for representing the Operation Technology functionality of each PUC. 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 first reporting period, the implementation of the service continuity software module has only been tested in vitro, and it has consistently shown a reduction of downtime to cyber attacks thanks to increased awareness and timely quantification of system-level consequences.

This reduction has been measured in virtual scenarios to be in excess of the % required. Still, this will have to be tested in upcoming demos, as the actual performance will depend on other 7SHIELD systems as well. Therefore, this KPI is considered to be only partially fulfilled (50%). Final integration into the 7SHIELD solutions and testing in vivo will be undertaken in the next period to fulfill the KPI.

IA4.2 – similarly to IA4.1, a generalized cyber operations model has been generated for representing the Information Technology functionality of each PUC. The cyber and physical models will be interconnected in order to produce a unified view of consequences to cyber-physical operations.

During the first reporting period, the implementation of the service continuity software module has only been tested in vitro, and it has consistently shown a reduction of downtime to physical attacks thanks to increased awareness and timely quantification of system-level consequences. This reduction has been measured in virtual scenarios to be in excess of the % required. Still, this will have to be tested in upcoming demos, as the actual performance will depend on other 7SHIELD systems as well. Therefore, this KPI is considered to be only 50% fulfilled. Final integration into the 7SHIELD solutions and testing in vivo will be undertaken in the next period to fulfill the KPI.

Innovation Objectives	Innovation Activities	KPIs
IO5. 7SHIELD platform development	**IA5.1** 7SHIELD platform integration (KR18)	**KPI 5.1.1**: 7SHIELD modules integrated and deployed in the Framework.
	IA5.2 Data Models for Combined Detection (KR19)	**KPI 5.2.1**: Semantic concept defined.
	IA5.3 User interfaces/Command and Control (C2) room (KR20)	**KPI 5.3.1**: Common Operational Picture refresh updates; **KPI 5.3.2:** Number of assets depicted on map (without clustering) without flickering; **KPI 5.3.3**: Standards supported.

Achievements

IA5.1 – during the first reporting period, 17 out of 32 components were integrated in the first prototype of the 7SHIELD FRAMEWORK released at M10 (June 2021). Details on the communication and interoperability interface as well as integration and deployment schema were provided in *D6.3 – System integration and interoperability v1* (classified as EU-RES).

During the reporting period, 16 out of 32 components were integrated and deployed at PC5 (SERCO) and PC4 (SPACEAPPS), respectively at M14 (October 2021) and M15 (November 2021). Therefore KPI 5.1.1 was partially achieved (50%). Next Pilot Operational Tests are going to take place in March 2022 (PC2 – NOA) and May 2022 (PC3 – DEIMOS), while Pilot Demos are going to take place in September 2022, October 2022 and November 2022, respectively in Greece (NOA), Finland (FMI) and Belgium (SPACEAPPS), according to the integration and validation plan (D6.3). KPI 5.1.1 will be fully achieved at the end of the year after SPACEAPSS demo pilot.

IA5.2 – during the reporting period, data models considered in the main 7SHIELD components were analysed and defined. A first set of ontologies was analysed with the aim to identify those can be adopted in the context of 7SHIELD. The 7SHIELD ontology was defined to be used in the context of WP4. During the first periodic period, the 17 fundamental classes of 7SHIELD ontology were described. Moreover, a new version of the Unified Alert Format (UAF) was released to be adopted in 7SHIELD for the exchange of information related to alerts, threats, and combined

threat scenarios. Here, 7 main classes along with the 17 categories described in the Reference Security Incident Taxonomy (RSIT) were defined. Finally, the design of the 7SHIELD Situational Awareness Data Model and the main 15 entities were accomplished and completed so as to be evaluated in the context of PUC4 and PC5**.** As result, the KPI 5.2.1 was fully achieved in the first reporting period.
IA5.3 – The baseline for the 7SHIELD User Interfaces & C2 components is the ENGAGE PSIM (Physical Security Information Management) system provided by STWS. It is a legacy system that provides the users with monitoring and management capabilities of information produced by physical security systems (e.g. CCTV, radars etc.). In the context of the 7SHIELD project, this legacy system has been enhanced (and will be further enhanced) in order to support the management of security data and tools. The integration with the dashboard components has been designed for that purpose. During the reporting period, an initial version of the 7SHIELD user interface components was designed and implemented. The User Interface (UI) was designed according to the user requirements, objectives of the project and the type of information to be presented to the users/operators of the platform. An initial version of the UI components was demonstrated and evaluated during the first two pilots. Taking into consideration the related KPIs, 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), hence currently, it is partially achieved (50%). 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. Currently, 70% of the 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
UO1. Use case definition and requirements	**UA1.1** Use case design, stakeholder engagement and user requirements	**KPI 1.1.1**: 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.
	UA1.2 Security requirements	**KPI 1.2.1:** Secure access to the system, secure communications.
	UA1.3 Ethics and legal framework	**KPI 1.3.1**: 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.

Achievements

UA1.1 – the objectives of the use case design, stakeholder engagement and user requirements activities for the first project period (M1-M16) were fully achieved. Five use cases of five different EU countries (Finland, Spain, Greece, Belgium and Italy) were thoroughly designed, in collaboration with actors and stakeholders with diverse roles in asset security management, Ground Segment (GS) operations and First Responder teams. The work carried out towards the achievement of the KPIs can be summarised as follows:

- A series of focus groups, bilateral interviews and site visits at the premises of the Pilot Leaders were organised in M2-M3, to ensure that the use cases are closely mapped to the operational context of the aforementioned organizations (who are the primary End Users of the 7SHIELD Key Results) and that the designed scenarios describe realistic situations and real needs in terms of cyber-physical protection. Five (5) main focus groups were organized (one by each Pilot Leader), complemented by several follow-up bilateral discussions and additional mini focus groups. Indicative roles of the GS professionals and First Responders that participated in the focus groups include: Facility Manager, Ground Segment Technical Coordinator, Cyber-security Engineer, System Administrator, DevOps Engineer, Copernicus Cloud Solution Architect, ONDA DIAS Cyber-security Responsible, ONDA DIAS Service Manager, ICE Cubes Operator, Critical Infrastructure Security Expert.
- A total of 19 use case scenarios (11 cyber-attacks, 3 physical attacks, 4 combined cyber-physical attacks, and 1 natural disaster scenario) were designed by the Pilot Leaders for the first version of the Pilot Use Cases, covering all macro-stages of crisis management. The scenarios were designed taking into account the situational factors increasing the risk of natural disasters and man-made attacks, the vulnerabilities of the Ground Segments, the history of past cyber- and physical attacks, the frequency of attacks, the severity of cascading effects and the recommendations by First Responders.
- A total of 16 questionnaires were completed by GS professionals of the Pilot Leaders and Critical Infrastructure Protection experts from the First Responder organizations, during the requirements elicitation activities. The respondents included Ground Station Duty Operator, Software Engineer, Ground Station Manager, Ground Segment Engineer, Telecommunication Systems Engineer, Security Expert, Cybercrime Expert, CIP Expert - National Contact Point for EPCIP, Security Manager, Infrastructure Security Responsible, and GS Service Manager.
- A total of 250 user requirements (103 functional and 147 non-functional) were collected during the stakeholder's engagement and requirements elicitation activities. The first version that guided the technical developments of the first prototype included scenario-based, performance, reliability, connectivity, expandability, usability, documentation, localization, security, ethical and safety requirements.
- A two-day User Requirements Workshop was organized with the participation of all Pilot Leaders, Key Result owners, technical partners responsible for the development of the 7SHIELD modules and First Responders of the consortium, to refine and finalize the user requirements. In addition, the Pilot Leaders revised their respective use case scenarios, taking into account the developments and available functionalities of the Key Results and

the updated needs of the Ground Segments. The second and final version of the use cases and requirements was released in M16.

Summarizing, KPI is fully achieved 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).

UA1.2 – in the reporting period, the identification of general security and privacy by design requirements in order to limit the risks of data breach, and to secure data exchange and storage procedures was accomplished. At the beginning of the project a literature review regarding the general security requirements and the privacy by design principles was conducted, that supported the identification of security requirements. The identified general security requirements and the interpretation of the general privacy by design principles into requirements were provided as input to tasks T2.2 and T6.1 and they were further translated into system requirements (M6). The analysis of the legal, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers must satisfy were analysed. Indicatively, the ISO 27001, 27002, 27005, 27035, the OWASP Application Security Verification Standard (ASVS) Project, the NIST, and NIS directive were considered. The produced consolidated list of the security requirements is further refined based on the use cases' deployment and operational tests and the 7SHIELD systems functionalities. The KPI 1.2.1 achievement during the reporting period was around 55%. It will be 100% completed with the advancement of the demos and operational tests scheduled within the project.

UA1.3 – this UA analysed, from EU and national perspectives, the relevant legislation relating to 7SHIELD, the legal and ethical safeguards required for each of the 7SHIELD technological solutions and the main considerations for operational deployment in relation to the piloting counties. In terms of KPI achievement, the deliverable D2.3 – Preliminary ethics and legal framework (M8) reviewed the research and envisaged operational system from a legal and ethical perspective highlighting significant legislation and protocols. Therefore, it is only partially achieved (25%). Further legal, ethical and data protection impact assessments will be carried out to assess the compliance level until M24

User-oriented Objectives	User-oriented Activities	KPIs
UO2. Pilot design, implementation and evaluation	**UA2.1** Development of the validation scenario and evaluation methodology	**KPI 2.1.1:** Evaluation metrics, User satisfaction metrics, user feedback, system usability metrics.
	UA2.2 Field demonstrations, testing and training	**KPI 2.2.1**: User satisfaction metrics, user feedback, system usability metrics.

Achievements

UA2.1 – the main achievements of the reporting period were the development of the common evaluation methodology, provided by NOA for all Pilot Use Cases, and the definition of the validation scenarios, evaluation metrics and KPIs for the operational tests of SERCO (PUC5) and SPACEAPPS (PUC4). The evaluation methodology was designed to capture the performance and usability of the KR modules, as well as the user satisfaction and feedback. Specifically, the evaluation document described the pilot validation scenarios in distinct steps, including a brief description of the expected result for each performed action, in order to be able to compare it with the actual result and monitor deviations during the test execution. The KRs demonstrated in the scenarios were then evaluated based on a) the KPIs and target values set for each pilot, and

b) the fulfilment of KR-related Acceptance Criteria (as defined in D2.2). The KRs were then reported by the user as accepted or not accepted depending on the deviations. The evaluation methodology included KPIs defined in the Grant Agreement for each KR. Finally, the user was asked to provide feedback for each KR in terms of user interfaces and user friendliness, adaptability and compatibility and overall feedback on the 7SHIELD prevention, detection, response and mitigation technologies.
The KPI 2.1.1 was 100% achieved. The pilot validation scenario and evaluation methodology include detailed steps of the scenarios to be simulated for the testing the 7SHIELD modules, evaluation metrics for each tested module, user-defined Acceptance Criteria, user-defined KPIs and target values where applicable, evaluation against DoA-defined KPIs, and user feedback on system usability.

UA2.2 – During the reporting period, the first two (four in total) Operational Tests of the 7SHIELD first prototype were conducted, following the evaluation methodology of UA2.1. The operational tests were performed on the PUC5 (ONDA DIAS) and on the PUC4 (ICE Cubes Service), following cyber-attack scenarios in realistic and heterogeneous operational environments.
Before each operational tests, 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 Tests, an evaluation of the 7SHIELD first prototype 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 first two operation tests of PUC5 and PUC4 is available in the report D7.1.
As a short summary, the evaluation results show the following figures:

- More than 95% of the KPIs were effectively tested and fulfilled. Only one KPI was tested and partially fulfilled due to limitations in the graphical resolution of the user PC used in the remote test execution.
- Two thirds of the Acceptance Criteria related to Key Results were effectively tested and all of them were fulfilled.
- One third of the KPIs were effectively tested and all of them were fulfilled.
- 45% of the pilot related Acceptance Criteria were effectively tested and fulfilled. Only one Acceptance Criteria was tested and partially fulfilled as the mitigation of DoD cyber-attack required user intervention. The associated user requirement will be reassessed.
- Feedback from users were positive, with a few suggestions for improvements.

Written and descriptive user feedback on KRs was converted to a subjective Likert scale values 1-5 that corresponds very unsatisfied, unsatisfied, neutral, satisfied and very satisfied, respectively. The analysis was made for each KR in three categories that were tested in pilots (PUC4 and PUC5) and the results are shown in a table below. The preliminary and first-hand analysis together with written user feedback provide KR owners valuable information where to focus before upcoming pilots.

Category	PUC4	PUC5	Overall
UI and user friendliness	3.67	3.00	3.33
Adaptability	2.33	2.29	2.31
Compatibility	3.56	3.83	3.69
Combined	3.19	3.04	3.11

The main work of this activity will be done during the second reporting period when two more operational tests will take place as well as three demonstrations where the complete system will be demonstrated and evaluated.
After two first pilots (in SERCO and SPACEAPSS), the KPI 2.2.1 is partially covered. The average user-satisfaction rate is about 90%, while the completion rate is 25 % when giving more weight to the incoming operation pilots and demo pilots .

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 first project period to support the communication of the project were as summarised as follows:

- establishment of the 7SHIELD visual identity,
- design of the project brochure and infoboard,
- development of the project's website and setup of a 7SHIELD LinkedIn page,
- preparation of the 1st newsletter issue,
- appearances in third-party media and posts of project news on the 7SHIELD website and LinkedIn.

During the first 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. As a result, the KPI 1.1.1 has been partially achieved (50%). It will be fully achieved during the second period.
In the same period, 7SHIELD consortium carried out the following dissemination activities:

- 4 publications
- participation in 12 conferences including Big Data from Space 2021, 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021), Leveraging EU infrastructure in Europe, and ESA's Phi-Week 2021.

In addition, for the next reporting period, SERCO is currently preparing an infoday, to be organised on Q4 2022 – Q1 2023. Non-project partners will be invited (relying on networks already established as well as new contacts to be collected in the future events). 7SHIELD is consolidating the relationships with other EU projects emphasizing the complementarity and the value added brought by the project outcomes. 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/)

We further consolidate the network by participating to events with the presence of major actors in the field of Cyber and Physical threats on critical Infrastructures. Our objective is to bring evidence of 7SHIELD's results to representatives of these institutions:

- ENISA
- Law Enforcement Agencies,
- Interpol and European Defense Agency
- DG Connect
- Critical infrastructure community

IMA1.2 – the 7SHIELD consortium, becaming a member of the European Cluster for Securing Critical Infrastructures (ECSCI – https://www.finsec-project.eu/ecsci) has partially achieved (50%) the KPI 1.1.2, starting 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. For the next reporting period, 7SHIELD will participate to the 2nd EU-HYBNET Annual Workshop (https://euhybnet.eu/) and the 2nd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop, consolidating the network with (in priority but not limited to) SU-INFRA-01 projects (e.g. DEFENDER, PRAETORIAN, INFRASTRESS, SATIE, SECUREGAS, PRECINCT and so forth). The fulfilment of KPI 1.1.2 will be achieved in the second perid.

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 – A first version of the Market Analysis report was produced and submitted.
The work performed focused on identifying the main market and technology trends of both the Critical infrastructure security and the Space sector. It brings insights to the partners for future developments to accelerate the access of the 7SHIELD framework to the Space market.
KPI 2.2.1 progress:
2 Operational Tests of the 7SHIELD framework were performed on SERCO's and Space Applications Services' infrastructures. 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).

IMA2.2 – The proposed and deployed cyber-physical security systems were very heterogeneous depending on the operator's maturity in cyber and physical security. In this heterogeneous context, the 7SHIELD partners identified and described in the Exploitation Plan their results (as demonstrated in the two operational tests), underlining the main features and the value of each result in order to take into account the options that the operators considered as valid and feasible for the future commercial exploitation.
To this end, the initial version of the Exploitation Plan for each 7SHIELD result was identified, along with the exploitation possibilities and a preliminary joint exploitation strategy which will be further elaborated towards the second version of the deliverable. A draft Exploitation Plan was defined and implemented in order to multiply the impact of the potential solutions that may arise from the 7SHIELD project and to prepare the transition towards commercial uptake to fully

achieve the expected impact. The Exploitation Plan describes the activities to be undertaken in order to ensure the exploitation beyond the project itself. Moreover, the Consortium forges as many partnerships as possible, in order to obtain the maximum exploitation of the Results. To strengthen the exploitation potential, 7SHIELD expects the development of joint exploitation strategies by groups of partners that can mutually benefit from a cooperative scheme and two main joint exploitation schemas were provided, and all the exploitation aspects were analysed for the joint results. The two joint exploitation schemas are the following:

- UAVs with on-board computer vision (ACCELI, CERTH) covering physical attack scenarios.
- Cyber risk assessment and cascading effects (ENG, RESIL, STWS) covering cyber-attack scenarios.

The collected information will be reviewed and further integrated throughout the project lifecycle as well as the number of exploitable results and joint exploitation schemas. As a result, another joint exploitation schema covering the combined cyber and physical threats will be added in the second period. In particular, this will be a portable integrated solution for quick insertion into the space industry. To this end, during the reporting period, 7SHIELD has strengthened the cooperation with other H2020 INFRA projects operating in the Critical Infrastructure domain, via a cross-projects collaboration and innovation, creating synergies within the ECSCI cluster, where 7SHIELD is a member. In order to maximise the collaboration and achieve KPI 2.2.1, partners decided to join their forces to demonstrate the 7SHIELD results might be migrated in other external installations to compare and evaluate the impact and value in other contexts. As result, KPI 2.2.1 will be achieved in the second period.

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 – This 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

Activities are organised to reach the end goal of having a strategy that aligns the innovations delivered by 7SHIELD and promote them to organisations procuring EU Ground Segments of Space Systems and inform policy-making communities to initiate discussions that could lead to future adoption of standards and policies.

7SHIELD partners have participated to 14 events and approached individually organisations reaching several hundred people.
The following communities were reached:

1. Space agencies

2. Satellite owners
3. Ground Station operators
4. Cyber-security experts
5. Policy making communities

In the 1st period, EETT initially identified the relevant specialized policy-making communities, namely ENISA and the ENISA ECASEC Expert Group, proceeding also in initial contacts and preparatory actions/negotiations for raising awareness about the project and its objectives. As a result of this and following the development of project results and 1st pilots run, a participation of 7SHIELD in ENISA's and ECASEC's events is under consideration to take place in the beginning of the 2nd project period, i.e. in the next ENISA-ECASEC meeting and in the ENISA Telecom Security Forum (to be confirmed) on the 28th and the 29th of June 2022, respectively, in Brussels. It is worth mentioning that EETT is the national regulatory authority in Greece that regulates and monitors electronic communications networks among others and as such is in close cooperation with similar EU authorities.

IMA3.2 – Standardisation work commenced contacting stakeholders responsible for procurement of Ground Segments with the objective to understand how they view an initiative such as 7SHIELD and to understand how policy and standards with respect to cyber security in their organisations is likely to change in the coming years. The following meetings were held:

- Several meetings with ESA/ESOC and the director at ESA responsible for security across all directorates at ESA.
- A presentation of current Critical Infrastructure Policies was made to the 7SHIELD Advisory Board during the Plenary meeting on 4 February 2021.
- An internal workshop was held to obtain a common understanding across the project of a policy, standards and potential recommendations.
- A meeting with Jean-Luc Trullemans, responsible for strategy at ESA Security Office - DG-5X was held in October 2021.

Focus was given to ESA for two reasons. Firstly, ESA is the major stakeholder both in terms of procurement and of operation of critical space ground infrastructure. Secondly, ESA is moving to a centralized policy and strategy for security with establishment of ESA's European Space Security and Education Centre, at Redu in Belgium as a centre of excellence for space cyber security services and the creation of the DG-5X responsible for security policy across ESA.

Actions for IMA3.2 are on track and KPI 3.2.1 is not yet achieved. For the 2nd period activities will be undertaken to:

1. Review the Security Requirements established in 7SHIELD investigating how the requirements have been implemented. Major input to this review are documents D2.2 (Consolidation of Stakeholder Requirements) and D2.5 (Security Requirements report).
2. Continue talks with ESA
3. Extend meetings to Ground Station operators and Policy-making communities;
4. Create awareness of 7SHIELD policy aspects through organisations such as EARSC (European Association of Remote Sensing Companies) members of which operate space ground infrastructure who are not members of the 7SHIELD consortium. Other organistions include BDVA (Big Data Value Association) where platforms such as ONDA operated by SERCO are relevant systems for the BDVA. We will approach BDVA Task Force TF7-SG13: Security where ENG is a task force lead;
5. In addition, a dedicated Policy and Strategy workshop is planned before the summer recess to collect project inputs on policy and strategy, communicate to stakeholders and identify steps to promote standardisation actions.

Points 1 and 5 will provide the starting point for creating the draft version of the deliverable D8.12 7SHIELD Security Standardisation Stratey and Policy-planning.

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

The work done in the first period, from M1 (September 2020) to M16 (December 2021) was devoted to the preparation of a **user requirements survey** and to the collection of **functional and non-functional requirements** for each Pilot Use Case (PUC). A preliminary list of functional and non-functional user requirements was provided and discussed and reviewed with technical partners. Moreover, the use case scenarios were also revised for all the PUCs, to provide input for the validation scenario and evaluation methodology of *T7.1 – Development of the validation scenario and evaluation methodology.*

Regarding the **security requirements**, the General Security by Design Principles to be adopted for the needs of the 7SHIELD were identified. A questionnaire, based on the threat modelling tool was prepared to collect information on the vulnerabilities per each PUC and based on the collected information the security requirements for each PUC will be further refined. The **general privacy by design and security requirements** were identified.

In the context of **ethics and legal framework**, pilot partner questionnaires relating to national legislations, and review and synthesis of EU legislation with regard to the space sector and critical infrastructure were gathered. A thorough review of legislation relating to data protection, critical infrastructure protection and cyber security placing them into the context of 7SHIELD and its goals and objectives was accomplished. Furthermore, a comprehensive review and analysis of the legal, ethical and societal considerations for each of the individual technologies proposed to be deployed within 7SHIELD, including the application of trustworthy AI was accomplished.

Regarding the 7SHIELD **pre-crisis and prevention technologies**, during the reporting period, the **risk assessment methodology** was defined. The core of this methodology relies on the definition of the threats and assets taxonomies and the way these taxonomies are used by the impact and risk assessment models. Furthermore, the role of the risk assessment components was clearly defined, and the integration of the components were designed and implemented. Several risk assessment functionalities related to the cyber threats were demonstrated and evaluated in the first two PUCs, namely PC4 (SPACEAPPS) and PC5 (SERCO).

During the reporting period, the analysis of the user requirements for **Threat Intelligence** (TI) was performed and the logical architecture of the prototype and the preliminary interfaces of the services were defined. The activity on **Cyber and Physical Threat Intelligence** was focused on state-of-the-art analysis of threat intelligence platforms, search for data sources of possible threats, internal architecture and first overview of threat

intelligence algorithms to be used in the service. In addition, during the reporting period, the 1st User Feedback Meeting was carried out aiming to demonstrate WP4's key technical solutions to 7SHIELD end-users. Furthermore, continuous updates with all the partners were done to better design the role of the TI service inside the different pilots. All the activities were completed successfully, and the results were shown during the pilot demonstrations.

The **design of 7SHIELD mission UAV** (included the mechanical, electronical and flight subsystems), considering the different parameters (physical and operational) from PUC1, PUC2 and PUC3 were defined. The 7SHIELD UAV 1st prototype was developed: connection of camera with embedded GPU (survey for available industrial interfaces) and configurations were setup as well as configuration and deployment of AI algorithms for object detection & identification.

Activities concerning the data collection, the experimental evaluation of **Face Detection and Recognition models' state-of-the-art**, the development of the Face Detection and Recognition framework for offline inference and its link with the criminal database were conducted. Questionnaires to end users to collect data about the PUCs were prepared. Furthermore, experimental evaluations of innovative Face Detection and Recognition models were launched. Moreover, a first draft of Face Detection and Recognition UAF message was created and the deployment of joint Face Detection and Recognition pipeline was realised.

The development of **Face Detection and Recognition** (FDR) module was completed. A new activity regarding the speed up of face detection was initiated. The integration of facial tracking into the next Face Detection and Recognition version was initiated.

The Video-based Object Detection (VOD) module encompasses activities related to the determination and clarification of objects of interest, the definition of suspicious and harmful human activities, and the assessment of available dataset for **object detection** were conducted. Moreover, a newer version of the object of interest for the object detection taking into account the initial PUC requirements from the users was redefined. The collection of available public datasets was completed. Research for relevant public datasets for activity recognition was carried out. Furthermore, based on the user requirements and the PUCs some of the possible crucial actions the service should recognize were identified. The activity concerning the examination of the available datasets for object detection has been completed. Furthermore, an initial **Activity Recognition** (AR) module for recognizing motion of persons as action implemented was developed.

In the reporting period, 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. Furthermore, the specification of system requirements for the **Cyber-attack Detection framework** was improved and linked with user requirements. Appropriate datasets were chosen to verify the detection features provided by the cyber-attack

detection layer and the cyber-attack correlation solution. The chosen datasets were analysed in order to prepare validation of the detection rules for cyber-attacks. The Cyber-attack Detection methods, including new monitoring rules, were successfully tested during the Pilot Use Case 4 and Pilot Use Case 5 trials. The framework was improved including a malware scanner, the IP geolocation of threat sources and improving reporting features. Dashboards were adapted for each use case scenario.

In the reporting period, activities related to the study, definition, selection and purchasing of the **Infrared (IR) and thermal sensors**, the development of thermal and **Near Infrared (NIR) sensor interface and networking** as well as the elaboration of techniques for detection of man-made attacks from thermal and IR data were carried out. Moreover, the development and test of the user interface for the MMAS operator, namely user functionalities related to visualization of video streaming, positioning of the camera, zooming and setting of alarms and warnings were performed. The techniques for detection of man-made attacks based on thermal cameras, namely detection of movements detection, classification and detection based on the level of heat were developed.

During the reporting period, upgradation work on PLS v3.0, LFS v3.0 and 3D MND v3.0 was progressed in terms of hardware and software. For PLS and LFS, a series of tests were carried out for sensitivity depending upon size and reflectivity of the object. Regarding 3D MND, false Alarm Rate (FAR) was tested with different sensitivity thresholds and APD gains, and optimum solution was determined.

The definition of the UAF message format that will be used to describe **physical, cyber and combined security alerts** was finalized. The Geospatial Complex Event Processor (G-CEP) component was enhanced in order to support the receiving and correlation of the events that will be detected by the physical sensors. The G-CEP component supports the correlation of the events that are detected by the physical sensors on the field.

The SPGU module was developed. Integration of data produced by other 7SHIELD tools in the Situational Picture and how data included in the Situational Picture can be exploited was discussed.

Regarding the **Post-Crisis management for response and mitigation** of physical and cyber threats of 7SHIELD, the connectivity process of the 7SHIELD Knowledge Base through the Apache Kafka was finalized. Moreover, during the last period, the Knowledge Base (mapping service JSON to RDF converter) module was updated to be compatible with the SPGU inputs. Updates were made to the 7SHIELD ontology and classes from the Situational Awareness Data Model were imported. The first FRSS's architecture and the definition of the hardware wearables were performed, as well as the acquisition of the equipment. The acquisition and implementation of the sensor network was made and the first integration of the wearables and the logical interconnection between the team leader and the team members was performed. Development of communication modules and tests with the

7SHIELD core via a Kafka Broker, using encryption and authentication methods. Update the FRSS architecture with inputs from user requirements and system integration.

The design of the **Crisis Classification scenario for annotation tool** was finalised. Using the annotation tool, the end users are able to characterise the scenarios according to the severity they would present to the pilot.

A thorough **review of the relevant international standards and guidelines**, in order to identify basic concepts for the establishment of a model Emergency Response Plan was accomplished. Moreover, a questionnaire is being developed for the creation of the pool of local security regulatory frameworks, best practices and procedures from pilot site stakeholders. This module was successfully demonstrated in the first two pilots (PUC5 and PUC4) so far. These lists of procedures were also pictured as flowcharts with the use of Visio, to provide an easy way for the operator to visualise a specific emergency response process in a user-friendly manner.

A literature review on crisis communications, specific focus on Critical Infrastructure and key concepts, identification of relevant social media outlets / accounts / groups for analysis and reviewing potential case studies / best practices communication guidelines was carried out. Several cases studies were identified to analyse the effectiveness of communication via social media in raising awareness of citizens and a literature review on crisis communications focus on the critical infrastructure sector was also undertaken.

A review of **service continuity standards and practices** was undertaken regarding telecommunication operators. Contacts with relevant users were done. The service continuity scenarios were finalised for the first pilot (PUC5). A generalized model of cyber-physical operations was developed so as to assess the existing vulnerabilities identified and plan for risk mitigation.

Regarding the **System Integration**, the initial work was aimed at defining how to integrate all the components developed in WP3, WP4, and WP5. The testing will allow checking the compliance of the components with their specifications, as defined in Task 2.2 and with the overall system architecture, as described in Task 6.1. The 7SHIELD design and specification was extensively discussed up to the definition of the **7SHIELD Architecture**. Since the 7SHIELD project is based on event-driven architecture, communication between the components is performed over a message broker. The set of rules and patterns of message structure was defined (e.g., topic naming, message type and naming, messaging patterns, component status validation mechanism) to make data exchange and integration between components more structured, organized, and successful. Thus, the system-level consequences of any disruptive event are quantified, enabling the accurate assessment of the resulting disruption and the rating of subsequent service continuity strategies to mitigate the damage. The modelling of pilot systems was carried on, analysing vulnerabilities and weaknesses, and identifying security solutions to mitigate the risks.

An initial version of the **7SHIELD User Interface (UI)** was designed and implemented according to the user requirements, objectives of the project and the type of the information that has to be presented to the users/operators of the platform.

Finalization of the **validation scenarios and evaluation methodology** for the operational test of the first and second pilot (PUC5 and PUC4), including definition of evaluation metrics and Key Performance Indicators for the demonstrated Key Results. Preparation of the validation scenarios for the operational test of the third pilot (PUC3), to be executed in March 2022. 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 will be prepared for all the pilot sites and provides 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 PUC5 and PUC4 end-users to get familiar with the technologies and the details of the 7SHIELD system. The first two pilots were executed successfully and the 1st prototype evaluation report was prepared based on validation and evaluation reports from PUC5 and PUC4.

The **communication and dissemination activities** during the reporting period were successfully conducted. In the context of WP8, the communication and dissemination plan's activities were implemented, monitoring the communication and dissemination actions executed by partners and drafting of communication and dissemination handbook. Delivery of the 7SHIELD brochure, collection of feedback from all partners and finalisation of brochure. The first version of the market analysis was finalised and submitted. Based on the competitiveness landscape analysis and market analysis, a detailed business plan was established. One of the main results of this task has been the first version of the "**Exploitation plan and Intellectual Property Report**". It represents a key result for assuring the future exploitation of the main reached results in the project. The 7SHIELD partners were identified and described their results underlining the main features and the value of each result in order to take into account the options that they consider valid and feasible for the future commercial exploitation.

The Support of The Horizon Result Booster was requested to help partners identify the most promising **Key Exploitable Results**. The **7SHIELD's Key Exploitable Results** (KERs) were presented and exploitation strategy detailed. A structured and in-depth analysis of the exploitable results was conducted in order to structure exploitation planning and ensure a sustainable exploitation. The **IPR theme** was also analysed. The IPR Management was focused on the careful handling of IPR issues in 7SHIELD project, that are of strategic importance in order to facilitate the exploitation of its solutions.

Regarding the **Standardisation Strategy**, work was commenced with contacting stakeholders responsible for procurement of ground segments with the objective to understand how they view an initiative such as 7SHIELD and to understand how policy and standards with respect to cyber security in their organisations is likely to change in the coming years. Work was spread over three aspects: 1) Staying abreast of the developments in the 7SHIELD project; 2) Following up with relevant organisations presenting 7SHIELD; 3) Keeping aware organisations and institutes actions.

3. Dissemination actions

During the project first 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

	Event Title	Type of Event	Event Dates	Location	Type of Participation	Presentation Title	Attendee
1	ESA Φ-Week 2020	Conference	1-Oct-20	Virtual	Speaker	ONDA Contribution to DTE	Franck Ranera (SERCO)
2	"Leveraging the EU infrastructures in Europe" Workshop	Workshop	19-Oct-20	Virtual	Speaker	General presentation of 7SHIELD project	Franck Ranera (SERCO)
3	Nicosia Risk Forum 2020	Conference	26-Nov-20	Virtual	Speaker	General presentation of 7SHIELD project	Gabriele Giunta ENG), Xavier Pothrat (CS)
4	H2020 – SOCIETAL CHALLENGE 7 "SECURE SOCIETIES" 2nd Project to Policy Kickoff Seminar	Conference	22/23-Mar-2021	Virtual	Speaker	7SHIELD Policy Brief presented	Gabriele Giunta (ENG)
5	Big Data from Space 2021	Conference	18/20-May-2021	Virtual	Speaker	ONDA DIAS: a Cloud-based platform to foster exploitation of geospatial information [mention of 7SHIELD]	Franck Ranera (SERCO)
6	Data Week 2021	Conference	25-27-May-2021	Virtual	Speaker	Presentation by ENG focused on AI and Big Data Analytics for Critical Infrastructure protection	Gabriele Giunta (ENG)

7	CPS4CIP 2021 Workshop	Workshop	8 Oct-2021	Virtual	Speaker	Severity level assessment from semantically fused video content analysis for physical threat detection in ground segments of space systems	Gerasimos Antzoulatos (CERTH)
8	ESA Φ-Week 2021	Conference	11/15-Oct-2021	Virtual	Poster	e-poster "ONDA: a Key Enabler for the New Space Economy" with mention of 7SHIELD	SERCO
9	BEYOND International Exhibition for Innovation and Technology	Exhibition	14/16-Oct-2021	Thessaloniki, Greece	Booth	General presentation of 7SHIELD project	Katerina Valouma, Dimitris Diagourtas, Antonis Kostaridis (STWS)
10	European Space Forum 2021	Conference	8/9-Nov-2021	Virtual	Booth	7SHIELD brochure + 7SHIELD general presentation shared at the Serco virtual booth	SERCO
11	Space Tech Expo I Europe	Conference	16/18-Nov-2021	Bremen, Germany	Booth	7SHIELD brochure shared at virtual booth	CS, SERCO
12	Industry Space Days	Conference	7/8-Dec-2021	Virtual	Speaker	General presentation of 7SHIELD project	Dimitrios Liaskos (HP), Nikolaidis Panagiotis (HP)

3.1.1. Scientific publications

- S. Andreadis, G. Antzoulatos, T. Mavropoulos, P. Giannakeris, G, Tzionis, N. Pantelidis, K. Ioannidis, A. Karakostas, I. Gialampoukidis, S. Vrochidis, I. Kompatsiaris. A social media analytics platform visualising the spread of COVID-19. Online Social Networks and Media [30/04/2021]

- D. Sykas, I. Papoutsis, D. Zografakis. Sen4AgriNet: A Harmonized Multi-Country, Multi-Temporal Benchmark Dataset for Agricultural Earth Observation Machine Learning Applications. IEEE International Geoscience and Remote Sensing Symposium IGARSS, July 11-16, 2021 [12.10.2021]
- G. Antzoulatos, G. Orfanidis, P. Giannakeris, G. Tzanetis, G. Kampilis-Stathopoulos, N. Kopalidis, I. Gialampoukidis, S. Vrochidis, I. Kompatsiaris. Severity level assessment from semantically fused video content analysis for physical threat detection in ground segments of space systems. ESORICS 2021 International Workshops, October 8, 2021.
- E. Schiavone, N. Nostro, F. Brancati. A MDE Tool for Security Risk Assessment of Enterprise.s Industrial Track of LADC 2021, the 10th Latin-American symposium on Dependable Computing, November 22-26, 2021 [22/11/2021]

3.2. Collaboration and networking activities

- 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021) [08/10/2021], 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.*
- EUSPA Space Conference (8-11/11/2021) - networking established with experts in Space Ground Segment

3.3. Hands-on plenary board meetings

- 1st Plenary Meeting [28-29/09/2020]
- 2nd Plenary meeting [03-04/02/2021]
- 3rd Plenary Meeting [22-23/06/202]
- 4th Plenary Meeting [03-04/11/2021]

3.4. Phone calls and virtual meetings

- Monthly TMC Telcos - Every month
- WP monthly Telcos - Every month
- Advisory Board kick-off meeting [04.02.2021]
- Teleconference on ESA Ground Segment security policy and standards with ESOC [18.02.2021]

- Threat Taxonomy Workshop - organized by RESIL. Speakers: KEMEA, STWS, RESIL, CERTH, CSNov [12.03.2021]
- Teleconference on ESA Ground Segment security policy and standards with DG-X, ESRIN [01.04.2021]
- 2nd Advisory Board meeting [25.06.2021]
- ONDA-DIAS User Training Workshop [30.09.2021]
- Various bilateral teleconference held by SERCO with partners (ENG, CeRICT, CSNov, RESIL, KEMEA, STWS) for definition of PUC5 scenarios during the period [07.2021 – 09.2021]
- ONDA-DIAS demonstration trials [13.10.2021, 15.10.2021, 22.10.2021]
- User Requirements Workshop [20-21.10.2021]
- ICE Cubes Services User Training Workshop [09.11.2021]
- ICE Cubes Services demonstration trials [15.11.2021, 17.11.2021, 19.11.2021]

3.5. Other important outcoming events

- 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]
- First demo of 7SHIELD tools on the Cyber-physical attack in the Ground Segment of NOA (Athens, Greece) [09.2022]
- First demo of 7SHIELD tools on the Physical attack in Arctic Space Centre of FMI (Sodankylä, Finland) [10.2022]
- First demo of 7SHIELD tools on the Threat detection and mitigation in the ICE Cubes Service of SPACEAPPS (Brussels) [11.2022]

4. Research ethics guidelines and recommendations

During the first 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 and future outlook

This document constitutes the first project progress report outlines the activities carried out by the project consortium during the following period: September 2020 (M1) - December 2021 (M16). As a result, in this document, an overview of the achieved 7SHIELD objectives and project's results in terms of scientific and technological outcomes was 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 was also reported with regard to the first period.

The 7SHIELD objectives and results achieved during the second period, namely January 2022 (M17) – February 2023 (M30), will be reported in *D1.5 – Public final activity report*, due at M30. Besides that, the final report will also report the impact achieved during the project lifecycle and the final data management plan.

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