7SHIELD

D1.4 Self-assessment & data management plan v2

Work Package:	WP1		
Lead partner:	ENG		
Author(s):	Gabriele Giunta (ENG), Emilia Gugliandolo (ENG), Irene Bicchierai (RESIL), Francesco Brancati (RESIL), Gerasimos Antzoulatos (CERTH), Ilias Gialampoukidis (CERTH), Vinod Ahuja (DFSL), Ilias Gkotsis (KEMEA), Galatea Kapellakou (KEMEA), Pantelis Velanas (ACCELI), Luigi Coppolino (CeRICT), Thomas Andrejak (CSNov), Dorothy Kim Chi Tran (CSNov), Paulo Chaves (INOV), Helen Gibson (CENTRIC), Leonidas Perlepes (STWS), Dimitris Vamvatsikos (RG), Souzana Touloumtzi (NOA), Xavier Pothrat (CS), Mathieu Schmitt (SPACEAPPS), Leslie Gale (SPACEAPPS)		
Due date:	M24		
Version number:	1.0	**Status:**	Final
Dissemination level:	Public		

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

Horizon 2020
European Union Funding
for Research & Innovation

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

Revision History

Revision	Date	Who	Description
0.1	04/07/2022	ENG	First release of the template
0.2	21/07/2022	ENG	First contribution
0.3	05/08/2022	ENG, CERTH, NOA, RESIL	Assessing plan of the project objectives
0.4	24/08/2022	ACCELI, CENTRIC, CERTH, CS, CSNov, DFSL, ENG, INOV, NOA, STWS, KEMEA	Integration of contributions - Dataset collection - Executive summary - Introduction and - Conclusion
0.5	01/09/2022	ENG, NOA, SPACEAPPS	Integration of new contributions and updates in WP7 table Version ready for peer review
0.6	14/09/2022	CERTH, INOV, NOA	Feedback after peer review
1.0	16/09/2022	ENG	Final version after internal peer review

Quality Control

Role	Date	Who	Approved/Comment
Internal reviewer	*14/09/2022*	INOV	Document accepted, only minor changes suggested
Internal reviewer	*14/09/2022*	*NOA*	Document accepted, only minor changes suggested
Internal reviewer	*14/09/2022*	*CERTH*	Document accepted, only minor changes suggested

Disclaimer

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

Executive Summary

The project addresses the challenges associated with the security and resilience of EU Ground Segments of Space Systems. Today, the ground segments of space systems receive massive amounts of satellite data. A physical/cyber-attack to their installations or communication networks, respectively, would cause debilitating impact on the distribution of satellite data and in its data storage, access and exchange affects not only the reliability of space data, but also their FAIR standards: findability, accessibility, interoperability and reusability. To reach this goal, the project makes use of advanced technologies for data integration, processing, analytics and visualisation as well as data security and cyberthreat protection to assess the prevention, detection and mitigation of threats, both physical and cyber. Moreover, running of the project requires the collection and generation of data to achieve the main project objectives and to directly support the technical development of 7SHIELD tools or the development of operational processes. This data is required to manage the project, disseminate the information about it, analyse and exploit its results. Moreover, the technology-oriented WPs will process both open and closed source data. Collecting and generating of the mentioned data requires compliance with data management strategies suggested by the EC. In accordance with the guidelines on data management in Horizon 2020, a data management plan is required to monitor the collected/generated data with respect to their privacy and confidentiality, ensure that the legal and potential ethical standards for data generation, use, storage and share are applied throughout the project.

This deliverable is the final version of the Self-assessment & Data Management Plan (DMP) of the 7SHIELD project. It represents a short, general outline of the evolution of project requirements and objectives and an updated data management report describing the project policy for data management. The described policy reflects the current state of consortium agreements regarding data management and is consistent with those referring to the exploitation and protection of results. The 7SHIELD Data Management Plan (DMP) has the objective to detail specifics of data which have already been collected/generated (or are foreseen to be collected/generated) during the lifespan of the project. In particular, it includes a summary of the data and how they will be FAIR (i.e., Findable, Accessible, Interoperable, and Re-usable) based on the "Guidelines on FAIR Data Management in Horizon 2020". The overall purpose of the DMP is to support the data management life cycle for all data that will be collected, processed or generated by the project.

The DMP is a living document which will be kept updated during the whole lifetime of the project, since data generation and collection, and therefore data management, will be active in 7SHIELD for a considerable time after the submission of the initial version of the Data Management Plan. The datasets may also be altered due to converging factors, such as project maturity, shifts in consumer usage, legislative changes, etc. DMP is a document that can evolve along the project and D1.4 Self-assessment & data management plan v2

represents the updated and final version (M24). The updates provide information related to the objectives' achievements and implemented activities to reach the objectives and include new sets of data and changes in consortium policies and datasets management.

Table of Contents

List of figures

List of Tables

Definitions and acronyms

AUC	Area Under Curve
C2	Command and Control
CA	Consortium Agreement
CAP	Common Alerting Protocol
CAPEC	Common Attack Pattern Enumeration and Classification
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
COCO	Common Object in Context
COTS	Common-off-the-shelf
C/P	Cyber/Physical
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versions System
CWE	Common Weakness Enumeration
DB	Database
DMP	Data Management Plan
DoA	Description of Action
EC	European Commission
ECSCI	European Cluster for Securing Critical Infrastructures
EDXL	Emergency Data Exchange Language
EU	European Union
EUCI	EU-classified information
FAIR	Findable, Accessible, Interoperable and Re-usable
FAQ	Frequently Asked Questions
FLIR	Forward Looking InfraRed
FOAF	Friend of a friend
FPR	False Positive Rate
FPS	Frames Per Seconds
GA	Grant Agreement
GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
IA	Innovation Activity
IMA	Impact-making Activity
IMO	Impact-making Objective
IO	Innovation Objective
IP	Intellectual Property
IPR	intellectual property rights
IVUL	Image and Video Understanding Lab
JSON	JavaScript Object Notation

KAUST	King Abdullah University of Science and Technology
NIR	Near-Infrared
NVD	National Vulnerability Database
OGC	Open Geospatial Consortium
ORD	Open Research Data Pilot
OWL	Web Ontology Language
PC	Project Coordinator
PCAP	Packet Capture
PDF	Portable Document Format
SC	Scientific Coordinator
SGS	Satellite Ground Station
SOSA	Sensor, Observation, Sample, and Actuator
SPGU	Situational Picture Generation and Update
SSN	Semantic Sensor Network
TM	Technical Manager
TPR	True Positive Rate
UA	User-oriented activity
UAF	Unified Alert Format
UAV	Unmanned Aerial Vehicle
UCF	University of Central Florida
UO	User-oriented Objective
VOC	Visual Object Classes
VPN	Virtual Private Network
WP	Work Package
XML	eXtensible Markup Language

1. Introduction

This deliverable is the second and final version of the Self-assessment & Data Management Plan (DMP) for the 7SHIELD project. It represents a short, general outline of the evolution of project requirements and objectives and an updated data management report describing the project policy for data management. DMP can evolve along the project and D1.4 – Self-assessment & data management plan v2 (M24) contains some updates. The updates provide information related to the objectives' achievements and implemented activities to reach the objectives and include new datasets and changes in consortium policies and datasets management.

It is fundamental to report the project achievements in terms of objectives realisation underlining all thee implemented activities carried out to reach the aforementioned objectives. A revised assessment plan, based on the experience gained until M24, and the monitoring of the evolution of project requirements and objectives along with the implementation of the plan and activities per objective have been reported.

Data of different nature will be collected, processed, and generated during the lifetime of the 7SHIELD project. Some of these data might contain personal information and thus require a clear data management plan on how they are to be handled, i.e., stored, processed, accessed, and protected against unauthorised or improper use, etc. The first version of this deliverable is submitted on the sixth month of the project follows the template provided by the European Commission[1]. In particular, this report provides an analysis of the main elements of the data management policy that will be used by the Consortium with regard to all the datasets that will be generated by the project, describing rules, best practices and standards that will be used with regard to the datasets preparation, cleansing and processing, including data analysis and analytics. The deliverable includes information related to accessibility, intelligibility, usability and interoperability of the data gathered and takes into account privacy and security aspects.

1.1. Purpose of the document

The overall purpose of the Self-assessment and Data Management Plan is to report the project achievements in terms of objectives realisation and to support the data management life cycle for all data that will be collected, processed or generated by the project. It will contribute to the management of the project through the following steps:

- Report the project achievements in terms of objectives realisation underlining all the implemented activities carried out to reach the aforementioned objectives.

[1] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

- A revised assessment plan, based on the experience gained until M24, and the monitoring of the evolution of project requirements and objectives along with the implementation of the plan and activities per objective have been reported.
- Outline the types of data collected and generated (or foreseen for collection and generation) during the course of the 7SHIELD project.
- Describe the methodology and standards required, but also identify whether and how data will be collected, shared, exploited, re-used or made accessible for verification, and how they will be curated and preserved.
- Specify the degree of privacy and confidentiality of the collected/generated data.
- Outline the considerations and measures that are foreseen for the adequate management of the data from the legal, ethical, and security points of view.
- Outline the main elements of the data management policy that will be followed by the 7SHIELD consortium to handle collected/generated data with respect to their sensitiveness during and after the project.
- Ensure project research data and records are accurate, complete, authentic, interoperable and reliable.
- Enhance data security and thereby minimize the risk of data loss.
- Ensure research integrity and reproducibility by others.

The described policy reflects the current state of consortium agreements regarding data management and is consistent with those referring to exploitation and protection of results.

1.2. Self-assessment & DMP Versioning and Data Repository

This Self-assessment & DMP provides the methodology which 7SHIELD has implemented to manage the data created within the project. This plan has been periodically reviewed and updated with contributions from 7SHIELD partners with the following schedule:

- Month M6 (version 1) – D1.2 Self-assessment & data management plan v1
- Month M24 (final version) – D1.4 Self-assessment & data management plan v2

The table below provides details of the changes that have been made to the initial version of the Self-assessment & Data Management Plan submitted at M6.

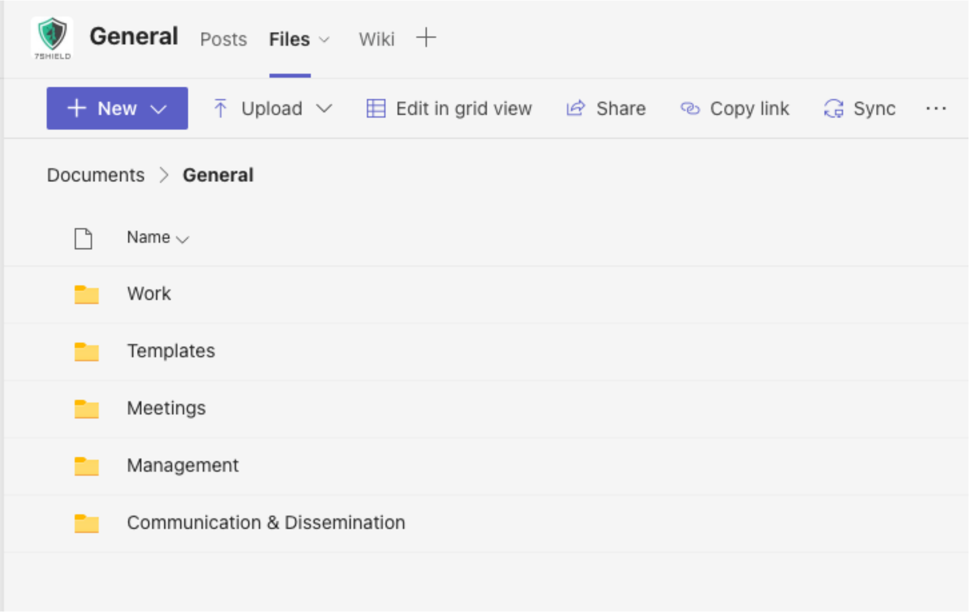
Section	Details
1.2 – Self-assessment & DMP Versioning and Data Repository	This section provides details of the changes that have been made to the initial version of the Data Management Plan submitted at M6 and the Data Repository Structure

2.4 – Project Objectives	In this section are listed the specific objectives and activities for the project as described in the DoA. The work carried out, during the 24 months, towards the achievement of each objective and the assessment of the progress in relation to the specific activities, considering also the expected KPIs, is described in detail.
3.2.2 – Data sources	Update of the data sources used in the project
4 – 7SHIELD Project Datasets	Update of the project datasets

The revisions of the Data Management Plan, along with related documentation and data sets (where applicable), are stored in the 7SHIELD document repository on MS Teams under the WP1 folder.

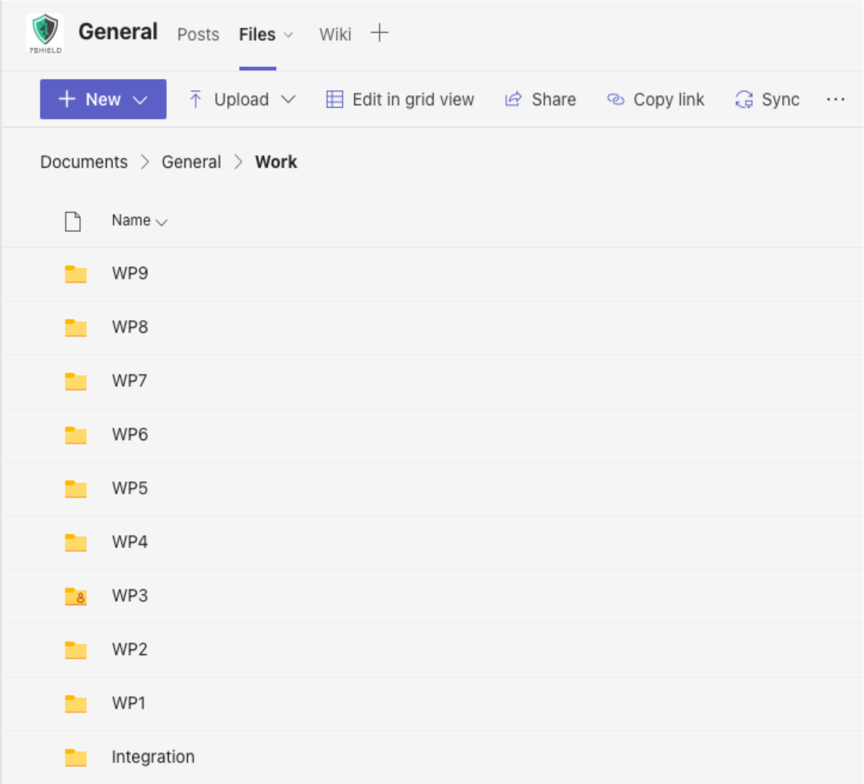
This MS Teams repository is structured as follows:

General



- Work
- Templates
- Meetings
- Management
- Communication & Dissemination

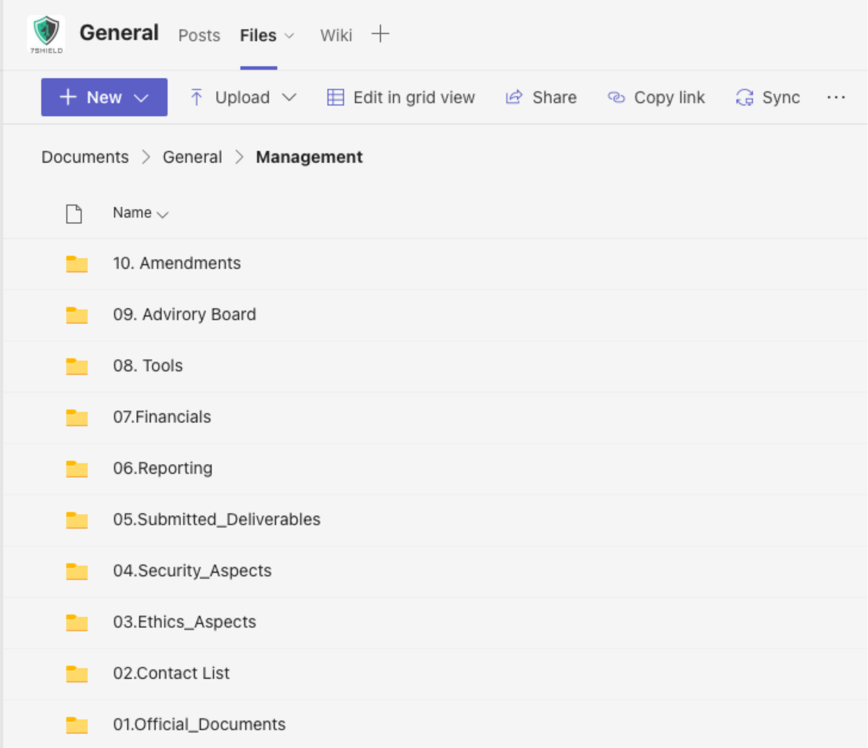
- Work



Documents > General > **Work**

- WP9
- WP8
- WP7
- WP6
- WP5
- WP4
- WP3
- WP2
- WP1
- Integration

- *Templates*
- *Meetings*
- Management



Documents > General > **Management**

- 10. Amendments
- 09. Advirory Board
- 08. Tools
- 07.Financials
- 06.Reporting
- 05.Submitted_Deliverables
- 04.Security_Aspects
- 03.Ethics_Aspects
- 02.Contact List
- 01.Official_Documents

- *Communication & Dissemination*

1.3. Structure of the document

This deliverable is structured as follows:

- Section 2 defines the assessing plan of the project objectives. The specific objectives for the project as described in section 1.1 of the DoA are listed and the work carried out towards the achievement of each listed objective has been assessed, considering also the expected KPIs and target value. Moreover, the activities carried out to reach the aforementioned objectives have been reported.
- Section 3 defines the data management structure to be followed during the 7SHIELD project according to the Guidelines on FAIR Data Management in Horizon 2020. Further updates are provided only in section 3.2.2 – Data sources.
- Section 4 describes the information about 7SHIELD datasets: 22 datasets have been identified.
- Section 5 presents IPR plan that focuses on the careful handling of IPR issues in 7SHIELD project. No further updates are provided in this final version.
- Section 6 presents the main conclusions and the references to the documentation sources used in this deliverable are included in the reference section.

2. Assessing Plan of the project objectives

7SHIELD addresses the security and resilience of EU Ground Segments of Space Systems, meeting the crosscutting and the sectoral criteria of the EU critical infrastructures (EC Directive 2008/114). The project aims at providing a holistic framework enabling the deployment of innovative services for cyber-physical protection of ground segments. The framework will enhance the infrastructures' protection capabilities, while integrating or interoperating with existing protection solutions already deployed. 7SHIELD resolves some Innovation, User-oriented and Impact-Making Objectives, as shown in the Figure 2-1.

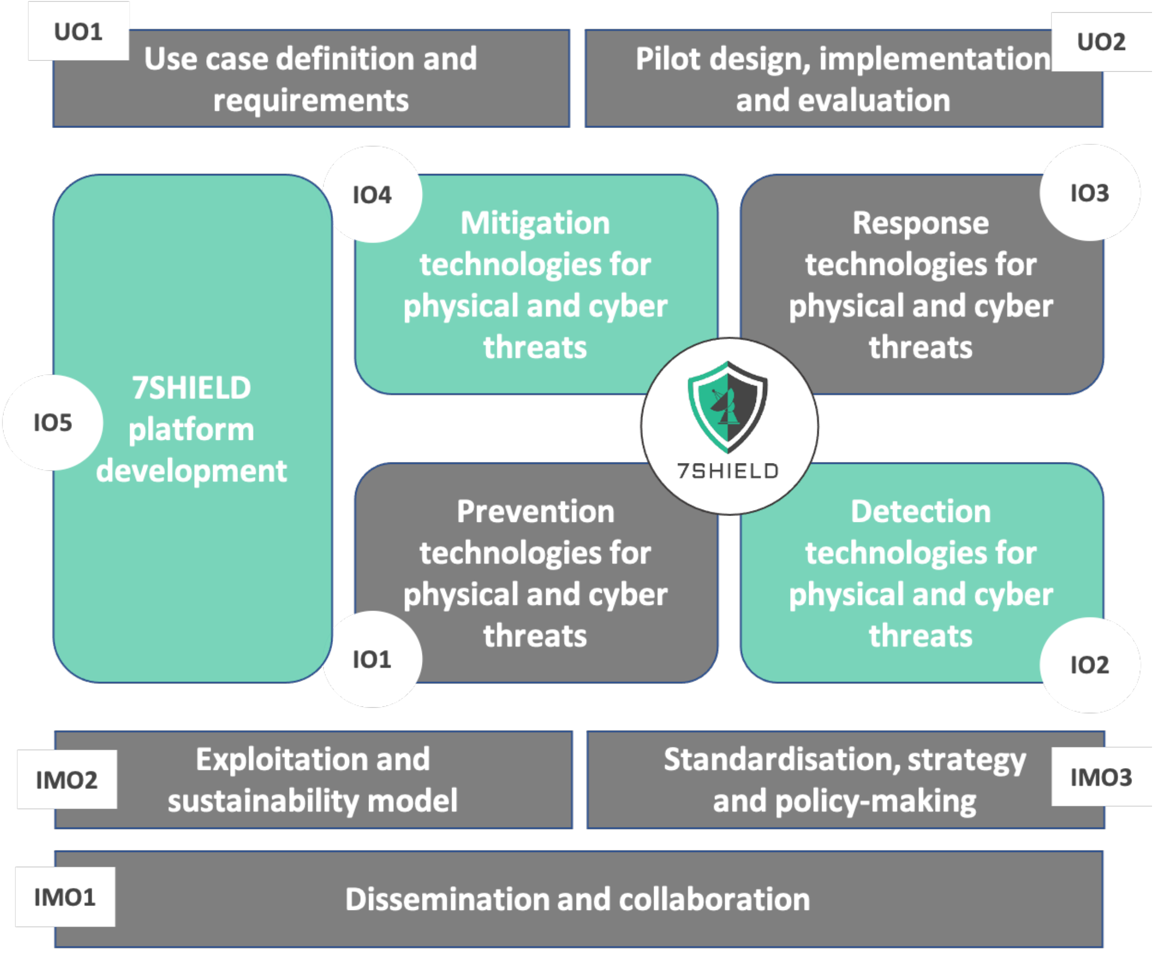

UO1
Use case definition and requirements
Pilot design, implementation and evaluation
UO2
IO4
Mitigation technologies for physical and cyber threats
Response technologies for physical and cyber threats
IO3
IO5
7SHIELD platform development
7SHIELD
Prevention technologies for physical and cyber threats
IO1
Detection technologies for physical and cyber threats
IO2
IMO2
Exploitation and sustainability model
Standardisation, strategy and policy-making
IMO3
IMO1
Dissemination and collaboration

Figure 2-1: 7SHIELD objectives

Each objective includes some specific activities. To follow the progress of the project activities on a regular basis and better understand potential difficulties, the deliverable reports the achievements and the activities carried out for each objective and tries to quantify, and thereby measure, a number of KPIs related to each activity and objective. KPIs ensure project management effectively and efficiently monitor the project evolution and progress towards such objectives. 7SHIELD has identified a number of KPIs related to each objective and activity to ensure the highest impact, as well as the quality and success of the expected outputs. Some activities have reached more than one achievement in the first six months of the project while others have just started. This document is constantly evolving so that progress can be taken into account in relation to each objective.

2.1. Innovation objectives and innovation activities

IO1. Prevention technologies for physical and cyber threats: 7SHIELD will assess the vulnerability of each asset of the space ground segment, whether it is some mechanic component or data asset. The foreseen technologies which contribute to the pre-crisis phase involve also analytical prediction models for future threats, secure authentication mechanism for data access and cascade effects from combined cyber-physical attacks.

In this period, the main achievements are related to the **vulnerability estimation for risk assessment** activities and in particular to the requirement definition for the CIRP platform and to the definition of a concreate roadmap for its integration with the technology for assessing cascading effect from physical and cyber-attacks. The main achievement was the design, development and release of an integrated prototype of the multi-hazard risk assessment tools which 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 Pilot Use Cases until M24.

Moreover, the SSO functionality and components to be developed for a **secure authentication mechanism** have been established. 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 end points (i.e. OpenID endpoint configuration and SAML 2.0 identity provider metadata) has been deployed on the OVH cloud environment. The Keycloak instance was interfaced with the SERCO reference environment and 5 7SHIELD modules (MBDA, DiVA, SPGU, CPTMD and the CADF) were successfully interfaced with the secure authentication mechanism.

Regarding the **cascading effects**, research on threat modelling and cascading risk assessment methods has been conducted and an analysis of the existing threats and attack paths modelling methods and tools to define a first conceptualization of the cascading effect. Then, a methodology for the assessment of cascading risk due to complex threats has been defined. Finally, the chosen methodology has been implemented in the MBDA tool. 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 achievements related to the **Cyber and Physical Threat Intelligence** have produced an analysis of the different data source to identify cyber and physical threats along with an understanding of the main capabilities of the current solutions. After that, the development of the data extractor for the Threat Intelligence service was performed. Then, implementation of the threat intelligence core has been developed and a first prototype of the Threat Intelligence service has been developed to be tested in the SERCO and NOA pilot.

IO2. Detection technologies for physical and cyber threats: 7SHIELD will encompass state-of-the-art detection technologies to seamlessly and accurately identify potential physical or/and cyber threats to Space Systems, ground Segments and Satellite data assets.

The activities concerning this objective have been finalised and the main achievements have been fulfilled.

The main achievement is the release of the final 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. 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 is 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.

Moreover, the development and release the final version of the **Face Detection and Recognition (FDR)** module and of the **Video-based Object Detection (VOD) and Activity Recognition (AR)** modules. · A series of evaluation measurements were utilised in order to estimate the modules' performance. Video-based surveillance technologies have been successfully evaluated during the NOA and DEIMOS operational tests.

Another achievement is 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.

Moreover, the **MultiModal Automated Surveillance (MMAS) system**, which is capable to detect possible threats through the use of video images has been developed. The final prototypes of the **Perimeter Laser Sensor (PLS), the Laser Fence Sensor (LFS) and the 3-Dimensional Mini drone (3D-MND) detectors** have been deployed.

Development and release 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; **Availability Correlation (AC)** module which takes availability alerts generated by the ADM module and aggregates alerts related to the same incident together; **Hyper-Correlation Component (HCC)** that mixes Cyber security alerts from the Cyber-Attack Correlation (CAC), physical attack events from the Geospatial Complex Event Processor (G-CEP) along with the Availability alerts from the Availability Correlator (AC). Moreover, 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. Finally, the final 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 has been developed and released.

Particularly, the final prototypes of physical and cyber detectors and correlators have been released and evaluated by their participation in the operational tests on pilot premises. These activities have been reported in detail in the seven deliverables that were issued on time during the reporting period.

IO3. Response technologies for physical and cyber threats: 7SHIELD will tailor innovative technologies to monitor the evolvement of a physical or/and cyber-attacks, to strengthen the responsiveness and social awareness.

The main achievements reached are related to the semantic representation and linking for reasoning and decision-making. The **7SHIELD Knowledge Base (KB)** or 7SHIELD ontology is a knowledge representation model for semantically representing concepts relevant to the cyber-physical threats. The KB framework has been developed and encompasses technologies for semantic content and sensor input modelling 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. Moreover, the final prototype 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 has been released.

The **Tactical Decision Support System (TDSS)** 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 main achievement 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.

In the period, the first prototype of the **warning message generation** and the final one was implemented. The main achievements for the period regarding the **UAV neutralization** 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. The final prototype was implemented, and more tests were performed. The tool is integrated with the engage tool to be used in the pilots.

IO4. Mitigation technologies for physical and cyber threats (including novel installation designs): 7SHIELD will consolidate the appropriate actions to mitigate the consequences of physical and cyber-attacks, focusing on the services continuity.

Regarding the development of **service continuity scenarios for cyber-attacks**, a generalized physical operations model was generated for representing the Operation Technology functionality of each PUC. In relation to the **service continuity scenarios for physical-attacks**, a generalized cyber operations model a generalized physical operations model was generated for representing the Operation Technology functionality of each PUC. The cyber and physical models are interconnected in order to produce a unified view of consequences to cyber-physical operations.

IO5. 7SHIELD platform development: This objective will deal with the design of 7SHIELD platform's architecture and integration of all subsystems.

The SPGU module initially not contemplated took shape. The need arose for a data collector that would collect all the information coming from the detectors and correlators and that allowed to have a general overview of the events that took place in a critical infrastructure (situational picture). Regarding the System Integration, the initial work was aimed at defining how to integrate all the components developed in WP3, WP4, and WP5. 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 integrations of the tools that interact with the detection modules have been updated.

The **Data Models** considered in the main 7SHIELD components, and a first set of known ontologies have been analysed. The design of a Situational Information Model has started and a format to be to be adopted for the exchange of information related to alerts, threats, and combined threat scenarios has been established. A Data Model was contemplated that would allow to manage data of the current Situational Picture and that would allow to historicize these SPs during the life cycle of the SP of the critical infrastructure.

Activities related to the **user interfaces implementation** are related to the 7SHIELD User Interface (GUI), whose main objective is to present to the users the status of the infrastructure, details of the crises that have to be confronted and to enable the management of the related response activities that are required. Integrations with the

7SHIELD tools have also been implemented, enabling the collection of the information from the field (operational picture) and facilitating the response and decision-making activities that are required to be executed by the commanders and the first responders, during a crisis.

2.2. User-oriented objectives and user-oriented activities

UO1. Use case definition and requirements: In 7SHIELD the systematic approach/study of the specific user requirements will bring out the general rules and procedures to consolidate them into a standardized framework which ensures the safety and security of Space Systems, ground Segment and Satellite data assets.

The objectives of the use case design, stakeholder engagement and user requirements activities have been 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. **Use case design, stakeholder engagement and user requirements** activities resulted in the definition of five use cases and 19 user scenarios of cyber, physical and combined cyber-physical attacks. 10 focus groups have been implemented by the Pilot Use Case Leaders for the design of the use cases and scenarios, with the participation of end-users from the Ground Segment operations teams, asset security management professionals, and first responders. Diverse end-users and stakeholders were engaged and participated in the use cases design and collection of user requirements. 16 questionnaires were answered by Ground Segment professionals, critical infrastructure protection experts, and first responders. At the end, 250 functional and non-functional user requirements were defined by the end-users and stakeholders.

The general **security requirements** and principles that will guide the development of the 7SHIELD system and its modules have been defined and established. More than 40 security requirements have been defined, including measures for access control, secure user authentication, traffic monitoring and encryption, data integrity, minimization of vulnerabilities, and secure backups. 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.

Activities to ensure compliance with **legal and ethical requirements** have been take place. 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 have been analysed.

UO2. Pilot design, implementation and evaluation: The 7SHIELD needs to be evaluated and testing within the operational environment to probe its performance to cope with real hazardous situations in Critical Infrastructures.

The achievements until M24 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), SPACEAPPS (PUC4), NOA (PUC3) and DEIMOS (PUC2). The evaluation methodology was designed to capture the performance and usability of the KR modules, as well as the user satisfaction and feedback.

Moreover, the four **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. They were then performed on the PUC3 (NOA) and PUC2 (Deimos) in hybrid physical and cyber attacks scenarios. 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.

2.3. Impact-making objectives and impact-making activities

IMO1. Dissemination and collaboration: In the context of 7SHIELD we aim at disseminating the project results with an emphasis in wide number of actors in the whole security management cycle, governmental authorities and academic institutes, as well as to the security agencies. The project aims at establishing close collaborations with existing projects working in similar research domains and external bodies.

For the **dissemination and communication of the project results**, the National/Regional Space Agencies community, the Ground segment operators' community and the Security experts community have been approached through the participation to several events.

Regarding the **collaboration and clustering**, 7SHIELD has integrated the Critical Infrastructure Protection community as it is now a member of the European Cluster for Securing Critical Infrastructures (ECSCI). 7SHIELD participated to the 2ndEU-HYBNET Annual Workshop (https://euhybnet.eu/) and the 2ndECSCI (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 invitation of SU-INFRA-01 projects to the Info

Day SERCO is currently preparing. 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 also consolidating the relationships with other EU projects emphasizing the complementarity and the value added brought by the project outcomes.

IMO2. Exploitation and sustainability model: This specific objective is linked to the achievement of an exploitable and sustainable model of 7SHIELD results and solutions at different levels as key to the success of the project vision.

The work carried out up to M24 to achieve the IMA2.1objective was done in two phases. The first phase started with the identification of the different Key Exploitable Results (preliminary version) and the building of the first version of a commercial-oriented presentation. Afterwards, an in-depth desk study has been performed to identify the market trends/drivers and draw a picture of the supply & demand landscape. Bottom-up and Top-down analyses have been performed to assess the total accessible market. 7SHIELD value proposition has been defined (preliminary version) and its competitive advantages identified. The second phase to achieve this objective was to finalise and submit the second version of the market analysis. To this end, the first market analysis was refined and completed by adding information and analysis for all components of the 7SHIELD framework. A first version of the Exploitation plan report was produced and submitted. Specifically, in the exploitation plan, the main 7SHIELD Key Exploitable Results have been presented and during the 7SHIELD Operational Tests have been tested and validated.

IMO3. Standardisation, strategy and policy-making: This objective deals with the 7SHIELD's aims to standardize and demonstrate strategies and policies to prevent, early detect, response and mitigate of amalgamated attacks in physical and cyber manner. The IMO3 is decomposed into the following activities.

For the **policy framework, standardisation, strategy and policy-planning**, the European Ground segment security policy and standards community has been approached.

Regarding the policy framework, we are exploring the current and proposed European policy framework regulating electronic communications operations to understand the current policy requirements and make policy recommendations. We will focus in particular on how the current policies could influence the solutions and what gaps in the policies are present that need to be put in place to make it possible to fully implement the 7SHIELD innovative technologies. Work has been performed to understand how the developments in 7SHIELD could possibly influence future policy and understand how requirements arising from existing policies have shaped the requirements on 7SHIELD key results. Regarding the Standardisation, strategy (investment measures) and policy-planning, we are investigating the current standards and practices being used by operators of ground segments of space systems, security authorities, industry, policy makers, and civil protection across the European Union. This activity will have its main effort in the last quarter of the project. In the current reporting period, some preparation work has been performed, meetings attended and being an observer at the demonstrations. Future work will focus on re-visiting contacts with the European Space Agency and contacting other organisations such as EUSPA and SatCen as well as the European Standards Organizations, CEN, CENELEC, and ETSI.

2.4. Project Objectives

In this section are listed the specific objectives and activities for the project as described in the DoA. The work carried out, during the 24 months, towards the achievement of each objective and the assessment of the progress in relation to the specific activities, considering also the expected KPIs, is described in detail.

2.4.1. Innovation objectives and innovation activities

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)	KPIs: Integrated Scientific Models; Ingested datasets size
	IA1.2 Secure authentication mechanism for data access (KR02)	KPI: 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: Number of identified threats due to cascading effects identified in pilot sites.
	IA1.4 Cyber and Physical Threat Intelligence (KR04)	KPI: Accuracy, Error rate.
Achievements		
IA1.1 – Vulnerability estimation and classification per asset for risk assessment (KR01) is related to KER01a: Risk Assessment tools (CIRP Platform) provided by STWS and KER01b: Cyber Risk Assessment (DiVA) provided by ENG, both activities implemented within task 3.1 Risk Assessment tools (M1-M16). The main achievement in the reporting period was the design, development and release of an integrated prototype of the multi-hazard risk assessment tools (KR1) which 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. The results		

of these activities were documented in deliverable D3.1 - "Risk Assessment tools", submitted at M10, while further details of the process were documented in D3.3 & D3.5. Functionalities related to the risk assessment of cyber threats were already implemented, demonstrated and evaluated during the Pilot Use Cases until M24. The risk assessment process of natural and physical threats will be demonstrated and evaluated during the upcoming PUCs which include respective scenarios. For the above demonstration purposes (from M16 to M24), integration tests have been conducted, as well as adaptations and enhancements based on the feedback received by the end users.

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 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 end points (i.e. OpenID endpoint configuration and SAML 2.0 identity provider metadata) has been deployed on the OVH cloud 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 5) took place in October 2021. In addition, 5 7SHIELD modules (MBDA, DiVA, SPGU, CPTMD and the CADF) were successfully interfaced with the secure authentication mechanism validated during SPACEAPPS (PUC4) pilot in November 2021, NOA (PUC3) in March 2022 and DEIMOS (PUC2) in May 2022.

IA1.3 – During the first six months of the project, as described in D1.2, it has been conducted a research of state of the art and requirements on threat modelling and cascading risk assessment methods and tool and an analysis of the existing threats and attack paths modelling methods and tools. In the same period, a preliminary conceptualization of the cascading effect issue and of the known modelling solutions to address such concepts have also been devised. 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 RESIL 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 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 at M24, the implementation of the cascading effects analysis functionality has been finalized and released. The functionality has been tested in the NOA and DEIMOS pilots and allowed to identify more than zero threats: therefore, the percentage of achievement is now 100%.

IA1.4 – During the first period of the project, ENG performed the analysis of the user requirements for Threat Intelligence (TI) and defined the logical architecture of the prototype and the preliminary interfaces of the services that will be implemented for communicating with the other modules of the 7 SHIELD system. In particular, ENG focused on different key activities: 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 that should be used in the service.

After that, the development of the data extractor for the Threat Intelligence service was performed. Furthermore, state of the art analysis on machine learning algorithms has been done to establish the algorithm that is developed inside the service. Secondly, the definition of the ToC of Deliverable 3.4 has been completed with the approval of other partners.

In the last period, implementation of the threat intelligence core has been developed and a first prototype of the Threat Intelligence service has been developed to be tested in the SERCO and NOA pilot. These two pilots helped in the collection of some feedbacks to improve the performances of the tool. In fact, a refinement of the Deep learning NLP algorithm for text analysis has been performed and the support to another source has been implemented (Reddit).

The latest version has been used 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 autonomous operation of each type of agent 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 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).
	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)	**KPI2.3.1**: # 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.

Achievements

IA2.1 – The main achievement in the reporting period is the release of the final 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 is 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 demonstrations. 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 2.1.3 – achieved) and 25 km^2 monitored area in one mission assessed (KPI A2.1.4). The KPI 2.1.4 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 is 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 2.1.2). Therefore, KPI 2.1.2 has been successfully achieved.

The 7SHIELD UAV has been demonstrated in DEIMOS pilot, while all the activities and results have been reported in deliverable D4.3 – Data collection from UAVs and processing at the edge techniques.

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

- Development and release the final version of the Face Detection and Recognition (FDR) module. The FDR processes offline and online 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 sacrificing 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 and release the final version of the Video-based Object Detection (VOD) and Activity Recognition (AR) modules. The VOD module processes offline or online 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 7SHIELD UAV and will be capable of performing on-board image/video processing by focusing on object detection from captured videos by the drone.

- Several evaluation tests have been conducted in order to estimate the modules' performance. Regarding the VOD module, there are 2 distinct cases: One involve the outdoor models which are expected to be used in outdoor environments. A variation of EfficientDet and Yolov4 networks have been trained for the project. In the following Tables the baseline and the improved model's evaluation results are presented. Table 1,2 and 4 have been trained on exactly the same dataset and, thus, the results are completely comparable to each other. Table 3 is presented as a reference only because it has been trained on a different dataset (which, nevertheless, contained some common samples with the previous dataset) and the comparison with this model cannot be considered straight forward. Despite this fact the dataset which was used for Tables 1, 2 and 4 is considered more appropriate for the project's purposes because it contains only samples relevant to the project's objectives. Table 3's dataset is a subset of COCO which contains the relevant classes from various perspectives and capturing conditions.

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

Table 1

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

Table 2

baseline outdoor Yolov4 Average Precision (AP)		
70.47% (person)	59.88% (car)	56.22% (truck)
81.16% (bus)	64.2% (motorcycle)	60.93% (mean AP)

Table 3

Improved model outdoor Yolov4 Average Precision (AP)		
59.21% (person)	80.72% (bus)	81.0% (car)
56.39% (motorcycle)	70.55% (truck)	**mAP 69.57%**

Table 4

Next, we present the results for the indoor models. These models are expected to be launched in order to cover indoor scenes and, thus, have different qualities than the previous ones. A different dataset has been compiled which contains just 2 classes (in contrast to the outdoors 5 classes). This dataset is also compiled for the purposes of the project yet instances correspond to the specific classes and scenery. The results are shown below. The model processing speed is about 35 fps.

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

Table 5

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

Table 6

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)

Table 7

Regarding the Object Detection at the Edge (ODE) model, preliminary experimental evaluations were carried out attempting to evaluate the model's performance at the edge. 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 8 fps that were processed by the Jetson AGX Xavier. The effectiveness remains the same of course:

Yolo v4 effectiveness evaluation - Average Precision (AP)		
59.21% (person)	80.72% (bus)	81.0% (car)
56.39% (motorcycle)	70.55% (truck)	**mAP 69.57%**

Table 8

Video-based surveillance technologies have been successfully evaluated during the NOA and DEIMOS operational tests. The activities and experimental results have been reported in the deliverables *D4.1 - Video surveillance techniques: Initial release* and *D4.5 - Video surveillance techniques: Final release.*

IA2.3 – The main achievement in the reporting period is 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 four operational Pilot Use Cases, in SERCO, SPACEAPPS, NOA and DEIMOS over a total of 7 misuse cases (KPI2.3.2 = 7).

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 7 high impact attacks (KPI2.3.1 = 7) with a percentage of achievement around 70%. 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 consolidate our results and confirm our expectations. The activities and experimental results have been reported in the deliverable *D4.4 - Cyber-attack detection methods.*
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 Near-InfraRed (NIR) and Thermal EO sensors that are supported by multiple processes, which process the video images from cameras, by employing Convolutional Neural Networks (CNN) to classify three kinds of entities: reindeers, vehicles and persons and movement detection algorithms. 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 permits an operator to monitor the area under surveillance, configure and set the alarms. During this period has been performed 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. Definition of the Interfaces with the 7SHIELD platform (security protocols and brokers) and of the main messages produced by the MMAS. Development and testing of the interfaces with 7SHIELD core, namely messages and security protocols like SSL with the Kafka broker. Transport the MMAS camera and processing unit to FMI demo premises. Created a data set based on images taken during the outdoor activities, by 7SHIELD cameras to be used during the demos. Testing of the CNN models in real environment and in real time with high performance GPUs. Development of 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. The algorithms developed exceeded the KPIs required values for the classical detection measures F-1 and tracking measure of MOTA. Delivered the document "*D4.6 Infrared and thermal image processing techniques*" and the scientific paper "*Study on the Application of EfficientDet to Real-Time Classification of Infrared Images from Video Surveillance*".
IA2.5 – The main achievements in the reporting period are the deployment of the final 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 reporting period, development and implementation work on all sensors have been completed, and in-house field trials commenced, the KPI was covered (80-90%). PLS and 3D-MND have been successfully evaluated during the DEIMOS operational test. The activities of the laser-based tools have been reported in deliverable *D4.7 - Combined Physical and Cyber Threat detection and correlation.*

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

- Development and release 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 operational tests (Pilot Use Cases), in SERCO, SPACEAPPS, NOA and DEIMOS. The ADM module successfully detected 100% of the simulated malfunctions used in Pilot Use Cases' testing phases. ADM is fully developed and its SSL secure connection has been developed and integrated.
- Development and release 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 being integrated into the 7SHIELD framework and evaluated in NOA and DEIMOS operational tests. AC fully developed and its SSL secure connection has been developed and integrated.
- Development and release the Hyper-Correlation Component (HCC) that mixes Cyber security alerts from the Cyber-Attack Correlation (CAC), physical attack events from the Geospatial Complex Event Processor (G-CEP) along with the Availability alerts from the Availability Correlator (AC). The HCC module is currently being integrated into the 7SHIELD framework and its SSL secure connection has been developed and integrated. It has been evaluated in NOA and DEIMOS operational tests.
- 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. It has been successfully evaluated during the pilots.
- Development and release of the final 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). It has been successfully evaluated during the SERCO, SPACEAPPS, NOA and DEIMOS pilot.

- 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).

The activities and the results have been reported in the deliverables *D4.2 - Combined Physical and Cyber Threat detection* and *D4.7 - Combined Physical and Cyber Threat detection and correlation.*

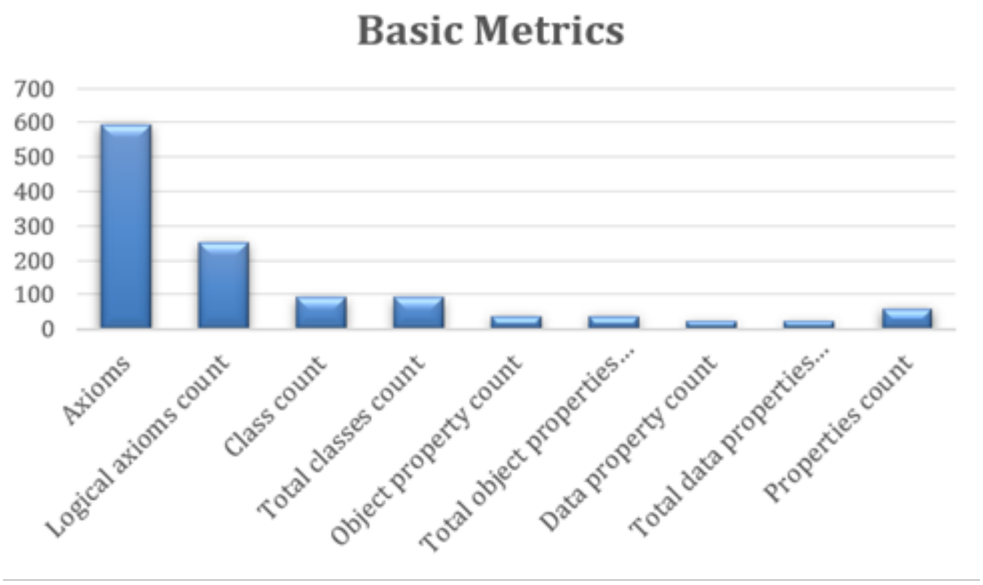
Innovation Objectives	Innovation Activities	KPIs
IO3. Response technologies for physical and cyber threats	**IA3.1** Semantic representation and linking for reasoning and decision-making (KR12)	KPIs: Quality (e.g. Content Quality Metric, Structural Quality Metric (Raad & Cruz, 2015)) and completeness 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)	KPIs: Precision and accuracy in the crisis level estimation.
	IA3.3 Decision Support mechanism (KR14)	KPIs: Quickness and quality of information provided and calculated in the reasoning process.
	IA3.4 Social awareness and interaction with the citizens (KR15)	KPIs: 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)	KPIs: 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 the OntoMetrics tool, an online framework that evaluates the ontology based on predefined metrics. The following tables present the results of the aforementioned process. It contains the base metrics which show the quantity of the ontology, numbers of triples, classes, object and data type properties and individuals.

Axioms	594
Logical axioms count	251
Class count	91
Total classes count	91
Object property count	36
Total object properties count	36
Data property count	22
Total data properties count	22
Properties count	58
Description Logic expressivity	ALCHI(D)



The retrieval of all the knowledge that was processed and stored to the developed Knowledge base, based on the 7SHIELD ontology is accomplished through a RESTApi service. Some of the Competency Questions were translated into SPARQL queries and applied on top of the Knowledge Base facilitating the process of retrieving historical information regarding the alerting events, based on geo-temporal inputs and producing a detailed report for each one of them respectively.

IA3.2 – The main achievements in the reporting period (M1-M24) were the release of final prototype 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). The Crisis Classification module has been evaluated through the operational tests that have been realised in the reporting period. The Crisis Classification module was applied for the first time in a previous project that called beAWARE [8]. 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%.

A detailed description of the Crisis Classification module accompanied by the experimental results has been provided in the submitted deliverable *D5.3 Security Risk Assessment Algorithms*.

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.

The TDSS system was established as the 1st lab prototype and the final one was also achieved, integrated with the 7SHIELD core and already used.

Based on the results already in the first exercise in NOA premises (PUC3) the KPI was achieved. With the data available and results obtained the objective defined for the TDSS is achieved (in it produces and makes available more than 75% of relevant information).

During the period the deliverable D5.2 was submitted.

IA3.4 – The 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. During the period a first phase analysed 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 developed a standardised warning message generation framework to support rapid and clear communication with citizens across multiple languages. In the period the first prototype of the warning message generation and the final one was implemented. In the period the deliverable D5.4 was achieved and submitted on time. 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 demonstration activities, NOA, FMI and SPACEAPPS demos and to be reported after.

IA3.5 – 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.

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 is fitted with under-belly net which will be used for "catching" the intruder drone. Initial phase of FH flight is 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 was 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. The final prototype was implemented and more tests were performed. The tool is integrated with the engage tool to be used in the pilots. KPI for UAV neutralisation is flying to the target drone and "catching" it and bringing it back to pre-determined location. In-house flight trials are being conducted. KPI was partially achieved (55%). The deliverable D5.5 was concluded and submitted on time.

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**: Downtime of critical services.
	IA4.2 Development of service continuity scenarios for physical attacks (KR17)	**KPIs**: 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.

<table>
<tr><td colspan="3">During the period, a generalized physical operations model was 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 a first phase 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 more than 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 integrated solution into the 7SHIELD core and testing in vivo will be undertaken in the next phase to fulfil the KPI.</td></tr>
<tr><td colspan="3"><b>IA4.2 –</b> Similarly to IA4.1, a generalized cyber operations model a generalized physical operations model was generated for representing the Operation Technology functionality of each PUC. The cyber and physical models are 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 more than 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 only 50% fulfilled. Final integration into the 7SHIELD solutions and testing in vivo will be undertaken in the next period to fulfill the KPI.</td></tr>
<tr><th>Innovation Objectives</th><th>Innovation Activities</th><th>KPIs</th></tr>
<tr><td rowspan="3"><b>IO5.</b> 7SHIELD platform development</td><td><b>IA5.1</b> 7SHIELD platform integration (KR18)</td><td>KPI: 7SHIELD modules integrated and deployed in the Framework</td></tr>
<tr><td><b>IA5.2</b> Data Models for Combined Detection (KR19)</td><td>KPI: Semantic concept defined</td></tr>
<tr><td><b>IA5.3</b> User interfaces/Command and Control (C2) (KR20)</td><td>KPIs: Common Operational Picture
refresh updates; Number of assets depicted on map (without clustering) without flickering; Standards supported.</td></tr>
<tr><th colspan="3">Achievements</th></tr>
<tr><td colspan="3"><b>IA5.1 –</b> 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).</td></tr>
</table>

During the second year of the project, 16 out of 32 components were integrated and deployed at PC5 (SERCO) and PC4 (SPACEAPPS), respectively at M14 (October 2021) and M15 (November 2021), 30 out of 32 were integrated and deployed at PC2 (NOA) and PC3 (DEIMOS), respectively at M19 (March 2022) and M21 (May 2022), while Pilot Demos are going to take place in September 2022, November 2022 and December 2022, respectively in Greece (NOA), Finland (FMI) and Belgium (SPACEAPPS), where all the 7SHIELD components will be integrated, deployed and validated. KPI will be fully achieved at the end of the NOA demo pilot.

IA5.2 – 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 was fully achieved in the first reporting period.

IA5.3 – The 7SHIELD User Interface (GUI) consists of the following dashboards: (a) cyber and physical dashboards to visualize threat data (both physical & cyber) that have been identified by the detection and correlation tools are provided by CeRICT and ENG, whereas (b) the management of the situation is available through the C2 system provided by STWS. During the reporting period (M1-M24), these components have been adapted to handle physical and cyber threats (also combined ones). Integrations with the 7SHIELD tools have also been implemented, enabling the collection of the information from the field (operational picture) and facilitating the response and decision-making activities that are required to be executed by the commanders and the first responders, during a crisis. In order to support these functionalities, integrations of the UI components with the other 7Shield tools, such as the detection and correlation tools, the crisis classification module, the emergency response plans, the FRSS, etc. have been designed, implemented and evaluated.

Moreover, the design of ENGAGE CSIM UI has been finalized facilitating the everyday operations of the commanders, including incident and resource management. A big number of resources (>4000 objects), such as vehicles, equipment and personnel, can be managed effectively by the users. The status and location of these resources are available on the map of the commanders, without the need for clustering techniques and the flickering of the visualization. Advanced technologies have been used for the exchange and the visualization of this information, having the events available and the commander monitors in less than 2 seconds.

Both for backend services, but also for the GUI of ENGAGE, a number of interoperability standards have been used, in order to support the effective management and the sharing of information. In more detail, the UAF message format has been used for the sharing of information among the 7SHIELD components whereas the EDXL DE, EDXL CAP, EDXL SitREP and OASIS TSO standards have been used for the management of the operational information internally by the ENGAGE CSIM system. Additionally, the management and visualization of the spatial data, have been based on a number of OGC standards, such as the GeoTIFF, WMS and WFS standards.

In the Cyber-physical Threat Monitoring dashboard (CPTMD) provided by ENG, during the reporting period (M1-M24), many activities were executed. The integration with the Keycloack Single Sign On System has been completed. The CPTMD visualizes the Situational Picture, with the current situation and the historical situations for each SGS Pilot. In addition, the integration with the Knowledge Base module for event filter has been completed. Finally, for each situation, it is possible to export the information as a pdf file. Regarding the other independent external dashboards (web applications) that are available through the CPTMD, the integration with the Cyber Attack Dashboard, DiVA, MDBA, and CIRP platform have been completed. In the SGS Infrastructure the information provided by the MDBA tool regarding the areas and assets of the SGS are visualised into the CPTMP map. In addition, the CPTMD visualise the risk assessment data provided byDiVA and CIRP module. Instead, the integration of the resilience data of the CIRP module is being developed. Finally, the information of the situation (events, area, assets) is visualized in the map via popup. Every popup is draggable.

2.4.2. User-oriented objectives and user-oriented activities

User-oriented Objectives	User-oriented Activities	KPIs
UO1. Use case definition and requirements	**UA1.1** Use case design, stakeholder engagement and user requirements	KPIs: 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	KPIs: Secure access to the system, secure communications.
	UA1.3 Ethics and legal framework	KPIs: 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 have been 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 main focus groups were organized (one by each Pilot Leader), complemented by several follow-up bilateral discussions and 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,

<table>
<tr><td colspan="3">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.</td></tr>
<tr><td colspan="3"><b>UA1.2 –</b> 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.</td></tr>
<tr><td colspan="3"><b>UA1.3 –</b> This UA has 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.</td></tr>
<tr><th>User-oriented Objectives</th><th>User-oriented Activities</th><th>KPIs</th></tr>
<tr><td rowspan="2"><b>UO2.</b> Pilot design, implementation and evaluation:</td><td><b>UA2.1</b> Development of the validation scenario and evaluation methodology</td><td>KPIs: Evaluation metrics, User satisfaction metrics, user feedback, system usability metrics.</td></tr>
<tr><td><b>UA2.2</b> Field demonstrations, testing and training</td><td>KPIs: User satisfaction metrics, user feedback, system usability metrics.</td></tr>
<tr><th colspan="3">Achievements</th></tr>
<tr><td colspan="3"><b>UA2.1 –</b> The achievements until M24 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), SPACEAPPS (PUC4), NOA (PUC3) and DEIMOS (PUC2). 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 "Evaluation metrics, User satisfaction metrics, user feedback, system usability metrics" 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.</td></tr>
<tr><td colspan="3"><b>UA2.2 –</b> During the reporting period, the four 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</td></tr>
</table>

operational environments. They were then performed on the PUC3 (NOA) and PUC2 (Deimos) in hybrid physical and cyber attacks scenarios.

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.

The operational test reports of the PUC3 and PUC3 are available to the project and will be used as inputs to the final evaluation report D7.3.

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 has been reassessed for the final 7SHIELD framework.
- Feedback from users were positive, with a few suggestions for improvements.

For PUC3, 4, and 5, a 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. For PUC2, an actual Likert scale was introduced at the operation test debriefing and evaluation. The analysis was made for each KR in three categories that were tested in the pilots (PUC2, PUC3, 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 demonstration of the final 7SHIELD framework.

Category	PUC2	PUC3	PUC4	PUC5	Overall
UI and user friendliness	3.5	4.83	3.67	3.00	3.75
Adaptability	3.6	4.75	2.33	2.29	3.24
Compatibility	4.08	4.58	3.56	3.83	4.01
Combined	3.7	4.72	3.19	3.04	3.66

The remaining work of this activity will consist of the three demonstrations where the complete system will be demonstrated and evaluated, in PUC3, PUC1 and PUC4.

After all the pilot's operational tests (in SERCO and SPACEAPPS, NOA and Deimos), the KPI 2.2.1 is partially covered. The average user-satisfaction rate is about 90%, while the completion rate is 50 % when giving more weight to the incoming operation pilots and demo pilots.

2.4.3. Impact-making objectives and impact-making activities

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

Achievements

IMA1.1 – The communication achievements until M24 are the following:

- establishment of the 7SHIELD visual identity,
- design of the project brochure and info board,
- development of the project's website, which has reached 3385 visitors by M24,
- setup of a 7SHIELD LinkedIn page, which has reached 236 followers by M24,
- Launch of the 1st 7SHIELD newsletter issue,
- appearances in third-party media and frequent posts of project news on the 7SHIELD website and LinkedIn.

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 has been partially achieved (50%). It will be fully achieved until the end of the project.

In the same period, 7SHIELD consortium carried out the following dissemination activities:

- 4 publications
- participation in 19 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, SERCO is currently organizing the 7SHIELD Infoday that will take place in December 2022 in Brussels, Belgium after the last pilot demo at SPACEAPPS. Non-project partners and stakeholders from the space industry and the domain of critical infrastructure security will be invited to attend the event.

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 thematic.

- 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, becoming a member of the European Cluster for Securing Critical Infrastructures (ECSCI–https://www.finsec-project.eu/ecsci) has partially achieved (75%) the KPI 1.1.2, starting the clustering and networking activities with other 24 H2020 research projects dealing with security of Critical Infrastructures. During the reporting period, 7SHIELD participated to the

- 2nd EU-HYBNET Annual Workshop (https://euhybnet.eu/)
- 2nd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop,
- Final conference of the ISFP project DroneWISE

consolidating the network with (in priority but not limited to) SU-INFRA-01 projects and now that more tangible results are achieved, we started to involve the prime of the projects in SU-INFRA-01 (DEFENDER, PRAETORIAN, INFRASTRESS, SATIE, SECUREGAS, PRECINCT and so forth).

The KPI will be achieved in the remaining period of the project, with the invitation of SU-INFRA-01 projects to the Info Day SERCO is currently preparing. Non-project partners will be invited (relying on networks already established as well as new contacts to be collected in the future events).

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

Achievements

IMA2.1 – The work carried out up to M24 to achieve the IMA2.1objective was done in two phases. The first phase started with the identification of the different Key Exploitable Results (preliminary version) and the building of the first version of a commercial-oriented presentation. Afterwards, an in-depth desk study has been performed to identify the market trends/drivers and draw a picture of the supply & demand landscape. Bottom-up and Top-down analyses have been performed to assess the total accessible market. 7SHIELD value proposition has been defined (preliminary version) and its competitive advantages identified (preliminary version). A comparison against the competitive landscape has been performed. In anticipation of the second version of the Market analysis, an interview process and guideline has been built to collect feedbacks from potential future users. The first version of the Market analysis has been finalised and submitted at M6. This Market analysis includes an analysis of the total accessible market and an overview of the competition landscape. The Support of The Horizon Result Booster has been requested to help partners identify the most promising Key Exploitable Results. A first list of potential Joint Exploitation Plans has been identified. A continuous market and competitive intelligence were performed to keep an up-to-date situational awareness that will feed the future version of the Market Analysis Report. Organisation of an internal workshop gathering all Key exploitable asset owners to identify which parts of the Market Analysis Report need to be updated and/or refined.

The second phase to achieve this objective was to finalise and submit the second version of the market analysis. To this end, the first market analysis was refined and completed by adding information and analysis for all components of the 7SHIELD framework. The local market study was also completed, as well as the continuous updating of the 2nd market analysis. The second version of the Market analysis has been finalised and submitted at M18.

IMA2.2

A first version of the Exploitation plan report was produced and submitted. Specifically, in the exploitation plan, the main 7SHIELD Key Exploitable Results have been presented and during the 7SHIELD Operational Tests have been tested and validated.

4 Operational Tests of the 7SHIELD framework were performed:

- The 1st Operational Test was performed on the ONDA DIAS (Copernicus' Data & Information Access Services).
- The 2nd Operational Test was performed on the ICE Cubes Service (ISS International Commercial Experiment Cubes).
- The 3rd Operational Test was performed on the facilities and infrastructure of the National Observatory of Athens in Penteli, Greece.
- The 4th Operational Test was performed on the Deimos Ground Segment in Spain.

Regarding, the Demonstrations to other external installations, some of the 7SHIELD's modules (Cyber-physical threat/attack detection service including SPGU and SA model, and the Cyber-physical Threat Monitoring Dashboard) will be adapted and tested in another EU project, PRECINCT in the context of two or more Living Labs (LLs).

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

		dissemination and clustering

Achievements

IMA3.1 – In this activity we are exploring the current and proposed European policy framework regulating electronic communications operations to understand the current policy requirements and make policy recommendations (EETT). We have focused in particular on how the current policies could influence the solutions and what gaps in the policies are present that need to be put in place to make it possible to fully implement the 7SHIELD innovative technologies. Work has been performed to understand how the developments in 7SHIELD could possibly influence future policy and understand how requirements arising from existing policies have shaped the requirements on 7SHIELD key results. The report D2.5 Security Requirements is a valuable input to the work being performed for this activity.
7SHIELD partners have participated to several events, reaching several hundred people. The following communities were reached:

- Space agencies
- Satellite owners
- Ground Station operators
- Cyber-security experts

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. EETT is a regulatory initiative in Greece and is very active in similar EU initiatives. 7SHIELD will contribute to relevant sectorial frameworks through the EETT.

IMA3.2 – In this activity we are investigating the current standards and practices being used by operators of ground segments of space systems, security authorities, industry, policy makers, and civil protection across the European Union. In the current reporting period attention has been given to contacting and discussing 7SHIELD with EUSPA and SatCen as well as the European Standards Organizations CEN/CENELEC.
In July 2022 initial contact was made with CEN/CENELEC. On the 19thJuly 2022 a meeting was held with Philip Maurer and Ashok Ganesh where 7SHIELD was presented. A follow-up meeting is planned for September.
Following initial contacts at the ESA Living Planet Symposium a meeting was held with Philippe Rosius, Head of Security Operations and Monitoring on 4th August 2022. A presentation was made to EUSPA. In the discussion held. Two aspects of interest arose. Firstly, GNSS systems are very susceptible jamming (low power signals used) future

developments should take this into account. Note that in 7SHIELD, EETT expertise is being exploited to include it in a completely new scenario at NOA Pilot Use Case. The second aspect was the result of the long planning and development cycles of satellite programmes such as Galileo. The ground segment is designed to meet the needs of the satellites and by will be outdated at delivery or shortly after. Changing circumstances ideally means introducing upgrades during the life of the ground segment. This is not always technically possible. This should be considered in the 7SHIELD framework. I.e upgrades now (performed in the project) but also future upgrades.

Initial contact was made with SatCen 3 August 2022 resulting in a meeting with Omar Barrilero from the RTDI group on 23 August 2022. SatCen expressed interest to attend demonstrations and join the Advisory Board. This was confirmed.15 September 2022.

Future work will now focus on:

1. Interviewing the Pilot Case teams to get insight into the applicable standards they use and if they need changing
2. Hold the planned meeting with CEN/CENELEC to investigate options for directing results of 7SHIELD to standardisation actions
3. Incorporate the results of D2.5 into the analysis of applicable standards to frameworks such as 7SHIELD
4. Contact stakeholders who attended the demonstrations to obtain feedback on the applicability of 7SHIELD to their organisation and potential impact of policy and standardisation
5. Prepare the deliverable D8.12 7SHIELD Security Standardisation Strategy and policy- planning
6. Incorporate the results of the activities of EETT into D8.12

3. Data Management Structure

DMPs are a key element of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by a Horizon 2020 project. As part of making research data findable, accessible, interoperable and re-usable (FAIR), a DMP should include information on:

- The handling of research data during & after the end of the project
- What data will be collected, processed and/or generated
- Which methodology & standards will be applied
- Whether data will be shared/made open access and
- How data will be curated & preserved (including after the end of the project).

A DMP is required for all projects participating in the extended ORD pilot, unless they opt out of the ORD pilot. Due to the Restricted and classified nature of the project, the Consortium has decided to Opt-out of the Commission's Open Research Data Pilot (ORD pilot) before signing the Grant Agreement.

"7SHIELD will cross-cut domains in the protection of critical infrastructure. Data related to each of these domains may be security sensitive and should not be exposed publicly to prevent misuse of the data by potential bad actors trying to subvert the very security systems the project is aiming to put in place. Furthermore, data collected by sensors and other means may expose the range of security systems be commercially sensitive and proprietary to specific installations and not be for general public consumption. That said, 7SHIELD, despite opting out of the open data pilot, will aim to make any non-sensitive data available where appropriate. These opportunities will be monitored within the data management plan."

However, 7SHIELD Consortium has decided to submit a DMP on a voluntary basis[2]. A DMP describes the data management life cycle for all data sets that will be collected, processed or generated by the research project. It is a document that outlines how research data will be handled during a research project, and even after the project is completed, describing which data will be collected, processed or generated and following specific methodologies and standards, whether and how this data will be shared and/or made open, and how it will be curated and preserved. Each dataset that will be generated by the project has to be described in compliance with the five dimensions provided by the EU Commission:

- **Dataset identification and description (reference and name)**: a unique persistent identifier for the data set as well as a description, which specifies the origin, scope, scale, partners and link(s) to the corresponding publications (if any),

[2] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

- **Standards and metadata**: a reference to relevant standards and a description of the metadata schema adopted to describe the data.
- **Data access and sharing**: all the information concerning access and reuse of the dataset including the nature of access (open or restricted), the tools or software needed, the reference and type of the repository where data are stored.
- **Archiving and preservation**: long-term preservation procedures, costs and volume of preserved data.
- **Ethics, privacy and legal requirements:** Any requirements to respect ethical and privacy regulations as well as legal compliance.
- **Storage and backup**: the standards and procedures for storing and backing-up the data, ensuring integrity, access control and security

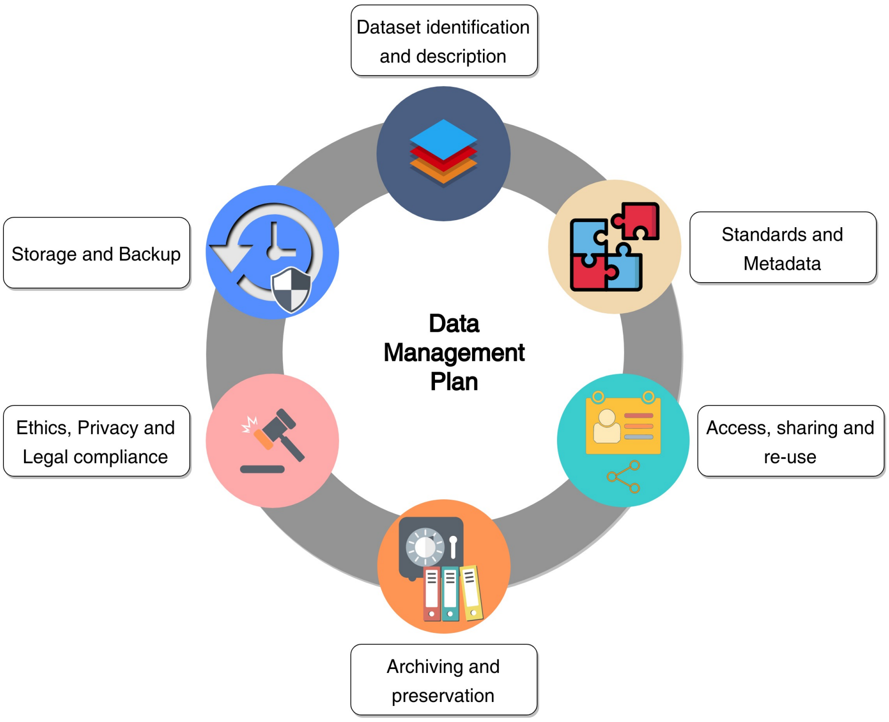

Dataset identification and description
Standards and Metadata
Access, sharing and re-use
Archiving and preservation
Ethics, Privacy and Legal compliance
Storage and Backup
Data Management Plan

Figure 3-2: Data Management Plan Key dimensions

The 7SHIELD DMP has been developed by taking into account the template of the Guidelines on Data Management in Horizon 2020[3]. This document aims to help applicants and beneficiaries of projects to meet their responsibilities with regards to research data quality, sharing and security. In addition to the guidelines provided by the European Commission, this document also refers to the plan to address the ethical issues related to data that will be collected during the project timeframe.

Therefore, the document follows the above structure, with each dimension presented in a dedicated section. Additionally, template for Dataset Management and for the Consent

[3] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

Form are reported in Annex. In Section 4, 7SHIELD Datasets reports each 7SHIELD dataset in detail. Moreover, this DMP is oriented to:

- The consortium partners;
- All stakeholders involved in the project;
- The European Commission.

This document reports the updates related to the objectives' achievements and progresses, the implemented activities to reach the objectives and new sets of data and changes in consortium policies and datasets management.

3.1. 7SHIELD Purposes

The project addresses the security and resilience of EU Ground Segments of Space Systems, meeting the crosscutting and the sectoral criteria of the EU critical infrastructures (2008/14). Due to the growing reliance on satellite communications for today's economy and governments, the ground segments of space systems receive massive amounts of satellite data. A physical/cyber-attack to their installations or communication networks, respectively, would cause debilitating impact on public safety and security of EU citizens and public authorities. A physical attack on a space ground segment makes the distribution of satellite data problematic and, on the other hand, a cyber-attack in its data storage, access and exchange affects not only the reliability of space data, but also their FAIR standards: findability, accessibility, interoperability and reusability.

7SHIELD provides a holistic framework able to confront complex threats by covering all the macro-stages of crisis management, namely pre-crisis, crisis and post-crises phases. Specifically, 7SHIELD framework enables the deployment of innovative services for the cyber–physical protection of ground segments, such as e-fences, passive radars and laser technologies, multimedia AI technologies, that enhance their protection capabilities, while integrating or interoperating with existing protection solutions already deployed at their installations. The project makes use of advanced technologies for data integration, processing, analytics and visualisation as well as data security and cyberthreat protection to assess the prevention, detection and mitigation of threats, both physical and cyber. The project will be evaluated and demonstrated in five installations of ground segments of space systems.

3.2. Data Summary

3.2.1. Purposes of data

The purpose of collection and generation of data throughout the 7SHIELD project is to achieve the main project and to directly support the technical development of 7SHIELD tools or the development of operational processes. 7SHIELD includes a number of technology-oriented WPs (WP3, WP4, WP5 and WP6) that will process both open and closed source data. Moreover, collection and generation of data are necessary to manage the project, disseminate the information about it, analyze and exploit its results.

3.2.2. Data sources

Data will be created within the 7SHIELD project in the work packages in the delivery of the project activities and details of this data is described in the following chapters of this report. The data that will be created with 7SHIELD includes but it not limited to:

- Work packages will produce data as a result of delivering the 7SHIELD outputs.
- Reports and deliverables (internal and external to 7SHIELD) in text, MS Word and other text files,
- Spreadsheets, such as MS XLS (or other),
- MS PowerPoint files (presentations),
- Surveys and questionnaires,
- Multimedia files (such as videos and recordings),
- Specification documents (text),
- Photographs and observation materials,
- Newsletters and promotional material e.g. info sheets, images etc.

The following data sources in the 7SHIELD project can be identified:

- *Questionnaires, surveys and interviews with end-users*: a set of interviews with end-users will be conducted as the part of activities within the tasks T2.1, T2.2, T2.3 and T2.4 in WP2 to investigate specific requirements and needs. Moreover, the project partners were interviewed about the data they generated and collected within the project to prepare this deliverable.
- *Data collected from the field by physical and cyber sensors:* 7SHIELD project will apply different technologies to collect data:
    - <u>UAV equipped with a set of different types of cameras</u> deployed on the field, used both for control and monitoring purposes, as well as allowing the live collection of raw and pre-processed data from all platforms. Moreover, different sensor payloads can be installed on-board the UVs depending on the specific operation needs.
    - <u>Thermal and near-infrared (NIR) cameras</u> are used to detect the presence of intruders, such as moving objects and people, within the boundaries of an area under surveillance. This system is based on a network of near-infrared (NIR) and thermal sensors that support the automated monitoring server.

  - Innovative laser-based detection system is used for detection of ground based and aerial intrusion. Laser- based technology is LIDAR technology (2D and 3D). When an intruder (human or drone) cuts across the laser screen, the intruder is detected and its location information is sent to the control station (a PC), a slaved camera is made to turn onto the intruder, follows its movements and records its locations continuously.
  - Cyber and physical threat intelligence data based on open-source feeds and commercial providers is collected and analysed.
  - A face detection and recognition framework that will process both single shots and video streams from the surveillance cameras is also considered. Face detection and face recognition will be deployed and linked either with a local host database.
  - Wearable sensors using IoT: wearables for the team members using common-off-the-shelf (COTS) components as much as possible and a dedicated terminal to connect the sensors with local IoT communications. Each team member will be a sensor and a same time receptor of the decisions taken. Engagement rules and other hierarchical constraints and pre-operation relevant data should be acquired to improve effectiveness and better support for the operation. Moreover, a connection to the main system of 7SHIELD to acquire data and provide feedback, is capable with à priori information loaded (adding to any that is collected locally) to operate and provide valid outputs.
  - Social media posts and other correspondence focusing on the output of credible voices such as ground space segment operators, civil contingency organisations and other stakeholders.

These technologies have been developed within the WP3, WP4, WP5, WP6 and used in pilots as part of WP7.

Other data sources in the 7SHIELD project have been identified:

- Workshops, demonstrations and piloting in WP7 (T7.3, T7.4 and T7.5). In particular datasets have been produced for each operational tests: PUC2 (Deimos), PUC3 (NOA), PUC 4 (SPACEAPPS), PUC4 (SERCO). For each of these pilots and operation test, the data sets have been collected and compiled in two type documents:
  - A pilot demonstration plan document. For each operational test it contains data sets covering: the pilot test environment, personnel information of the pilot, tools and methods in used in the pilots, scheduling information.
  - A pilot evaluation methodology document. For each operational test this document contains datasets covering the as-run procedure of the tests, the

raw evaluation of the 7SHIELD KRs and the collection of the pilot's users feedback.

- Meetings and stakeholders' engagement in WP8 (T.8.2, T8.3 and T8.4).

The following Table 3-1 summarize the events in which 7SHIELD has participated during the reporting period and the type of participation of partners attending to the event.

During all of the event listed, the intent was to promote as much as possible the 7SHIELD project and build a list of contacts expressing their interest to the project and willing to be updated about its progress throughout newsletters and invitation to the infoday 7SHIELD is going to organize in the final part of the project.

Table 3-1 Events with 7SHIELD participation

Event Title	Event Website	Type of Participation	Start Date	End Date
CERIS Disaster-Resilient Societies (DRS) Event	https://www.cmine.eu/page/ceris	Auditor	23-Mar-22	25-Mar-22
Space 4 Critical Infrastructure - Introduction into the EU-Directive on the resilience of critical entities [WEBINAR]	https://www.nereus-regions.eu/2022/02/24/space-4-critical-infrastructure-introduction-into-the-proposed-eu-directive-on-the-resilience-of-critical-entities-on-29-march-2022-10-00-11-00/#:~:text=Space%204%20Critical%20Infrastructure%20aims,and%20maintenance%20of%20critical%20entities.	Auditor	29-Mar-22	29-Mar-22
EU-HYBNET 2ndAnnual Workshop	https://euhybnet.eu/upcoming-events/eu-hybnet-2nd-annual-workshop-aw/?occurrence=2022-04-06	Speaker	06-Apr-22	06-Apr-22
CYSAT PARIS 2022	https://cysat.eu/	Speaker	06-Apr-22	07-Apr-22
CERIS FCT workshop on protection of public spaces	https://eu.eventscloud.com/website/7438/home-71/	Auditor	07-Apr-22	07-Apr-22

2nd ECSCI workshop on Critical Infrastructure Protection	https://www.finsec-project.eu/ecsci	Speaker	27-Apr-22	29-Apr-22
Security Mission Information & Innovation Group (SMI2G) Workshop 2022	https://www.cmine.eu/events/83839	Poster	16-mag-22	17-mag-22
DroneWISE final conference (ISFP project)	https://dronewise-project.eu/final-conference/	Poster	20-mag-22	20-mag-22
Living Planet Symposium 2022	https://lps22.esa.int/frontend/index.php	Booth, Speaker	23-mag-22	27-mag-22
13th International Conference "days of Corporate Security 2022"	https://www.ics-institut.si/en/events/13th-international-conference-days-of-corporate-security	Speaker	31-mag-22	01-giu-22
11th EU-US-Canada Expert Meeting on Critical Infrastructure Resilience		Speaker	01-giu-22	02-giu-22
FIC (International CyberSecurity Forum)	https://www.forum-fic.com/en/home/	Speaker	07-giu-22	09-giu-22
CIPRE-EXPO - 2022 Critical Infrastructure Protection and Resilience Europe	https://www.cipre-expo.com/	Speaker	14-giu-22	16-giu-22
EU-HYBNET Innovation and Standardisation Workshop	https://euhybnet.eu/upcoming-events/eu-hybnet-standardisation-workshop/	Speaker	15-Jun-22	15-giu-22

37th ECASEC EG of Telecom Security Authorities meeting	https://enisa.europa.eu	Speaker	28-giu-22	28-giu-22
ICONHIC 2022 - 3rd International Conference on Natural Hazards & Infrastructure	https://iconhic.com/2021	Booth, Speaker	05-lug-22	07-lug-22
CERIS INFRA event: "How research supports the directive on the resilience of critical entities?"		Speaker	12-lug-22	12-lug-22
ICECET 2022	http://www.icecet.com/	Speaker	20-Jul-22	22-Jul-22
IEEE International Conference on Cyber Security and Resilience	https://www.ieee-csr.org/	Speaker	27-Jul-22	29-Jul-22

A multimodal data flow will be collected from these data sources. Leveraging innovative techniques for extracting and filtering features and information, only the "relevant" data for the specific 7SHIELD domain will be identified, selected, and processed.

Different datasets will be taken into account:

- Dataset 1: User Requirements
- Dataset 2: Security Requirements
- Dataset 3: Assets Dataset
- Dataset 4: Risk Assessment
- Dataset 5: Secure authentication mechanism dataset management
- Dataset 6: Common Weakness Enumeration
- Dataset 7: Common Vulnerabilities and Exposures
- Dataset 8: Common Attack Pattern Enumeration and Classification
- Dataset 9: CPTI module Twitter dataset
- Dataset 10: Data collection from UAVs and processing at the edge
- Dataset 11: Face detection and face recognition from video surveillance
- Dataset 12: Object detection and activity recognition from video content
- Dataset 13: Cyber-attack detection methods

- Dataset 14: Infrared and thermal image processing for the detection of man-made disasters
- Dataset 15: Laser-based technologies for the detection of ground-based and aerial threat detection
- Dataset 16: Combined Physical and Cyber Threat Detection and Early Warning
- Dataset 17: Semantic Representation
- Dataset 18: Data Severity Level
- Dataset 19: 7SHIELD Space Ground Segment Cyber/Physical dataset
- Dataset 20: Emergency Response Plan
- Dataset 21: Social Awareness
- Dataset 22: Pilot Critical Operation

Each of these has specific type, attributes and dimensions and will be treated in different manner. The general strategy for data management will be based on the identification and classification of data generated and collected, standards and metadata to be used, exploitation and availability of data as well as how the data will be shared and archive to preserve the information.

3.2.3. Types of data

Several types of data are acquired and generated in 7SHIELD. A first classification can be done but, during the project, other types of data not envisaged at this time could be considered and included in the next version of this deliverable:

(i) **Personal data**, which will be used to provide personalized guidelines and 7SHIELD support including profile data and data from end-user/user group activity. Under article 4 of the GDPR[4] the personal data is defined as any information relating to an identified or identifiable natural person (data subject). In turn, the “identifiable natural person” is "anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (e.g. IP addresses) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”[5]. The personal data will be collected and processed within the project under the current EU regulations.

(ii) **Evaluation data and other-not personal-data**, including data used for assuring the functionality of the 7SHIELD solution, data collected during the scenarios and pilot

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[5] GDPR, art. 4.

use cases to assess the evolution of the users, and data from demonstration and evaluation tasks. Different measures will be applied depending on the utilisation of the gathered data.

(iii) **Data collected from the field by physical and cyber sensors**, including data coming from different technologies and sensors (cyber and physical) applied in the project to collect data.

3.3. FAIR data

The European Commission has produced guidelines to ensure that data created through research activities is Findable, Accessible, Interoperable and Reused[6] referred to as FAIR data management.

3.3.1. Making data findable, including provisions for metadata

Data standards are the rules by which data are described and recorded. In order to share, exchange, and understand data, the format as well as the meaning has to be standardized. Standardization can be achieved by subdividing information into two main categories: data values, that are responsible of the result that can be obtained by the analysis of the data, and metadata, that allow users to understand, analyse, synthesize and research the datasets, as well as following and monitoring the progress of the research project. The use of data standards allows agencies to move from "project-based" data files to "enterprise" data files - and vice versa. In other words, the data become usable to more than just the project or person that created the data, because whoever uses the data knows the data will be in an expected format and what it represents. Since datasets will come from distributed and heterogeneous sources, an ontology-based data mapping approach will be designed to characterize these datasets. Each data source will provide metadata that expresses the rules/conditions that each schema realizes.

The metadata for the different identified datasets will be generated either automatically or through manual content annotation. A metadata framework will be used to identify the data types, owners and allowable use. This will be combined with a controlled access mechanism and with efficient encoding and encryption mechanisms. For the considered datasets, no definitive standards have been identified yet, but a set of metadata will be defined in relationship with the own data source.

For this reason, more mature description of metadata used have been provided during the project development, with respect to the needs that could arise and in particular, as part of the work in various WPs related to the development of technical solutions (WP3, WP4, WP5 and WP6), conducting pilots and evaluating their results (WP7) and have been duly reported in this deliverable.

[6] H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, Version 3.0 26 July 2016, available at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

3.3.2. Making data openly accessible

In the context of Research and Development, Open Access typically focuses on access to "scientific information", which refers to two main categories:

- Peer-reviewed scientific research articles (published in academic journals);
- Scientific research data (data underlying publications and/or raw data) [8].

The EU does not impose to researchers the obligation to publish their Results. It is always up to them to decide whether they want to publish some results or not. If researchers decide to proceed with such publication, art. 29 of the GA should be respected. More specifically, Art.29 of the GA foresees that "beneficiary must ensure open access (free of charge online access for any user) to all peer-reviewed scientific publications relating to its results." Therefore, open access becomes an issue only if publication is chosen as a means of dissemination.

At the same time, Open Access does not aim to affect IPRs. The beneficiary has to decide if, when and which Results to disseminate, in a way that does not affect the IP generated by research results and more specifically in a way that will not disrupt the decision to exploit research results commercially, e.g. through patenting. The decision on whether to publish through open access must come after the more general decision on whether to publish directly or to first seek protection for IPRs. This means that the beneficiary will decide the dissemination of the scientific information, having taken into consideration if and how to protect IPRs generated in the lifetime of the Project.

Following the general aim of the EU Open Science policy, Open Access objective is to enable the replicability and/or the uptake of research results by others. The end goal is to enable these research results to be used in an Open Innovation context, thereby speeding up the uptake of innovation with high impact for society. [EARTO Paper: Towards a Balanced Approach Between IPRs and Open Science Policy 31 July 2020, 2.1 Complementarity Between Open Science and IPRs, p.7]

Open Access does not aim to demise or diminish IPRs preventing industry from securing the element of shared "value capture" essential to Open Innovation. IPR remains a key to offer balanced rights to both the users and creators of Open Science content.

7SHIELD recognises the importance of making the research output of the project accessible as widely as possible. To this end, where permitted by the sensitivity of the data, the consortium takes active approach to the open access policy in Horizon 2020 in order to promote diffusion of knowledge and dissemination. More specifically, Open Access i.e. free on-line access, such as the "green[7]" or "gold[8]" model will be provided for the peer-reviewed scientific publications that relate to the project scientific results. Moreover, presentations by project participants about the project and public deliverables will be made publicly available through the project's website and will be posted in a public service like SlideShare. These will all be licensed via a Creative Commons license, like the project documents.

For what concerns data management, some of the collected data, in particular that concerning business-relevant data, organisational data, or personal data, could be sensitive and in this case will not be made available. Therefore, the consortium opts-out from the Pilot on Open Research Data in H2020. The data collected will only be exploited and/or shared/made accessible to project partners with a direct requirement to support their respective piece of work within 7SHIELD. Some data from end-users may not be made available if it is felt that it contains information of sensitive nature which would be unnecessarily disclosed. All data will be anonymised and held with the secure systems of the appropriate partner requiring access to the data. A data minimization policy will be also adopted. The latter implies that no data which is not strictly necessary for running the activity will be collected from individual participants and therefore processed.

7SHIELD framework will provide security policies in order to maintain the integrity of data and to make sure that the data will not be accessible by unauthorized parties or susceptible to corruption of data. In 7SHIELD, a Secure authentication mechanism for data access (T3.2) is designed and developed to support:

- Secure personal data storage in the system backend;
- Secure encrypted personal data search;
- Expressive and advanced access control over encrypted data;
- Secure data integrity verification.

A hybrid encryption mode that merges symmetric encryption, attribute-based encryption, proxy re-encryption and searchable encryption is used in the project. Light-weight hash-based message authentication is considered to achieve the integrity of personal data. Access control mechanisms will be developed for the authentication processes to allow secure data access in a controlled manner. This security level is needed to ensure the data access control to authorized users and entities.

[7] Self-archiving / 'green' open access – the author, or a representative, archives (deposits) the published article or the final peer-reviewed manuscript in an online repository before, at the same time as, or after publication. H2020 "Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020", https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

[8] Open access publishing / 'gold' open access - an article is immediately published in open access mode. In this model, the payment of publication costs is shifted away from subscribing readers. H2020 "Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020", https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

3.3.3. Making data interoperable

Data interoperability is an important aspect of 7SHIELD's data management strategy while it enables to foster collaboration and increase the efficiency of data's use between the partners. Whenever possible, existing, well-defined data-exchange standards will be used.

Moreover, a 7SHIELD ontology will be created, based on the user requirements and standard representations. The metadata will be effectively represented via semantic models, populating the ontological structures, building on top of existing ontologies in the context of H2020 security projects. These structures will build upon already existing standards for semantically representing geospatial, multimedia and user information. The reasoning mechanism will create a cross-modal linking of sources and historical data to increase the completeness and intelligence of the models. Many ontological frameworks have been proposed which are related with the 7SHIELD ontologies: The Semantic Sensor Network (SSN) ontology [3] models sensor devices, systems and procedures; the Time ontology [4] models temporal aspects such as temporal entities, time positions, durations etc. and relations such as before, finishes, during etc.; OGC GeoSPARQL standard [5] models geospatial objects and their topological and geometrical properties. Additionally, more abstract ontologies may be deployed, like e.g. FOAF [6], which connects people and information using the Web, or DOLCE+DnS Ultralite [7] which establishes interoperability among domain-specific ontologies.

3.3.4. Increase data re-use

The datasets, in general, will be stored during the periods necessary for achieving the purposes of its collection and later when it is necessary for the use within the project or later to employ and disseminate the project's results. For sensitive/restricted data access restrictions will be enforced (e.g. by requiring specific credentials, anonymization) while providing the specific data to authorized users only.

3.4. Allocation of resources (Responsibility and Resources)

All research data collected as part of this project and all the results are owned by the beneficiary that generates them. The whole Consortium will take responsibility for the collection, management, storage, security, sharing and quality assurance of the research data. ENG as the leader of T1.5 and of the WP1 that includes the preparation of DMP, have a particular responsibility in creating and updating the DMP. Each 7SHIELD partner has to respect the policies set out in this DMP. Datasets have to be created, managed and stored appropriately and in line with applicable legislation.

3.5. Data security

The 7SHIELD project will involve activities or generate results raising security concerns (in contrast it will contribute to resolve serious security-related challenges), as well as, due to the nature of the topic, i.e. Critical Infrastructures, will generate and handle classified information 'EU-classified information' (EUCI) as foreground.

The classification of the information of this project, according to Security Scrutiny after the proposal evaluation phase and the 7SHIELD GA, is EU-RES[9] (the lowest classification level of 4 levels).

The assessment and the monitoring of these EUCI will be managed from the Security Advisory Board (3 members from three different partners) and the Project Security Officer (chairman of the SAB). In this direction and based on the EU Legislations[10], the SAB & PSO have produced the Project Security Management Plan (an internal document) in order to help the members of the consortium with EUCI.

The PSMP provides a simple but efficient guide for the management of classified information among the partners of the 7SHIELD Project, in order to avoid security breach and support the secure implementation of the project, provides instructions on the protection of Classified Information that are provided or generated on behalf of the 7SHIELD project.

Based on this document, all Consortium Partners are informed on their obligations to deter breaches of security and compromise of Classified Information, by following instructions on the classification of the information, security procedures, including the handling and transfer of Classified Information, and visit procedures for 7SHIELD project.

There are specific rules for producing, accessing, opening, sending, reading, handling, discussing, exchanging, keeping safe/protecting etc the classified information.

For example:

EUCI will only be produced on a "safe" computer (not connected to any network)

The members of the consortium will not discuss EUCI with project partners over the phone or mail or on an unsecure area

EUCI will be stored in a suitable locked office

EUCI will be exchanged only after following a specific procedure (encryption of the information)

More specifically, below the foreseen process on how to exchange EUCI (e.g. in the framework of a deliverable) is presented:

[9] information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

[10] Commission's provisions on security and the rules on security as laid down in Commission Decision 2015/444 of 13 March 2015 on the security rules for protecting EU classified information & Commission Decision (Eu, Eratom) 2019/1962 "Implementing Rules for Handling Restreint UE/EU RESTRICTED information"17-10-2019

1. Deliverable Leader using a safe computer (without any network) in order to encrypt the document using the approved cryptographic software ZED!
2. Using an electronic storage (USB) transfer the encrypted document to a computer with network connection
3. Sending through mail the encrypted document to the partners
4. Sending the password (key) to the partners through SMS
5. Partners receive the encrypted document, transfer the document using an electronic storage to a "safe" computer
6. Partners decrypt the document using the password that have received to their mobile phones via SMS
7. Partners contribute to the specific deliverable and follows the same process to send back their contribution to the deliverable leader, until the final version is ready
8. The final version of the deliverable is reviewed by the SAB and when the security check is completed, the SAB will communicate with the Deliverable Leader in order to send it to the Coordinator.
9. The Coordinator then proceeds to the submission of the deliverable to the EC, following the agreed and appropriate procedures.

Respective procedures are followed also for the production and release of any dissemination material or scientific publications to deter potential data breach.

In order to ensure the efficient EUCI handling by all partners who are being involved with classified information, a training has been provided by the SAB, combined with the PSMP and with the necessary tools, such as the cryptographic software in order to be able to exchange EUCI. Through this process, all the data (EUCI) will be kept safe and not being used for any purpose other than that of carrying out the Grant Agreement.

Last but not least, sensitive information that may not be EUCI but still need to be secured and handled with caution, are foreseen within 7SHIELD activities. These kinds of data will be stored in a secure environment. More specifically, sensitive information needs to be stored in the appropriate infrastructure and format, corresponding to the related requirements and specifications of each pilot. Accessibility to the information needs to be maintained controlled and the networking configuration should not allow data duplication and circulation.

The following security measures will be applied:

- Data generated in the pilots will be stored in each pilot site based on the security measures specified in national legislations and the European General Data Protection Regulation.

- End-users will be requested to fill an informed consent form, which indicates the possible usage of their data.
- Files with personal information, including personal data and data collected from the 7SHIELD tools, will be protected by means of robust encryption schemes.
- Evaluation results of the pilots will be anonymised, applying the appropriate security measures.
- Ethical Committee approval from different pilot site will be sought if necessary.

3.6. Ethics and legal compliance

Given the complexities of data protection law across Europe, a data protection policy in line with relevant EU, national and local policies for the 7SHIELD project will be agreed within the first months of the project, in line with the agreed informed consent and other legal requirements. Finally, all data protection documentation will be centrally held by the project and will therefore be available for audit. Moreover, WP1 will make sure that data collection, management and access throughout and after the project is properly addressed.

All the personal data collected in the project will be processed under the EU's Data Protection laws, where the main legislation is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, also known as the 'General Data Protection Regulation' (GDPR), which entered into force on 25 May 2018.

Further information on how personal data collection and handling should be approached in the 7SHIELD project, as well as other legal and ethical requirements are provided in WP9 and in particular in D9.1.

As explained, the DMP is a living document which will be kept updated during the whole lifetime of the project, since data generation and collection, and therefore data management, will be active in 7SHIELD for a considerable time after the submission of the initial version of the Data Management Plan. Whenever necessary this part of the deliverable will be updated accordingly.

4. 7SHIELD Project datasets

4.1. DATASET 1: User Requirements

Table 4-2 Dataset 1 – User Requirements

Template Field	Description
Overview	
Dataset Name	User requirements
Dataset Category	Primary data collected by partner (NOA) in 7SHIELD
Partner	NOA
Provider (if different from partner)	FMI, DEIMOS, DES, SPACEAPPS, SERCO
Work Package	2
Task/Deliverable	T2.2/D2.2/D2.4
Details	
Short Description	Functional and non-functional user requirements for the 7SHIELD system and its modules, collected from the end-users (satellite ground segment operators) and stakeholders (first responders) of the 7SHIELD Consortium via offline questionnaires in docx format.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The user requirements have been shared with the technical partners responsible for the delivery of the 7SHIELD Key Results and the modules of the integrated system, in order to guide the technical developments and define the specifications of the 7SHIELD architecture as described in deliverable D6.1. The user requirements constitute the core of deliverable *D2.2 Consolidation of Stakeholder Requirements* and its updated version, namely deliverable *D2.4 Use cases and requirements v2.*
Use beyond 7SHIELD	Not foreseen.
Storage and access details	
Is the data open?	No (Classified Information: EU-RESTRICTED)
Available to 7SHIELD partners?	YES (through deliverables D2.2 and D2.4)

Access control	Following handling EUCI procedures (e.g., use of encryption software to exchange and read the report).
What kind of processing is involved?	Processes on EUCI handling, based on Commission Decision 2015/444/EC and the developed PSMP by the SAB in order to support the consortium (e.g., encryption/decryption process through approved software, in order to exchange the classified deliverable between the partners involved).
What kind of derivative data is produced?	No derivative data.
How it becomes accessible to stakeholders outside the consortium?	Only after need-to-know basis and approval by the SAB.
Data flows and views	The user requirements will be reviewed by the 7SHIELD technical partners for the definition of technical specifications of the 7SHIELD system corresponding to each user requirement.
How can be managed after the project?	Only generic data that are not linked to CIs and are not contradictory with the Commission Decision 2015/444/EC and the developed PSMP.
License	Not applicable.
Type and format	.doc and .pdf
Data Size	Less than 5 MB.
Storage location	Partners' PCs
Storing responsible	NOA
Secure storage procedures	Classified information in electronic format will be stored encrypted through ZED! or following any other procedure indicated by the PSMP (e.g., secure room/administrative area for hardcopies).
Metadata	Not applicable.
Ethics and Data Protection	
Dataset contains personal data?	Data: name, surname, job title, expertise, employer. Informed consent was given for use/re-use. Personal data is anonymised.
DPIA required	NO
Dataset ethics and legal requirements	D9.1, Recruitment of participants, Informed Consent. Requirement respected.

4.2. DATASET 2: Security Requirements

Table 4-3 Dataset 2 – Security Requirements

Template Field	Description
Overview	
Dataset Name	Security Requirements
Dataset Category	Primary data collected by partner (KEMEA) in 7SHIELD Synthetic / generated data (Data generated from bibliographic research; Data generated in collaboration with 7SHIELD operators and technical partners regarding the security requirements for their infrastructures and technical components; analysis deriving from processed public data such as papers, documents, standards etc.)
Partner	KEMEA
Provider (if different from partner)	FMI, SPACEAPPS, SERCO, NOA, DEIMOS, 7SHIELD technical partners
Work Package	2
Task/Deliverable	T2.3/D2.5 (input also to D2.3)
Details	
Short Description	A generic list of security requirements and various aspects of security into a hierarchy of concepts based on existing standards, policies, and guidelines elicited through the 7SHIELD project technical solutions and use cases based on structured questionnaires.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The aim of the dataset is to introduce a generic list of security requirements and organize various aspects of security into a hierarchy of concepts based on existing standards, policies, and guidelines elicited through the 7SHIELD project technical solutions and use cases. The consolidated list of these requirements is mapped to specific categories covering cyber and physical security fields such as access control, system development, data protection, etc.
Use beyond 7SHIELD	NONE
Storage and access details	

Is the data open?	No (Classified Information: RESTREINT UE)
Available to 7SHIELD partners?	YES (through D2.4 report)
Access control	EUCI procedures (e.g. usage of encryption software to exchange and read the report)
What kind of processing is involved?	In case, processing of classified information is involved, then processes on EUCI handling, based on Commission Decision 2015/444/EC and the developed PSMP by the SAB in order to support the consortium will be adopted (e.g. encryption/decryption process through approved software, in order to exchange the classified deliverable between the involved partners). Additionally, no technical processing on the collected data has been performed.
What kind of derivative data is produced?	No derivative data.
How it becomes accessible to stakeholders outside the consortium?	Only after need-to-know basis and approval by the SAB
Data flows and views	An appropriate set of security requirements should be defined, based on policies, processes, procedures, organisational structures, software, and hardware functions, that an organisation must follow to ensure its smooth operation and the confidentiality, availability, and integrity of assets from threats and vulnerabilities.
How can be managed after the project?	Only generic data that are not linked to specific CIs and are not contradictory with the Commission Decision 2015/444/EC and the developed PSMP will be used after the project. Security requirements, and the goals that produce them, can be particularly reusable because security needs and countermeasures are common across different domains and independent of many functional attributes and other quality requirements.
License	N.A.
Type and format	.xls, .doc
Data Size	~5mb
Storage location	Partners' PCs and project MS TEAMS
Storing responsible	KEMEA
Secure storage procedures	Classified information in electronic format will be stored encrypted through ZED! or following any other procedure indicated by the PSMP (e.g. secure room/administrative area for hardcopies)

Metadata	N.A.
Ethics and Data Protection	
Dataset contains personal data?	• Deliverable to be submitted in December 2022. Data expected to be collected: name/surname & email. • Informed consent will be given for use/reuse in case dataset contains personal data. So far, no personal data have been contained in the datasets • Personal data will be anonymised.
DPIA required	Data Privacy Impact Assessment Required - NO
Dataset ethics and legal requirements	D9.1, Recruitment of participants, Informed Consent. Requirement respected.

4.3. DATASET 3: Assets Dataset

Table 4-4: Dataset 3 - Assets Dataset

Template Field	Description
Overview	
Dataset Name	Assets Data
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	RESIL and pilot partners
Provider (if different from partner)	n.a.
Work Package	WP3
Task/Deliverable	n.a.
Details	
Short Description	The dataset will contain cyber and physical site assets, the interfaces between them and the messages exchanged.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	Assets data will be included in the model of the site infrastructure in the MBDA and used to evaluate cascading risk; they will be visualized in the 7SHIELD dashboard.
Use beyond 7SHIELD	n.a.

Storage and access details	
Is the data open?	NO
Available to 7SHIELD partners?	YES with restricted access
Access control	SSO credentials
What kind of processing is involved?	n.a
What kind of derivative data is produced?	n.a.
How it becomes accessible to stakeholders outside the consortium?	Not accessible.
Data flows and views	The data will be entered in the system by operators, then will be elaborated by tools.
How can be managed after the project?	n.a.
License	n.a.
Type and format	Ecore XML, JSON
Data Size	n.a
Storage location	RESIL server
Storing responsible	RESIL
Secure storage procedures	VPN, firewall, two factors authentication, secure communication
Metadata	n.a.
Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	n.a.
Dataset ethics and legal requirements	n.a.

4.4. DATASET 4: Risk Assessment

Table 4-5: Dataset 4 - Risk Assessment Dataset Management

Template Field	Description
Overview	
Dataset Name	Risk Assessment Data
Dataset Category	Derived data
Partner	RESIL - STWS
Provider (if different from partner)	n.a.
Work Package	WP3
Task/Deliverable	T3.1, T3.3
Details	
Short Description	The dataset will contain threats and vulnerabilities associated with the pilot infrastructures and the level of risk (likelihood, impact) connected with them.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The dataset will be used to perform analysis, run "what if" scenarios and better plan response and mitigation.
Use beyond 7SHIELD	n.a.
Storage and access details	
Is the data open?	NO
Available to 7SHIELD partners?	YES with restricted access
Access control	The access is regulated by EU legislation
What kind of processing is involved?	n.a
What kind of derivative data is produced?	n.a.
How it becomes accessible to stakeholders outside the consortium?	Not accessible.

Data flows and views	The data will be entered in the system by operators, then will be elaborated by tools. They will be available for planning countermeasures and mitigation.
How can be managed after the project?	n.a.
License	n.a.
Type and format	Ecore XML, CSV
Data Size	n.a
Storage location	RESIL server, STWS server
Storing responsible	RESIL, STWS
Secure storage procedures	VPN, firewall, two factors authentication, secure communication
Metadata	n.a.
Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	n.a.
Dataset ethics and legal requirements	n.a.

4.5. DATASET 5: Secure authentication mechanism Dataset Management

Table 4-6: Dataset 5 - Secure authentication mechanism Dataset Management

Template Field	Description
Overview	
Dataset Name	User information the dataset
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	SERCO/CS/CLS
Provider (if different from partner)	
Work Package	WP3
Task/Deliverable	Task 3.2 Secure authentication mechanism for data access D3.2 Secure authentication mechanism v1 D3.6 Secure authentication mechanism final version

Details	
Short Description	User information, including at least Username, email, and password, have been generated by each of the pilot partners or the technical partners interfacing a module with the SSO function enabled by the secure authentication mechanism.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	User account for login in 7SHIELD modules and GS data access websites
Use beyond 7SHIELD	Identity access management
Storage and access details	
Is the data open?	NO
Available to 7SHIELD partners?	YES (only email and username -passwords are encrypted)
Access control	Credentials
What kind of processing is involved?	N/A
What kind of derivative data is produced?	Access to 7SHIELD modules providing other data (MBDA, DiVA, SPGU, CPTMD, CADF)
How it becomes accessible to stakeholders outside the consortium?	It is not accessible from outside
Data flows and views	Data are manually entered in the system during the user creation, and are manually removed when during user removal and deletion.
How can be managed after the project?	Data will not be maintained at the end of the project
License	N/A
Type and format	A few tens of kilobytes
Data Size	Records
Storage location	OVH Public cloud infrastructure in FRANCE, Strasbourg
Storing responsible	SERCO/CS/CLS

Secure storage procedures	The personal information is protected and all data treatments are compliant to the General Data Protection Regulation (EU) 2016/679 (GDPR). User data will be stored through Oauth2 gateway server which offers availability to encrypt data. To guarantee the confidentiality and the integrity of this data it is also necessary to provide an encryption system. We proposed to use Asymmetric encryption as we need a strong integrity and regarding the time spent to encrypt/decrypt is not significant compared to the need.
Metadata	User Roles, created by and in agreement with the interfaced 7SHIELD modules
Ethics and Data Protection	
Dataset contains personal data?	Email addresses have been provided by partners and they were not informed without any consent form for use. Personal data are not shared outside the 7SHIELD project partners.
DPIA required	Data Privacy Impact Assessment submitted, and the feedback was: "Not assessed as being high risk to data subjects. No Full DPIA required. Website accesses should be separately checked for general compliance re Cookies, Privacy Notices, etc"
Dataset ethics and legal requirements	D9.8 Requirement No.9

4.6. DATASET 6: Common Weakness Enumeration

Table 4-7: Dataset 6 - CWE Dataset Management

Template Field	Description
Overview	
Dataset Name	CWE (Common Weakness Enumeration)
Dataset Category	Publicly available dataset
Partner	RESIL
Provider (if different from partner)	MITRE Corporation

Work Package	3
Task/Deliverable	T3.3
Details	
Short Description	A Community-Developed List of Software & Hardware Weakness Types. It can be downloaded from: https://cwe.mitre.org/data/downloads.html
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	It will be integrated in the MBDA module for associating weaknesses to assets and components of ground segment of space systems
Use beyond 7SHIELD	It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts
Storage and access details	
Is the data open?	Yes – Public;
Available to 7SHIELD partners?	YES
Access control	The dataset can be downloaded in different alternative formats without any need of authentication
What kind of processing is involved?	The dataset is stored in a database and then retrieved for associating weaknesses to blocks and interfaces of a MBDA module's profiles/models
What kind of derivative data is produced?	The list of weaknesses affecting all the components and interfaces of a use case system
How it becomes accessible to stakeholders outside the consortium?	The dataset is already available. The derived data can be exported in a standard format e.g., Ecore XML.
Data flows and views	The dataset is manually downloaded from MITRE website and imported into a database. The database is then accessed by the module to retrieve weaknesses and associate them to system components.
How can be managed after the project?	The dataset is already available. The derived data, i.e., the list of weaknesses affecting all the components and interfaces of a use case system could be made publicly available for dissemination purposes and provided on a website in the form of downloadable Ecore XML.

License	CWE™ is free to use by any organization or individual for any research, development, and/or commercial purposes, per the CWE Terms of Use available at https://cwe.mitre.org/about/termsofuse.html
Type and format	XML, CSV, HTML, PDF
Data Size	10MB
Storage location	Dataset is available at https://cwe.mitre.org/ The downloaded version will be stored on RESIL's servers
Storing responsible	RESIL
Secure storage procedures	VPN, Firewall, two factors authentication, secure communication
Metadata	xsd
Ethics and Data Protection	
Dataset contains personal data?	no
DPIA required	no
Dataset ethics and legal requirements	none

4.7. DATASET 7: Common Vulnerabilities and Exposures

Table 4-8: Dataset 7 - CVE Dataset Management

Template Field	Description
Overview	
Dataset Name	CVE (Common Vulnerabilities and Exposures)
Dataset Category	Publicly available dataset
Partner	RESIL
Provider (if different from partner)	MITRE Corporation
Work Package	3
Task/Deliverable	T3.3
Details	
Short Description	A list of records for publicly known cybersecurity vulnerabilites. It can be downloaded from: https://cve.mitre.org/data/downloads/index.html

Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	It will be integrated in the MBDA module for associating vulnerabilities to assets and components of ground segment of space systems
Use beyond 7SHIELD	Is used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD)
Storage and access details	
Is the data open?	Yes – Public;
Available to 7SHIELD partners?	YES
Access control	The dataset can be downloaded in different alternative formats without any need of authentication
What kind of processing is involved?	The dataset is stored in a database and then retrieved for associating vulnerabilities to blocks and interfaces of a MBDA module's profiles/models
What kind of derivative data is produced?	The list of vulnerabilities affecting all the components and interfaces of a use case system
How it becomes accessible to stakeholders outside the consortium?	The dataset is already available. The derived data can be exported in a standard format e.g., Ecore XML.
Data flows and views	The dataset is manually downloaded from MITRE website and imported into a database. The database is then accessed by the module to retrieve vulnerabilities and associate them to system components.
How can be managed after the project?	The dataset is already available. The derived data, i.e., the list of vulnerabilities affecting all the components and interfaces of a use case system could be made publicly available for dissemination purposes and provided on a website in the form of downloadable Ecore XML.
License	As stated in https://cve.mitre.org/about/termsofuse.html : MITRE grants a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute the CVE®
Type and format	XML, CSV, HTML, Text
Data Size	35MB

Storage location	Dataset is available at: https://cve.mitre.org/data/downloads/index.html The downloaded version will be stored on RESIL's servers
Storing responsible	RESIL
Secure storage procedures	VPN, Firewall, two factors authentication, secure communication
Metadata	xsd
Ethics and Data Protection	
Dataset contains personal data?	no
DPIA required	no
Dataset ethics and legal requirements	none

4.8. DATASET 8: Common Attack Pattern Enumeration and Classification and Exposures

Table 4-9: Dataset 8 - CAPEC Dataset Management

Template Field	Description
Overview	
Dataset Name	CAPEC (Common Attack Pattern Enumeration and Classification)
Dataset Category	Publicly available dataset
Partner	RESIL
Provider (if different from partner)	MITRE Corporation
Work Package	3
Task/Deliverable	T3.3
Details	
Short Description	A publicly available catalogue of common attack patterns https://capec.mitre.org/index.html
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	It will be integrated in the MBDA module for determining possible attack patterns undermining assets and components of ground segment of space systems

Use beyond 7SHIELD	It can be used by analysts, developers, testers, and educators to advance community understanding on how adversaries exploit weaknesses in applications and other cyber-enabled capabilities and enhance defenses.
Storage and access details	
Is the data open?	Yes – Public;
Available to 7SHIELD partners?	YES
Access control	The dataset can be downloaded in different alternative formats without any need of authentication
What kind of processing is involved?	The dataset is stored in a database and then retrieved for determining possible attack patterns undermining components and interfaces of a MBDA module's profiles/models
What kind of derivative data is produced?	The list of attack patterns undermining a use case system
How it becomes accessible to stakeholders outside the consortium?	The dataset is already available. The derived data can be exported in a standard format e.g., Ecore XML.
Data flows and views	The dataset is manually downloaded from MITRE website and imported into a database. The database is then accessed by the module to retrieve attack patterns and associate them to system components.
How can be managed after the project?	The dataset is already available. The derived data, i.e., the list of attack patterns undermining a use case system could be made publicly available for dissemination purposes and provided on a website in the form of downloadable Ecore XML.
License	As stated in https://capec.mitre.org/about/termsofuse.html The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use Common Attack Pattern Enumeration and Classification (CAPEC™) for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.
Type and format	XML, CSV, HTML
Data Size	3MB
Storage location	Dataset is available at: https://capec.mitre.org/data/downloads.html

	The downloaded version will be stored on RESIL's servers
Storing responsible	RESIL
Secure storage procedures	VPN, Firewall, two factors authentication, secure communication
Metadata	xsd
Ethics and Data Protection	
Dataset contains personal data?	no
DPIA required	no
Dataset ethics and legal requirements	none

4.9. DATASET 9: CPTI module Twitter dataset

Table 4-10: Dataset 9 - CPTI module Twitter dataset

Template Field	Description
Overview	
Dataset Name	CyberTweets dataset
Dataset Category	Publicly available dataset
Partner	ENG
Provider (if different from partner)	ENG
Work Package	WP4
Task/Deliverable	T3.4
Details	
Short Description	CyberTweets repository contains the dataset of already annotated tweets as well as the web application used to annotate the tweets.
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	Training of the AI algorithm to detect vulnerabilities in tweets
Use beyond 7SHIELD	Collection of tweets related to cyber vulnerabilities.

Storage and access details	
Is the data open?	Yes – Public;
Available to 7SHIELD partners?	YES
Access control	The dataset is published on github.
What kind of processing is involved?	NA
What kind of derivative data is produced?	NA
How it becomes accessible to stakeholders outside the consortium?	Via official website
Data flows and views	The data are used to compute the distance between a new Tweet and the pre-annotated ones of the dataset.
How can be managed after the project?	The dataset is publicly available.
License	NA
Type and format	mongoDB dump
Data Size	NA
Storage location	https://github.com/behzadanksu/cybertweets
Storing responsible	Github
Secure storage procedures	NA
Metadata	All the metadata are stored in the mongoDB dump.
Ethics and Data Protection	
Dataset contains personal data?	Only the original text of the tweet without any other indication about the users.
DPIA required	Not Required

Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues .

4.10. DATASET 10: Data collection from UAVs and processing at the edge

Table 4-11 Dataset 10 - Data collection from UAVs and processing at the edge

Template Field	Description
Overview	
Dataset Name	UAV Data
Dataset Category	Raw data by sensors or embedded camera
Partner	ACCELI
Provider (if different from partner)	N/A
Work Package	WP4
Task/Deliverable	T4.1 Data collection from UAVs and processing at the edge D4.3 Data collection from UAVs and processing at the edge techniques
Details	
Short Description	The data fusion and object detection/identification algorithms collect data from sensors (e.g. LiDAR, Camera and UAV), fuses them and send the output results to the 7SHIELD C2.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	Will provide alerts in case of a human or other object type intrusion in specific areas. Also, will send videos of inspected areas.
Use beyond 7SHIELD	- To train new object detection/identification algorithms - To train new UAV architectures
Storage and access details	
Is the data open?	TBD
Available to 7SHIELD partners?	YES
Access control	Through 7SHIELD control room or directly through 7SHIELD repository

What kind of processing is involved?	Image processing embedded algorithms provided by CERTH in the framework of the T4.3 task.
What kind of derivative data is produced?	N/A at this stage
How it becomes accessible to stakeholders outside the consortium?	N/A at this stage
Data flows and views	7SHIELD UAV will collect video data through its embedded camera and raw data from the embedded sensors. It will receive notifications and commands from 7SHIELD C2 and it will transmit the outcomes from the edge processing to C2 (JSON Format)
How can be managed after the project?	N/A at this stage
License	N/A at this stage
Type and format	RSTP, XML, JSON, etc.
Data Size	Up to 10 GB.
Storage location	End user sites
Storing responsible	End Users
Secure storage procedures	N/A at this stage
Metadata	N/A at this stage
Ethics and Data Protection	
Dataset contains personal data?	Does the dataset contain personal data, and if YES, which? NO Was informed consent given for use/reuse? YES Is personal data anonymised? YES
DPIA required	Data Privacy Impact Assessment Required / NO
Dataset ethics and legal requirements	N/A at this stage

4.11. DATASET 11: Face detection and face recognition from video surveillance

Table 4-12: Dataset 11 – Labelled Faces in the Wild

Template Field	Description
Overview	
Dataset Name	Labelled Faces in the Wild
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	University of Massachusetts – Computer Vision Lab
Work Package	WP4
Task/Deliverable	T4.2 Face detection and face recognition from video surveillance D4.1 Video surveillance techniques: Initial release D4.5 Video surveillance techniques: Final release
Details	
Short Description	A database of face photographs designed for studying the problem of unconstrained face recognition. The data set contains more than 13,000 images of faces collected from the web.
Existing already before the 7SHIELD project?	Yes
Use in 7SHIELD	Will be used evaluate the face recognition module
Use beyond 7SHIELD	This is a well-known public benchmark for face verification, widely referenced in the related literature. It can be used for research purposes outside the 7SHIELD scope.
Storage and access details	
Is the data open?	Yes
Available to 7SHIELD partners?	Yes, from the original provider.
Access control	The dataset is available to download from the website: http://vis-www.cs.umass.edu/lfw/
What kind of processing is involved?	Facial feature extraction will be performed on the images.

What kind of derivative data is produced?	Facial features will be derived from the dataset images, which will be then used to evaluate the face recognition component. The features and models will exist in the 7SHIELD storage.
How it becomes accessible to stakeholders outside the consortium?	From the original provider.
Data flows and views	The raw data may enter the system as an input to the face recognition module. The raw data will not be forwarded to other modules or system components.
How can be managed after the project?	The dataset will not continue to be stored or managed outside the lifetime of the project.
License	Public Domain
Type and format	JPG images
Data Size	326.7 MB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	The dataset contains personal data of famous celebrities (i.e., photos of their faces). The data will be used for research purposes within the scope of the 7SHIELD project. The dataset was collected from another institution, other than CERTH, and was made publicly available to the web. No formal consent has been requested. The distributor has provided direct access to retrieve all the data through their website using a published download link, without requiring to fill a consent request. The dataset, as distributed originally, includes non-anonymised personal data.
DPIA required	No
Dataset ethics and legal requirements	Legal req.: the photos in the dataset are in the public domain and are free of any copyright restrictions. Proper citation will be added in the project's deliverables in order to credit the creators of the dataset.

	Ethics req.: • Privacy – the photos found in this dataset contain personal identifiers (i.e., faces) of famous people that have consented to the public use of their photograph. If withdrawal of this consent is communicated to the dataset provider, CERTH will also ensure the deletion of the indicated photograph from its training model. • Bias - as mentioned in the dataset's main page, some groups (such as women) are not equally represented in the dataset. CERTH will amend this issue with the use of additional publicly available datasets that will enable the creation of a non-biased face recognition module. • Data minimisation principle - the data to be processed from this database will be strictly necessary for the training of the face recognition module and will not be used for any other purpose. The dataset's processing will be done in accordance with deliverables produced within the context of WP9 – Ethics requirements.
Template Field	Description
Overview	
Dataset Name	Labelled Faces in the Wild
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	University of Massachusetts – Computer Vision Lab
Work Package	WP4
Task/Deliverable	T4.2 Face detection and face recognition from video surveillance D4.1 Video surveillance techniques: Initial release D4.5 Video surveillance techniques: Final release
Details	
Short Description	A database of face photographs designed for studying the problem of unconstrained face recognition. The data set contains more than 13,000 images of faces collected from the web.
Existing already before the 7SHIELD project?	Yes
Use in 7SHIELD	Will be used evaluate the face recognition module

Use beyond 7SHIELD	This is a well-known public benchmark for face verification, widely referenced in the related literature. It can be used for research purposes outside the 7SHIELD scope.
Storage and access details	
Is the data open?	Yes
Available to 7SHIELD partners?	Yes, from the original provider.
Access control	The dataset is available to download from the website: http://vis-www.cs.umass.edu/lfw/
What kind of processing is involved?	Facial feature extraction will be performed on the images.
What kind of derivative data is produced?	Facial features will be derived from the dataset images, which will be then used to evaluate the face recognition component. The features and models will exist in the 7SHIELD storage.
How it becomes accessible to stakeholders outside the consortium?	From the original provider.
Data flows and views	The raw data may enter the system as an input to the face recognition module. The raw data will not be forwarded to other modules or system components.
How can be managed after the project?	The dataset will not continue to be stored or managed outside the lifetime of the project.
License	Public Domain
Type and format	JPG images
Data Size	326.7 MB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	The dataset contains personal data of famous celebrities (i.e., photos of their faces). The data will be used for research purposes within the scope of the 7SHIELD project. The dataset was collected

	from another institution, other than CERTH, and was made publicly available to the web. No formal consent has been requested. The distributor has provided direct access to retrieve all the data through their website using a published download link, without requiring to fill a consent request. The dataset, as distributed originally, includes non-anonymised personal data.
DPIA required	No
Dataset ethics and legal requirements	Legal req.: the photos in the dataset are in the public domain and are free of any copyright restrictions. Proper citation will be added in the project's deliverables in order to credit the creators of the dataset. Ethics req.: • Privacy – the photos found in this dataset contain personal identifiers (i.e., faces) of famous people that have consented to the public use of their photograph. If withdrawal of this consent is communicated to the dataset provider, CERTH will also ensure the deletion of the indicated photograph from its training model. • Bias - as mentioned in the dataset's main page, some groups (such as women) are not equally represented in the dataset. CERTH will amend this issue with the use of additional publicly available datasets that will enable the creation of a non-biased face recognition module. • Data minimisation principle - the data to be processed from this database will be strictly necessary for the training of the face recognition module and will not be used for any other purpose. The dataset's processing will be done in accordance with deliverables produced within the context of WP9 – Ethics requirements.

Table 4-13: Dataset 11 - WIDER Face

Template Field	**Description**
Overview	
Dataset Name	WIDER Face
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	Multimedia Laboratory, Department of Information Engineering, The Chinese University of Hong Kong
Work Package	WP4

Task/Deliverable	T4.2 Face detection and face recognition from video surveillance D4.1 Video surveillance techniques: Initial release D4.5 Video surveillance techniques: Final release
Details	
Short Description	This is a database that contains over 30000 images which mostly show people participating in various activities of everyday life. The human faces appear with a high degree of variability in scale, pose and occlusion.
Existing already before the 7SHIELD project?	Yes
Use in 7SHIELD	Will be used to evaluate the face detection module
Use beyond 7SHIELD	This is a well-known public benchmark for face detection, widely referenced in the related literature. It can be used for research purposes outside the 7SHIELD scope.
Storage and access details	
Is the data open?	Yes
Available to 7SHIELD partners?	Yes, from the original provider.
Access control	The dataset is available to download from the website: http://shuoyang1213.me/WIDERFACE/
What kind of processing is involved?	Facial feature extraction will be performed on the images.
What kind of derivative data is produced?	Facial features will be derived from the dataset images, which will be then used to evaluate the face detection component. The features and models will exist in the 7SHIELD storage.
How it becomes accessible to stakeholders outside the consortium?	From the original provider.
Data flows and views	The raw data may enter the system as an input to the face detection module The raw data will not be forwarded to other modules or system components.
How can be managed after the project?	The dataset will not continue to be stored or managed outside the lifetime of the project.
License	Public Domain
Type and format	JPG images, TXT files

Data Size	3.7 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are additional metadata in the form of bounding box annotations of human faces (pixel coordinates) for every image.
Ethics and Data Protection	
Dataset contains personal data?	The dataset contains personal data (i.e., photos of human faces). The data will be used for research purposes within the scope of the 7SHIELD project. The dataset was collected from another institution, other than CERTH, and was made publicly available to the web. No formal consent has been requested. The distributor has provided direct access to retrieve all the data through their website using a published download link, without requiring to fill a consent request. The dataset, as distributed originally, includes non-anonymised personal data.
DPIA required	No
Dataset ethics and legal requirements	Legal req.: the photos in the dataset are in the public domain and are free of any copyright restrictions. Proper citation will be added in the project's deliverables in order to credit the creators of the dataset. Ethics req.: • Privacy – the photos found in this dataset contain personal identifiers (i.e., faces) of people that have consented to the public use of their photograph. If withdrawal of this consent is communicated to the dataset provider, CERTH will also ensure the deletion of the indicated photograph from its training model. • Data minimisation principle - the data to be processed from this database will be strictly necessary for the training of the face recognition module and will not be used for any other purpose. The dataset's processing will be done in accordance with deliverables produced within the context of WP9 – Ethics requirements.

Table 4-14: Dataset 11 – FDDB

Template Field	**Description**

Overview	
Dataset Name	FDDB
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	University of Massachusetts – Computer Vision Lab
Work Package	WP4
Task/Deliverable	T4.2 Face detection and face recognition from video surveillance D4.1 Video surveillance techniques: Initial release D4.5 Video surveillance techniques: Final release
Details	
Short Description	This is a dataset of face regions designed for studying the problem of unconstrained face detection. This dataset contains the annotations for 5171 faces in a set of 2845 images taken from the Labelled Faces in the Wild dataset.
Existing already before the 7SHIELD project?	Yes
Use in 7SHIELD	Will be used to evaluate the face detection module
Use beyond 7SHIELD	This is a well-known public benchmark for face detection, widely referenced in the related literature. It can be used for research purposes outside the 7SHIELD scope.
Storage and access details	
Is the data open?	Yes
Available to 7SHIELD partners?	Yes, from the original provider.
Access control	The dataset is available to download from the website: http://vis-www.cs.umass.edu/fddb/
What kind of processing is involved?	Facial feature extraction will be performed on the images.
What kind of derivative data is produced?	Facial features will be derived from the dataset images, which will be then used to evaluate the face detection component. The features and models will exist in the 7SHIELD storage.
How it becomes accessible to stakeholders outside the consortium?	From the original provider.

Data flows and views	The raw data may enter the system as an input to the face detection module. The raw data will not be forwarded to other modules or system components.
How can be managed after the project?	The dataset will not continue to be stored or managed outside the lifetime of the project.
License	Public Domain
Type and format	JPG images, TXT files
Data Size	553.7 MB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are additional metadata in the form of bounding box annotations of human faces (pixel coordinates) for every image.
Ethics and Data Protection	
Dataset contains personal data?	The dataset contains personal data (i.e., photos of human faces). The data will be used for research purposes within the scope of the 7SHIELD project. The dataset was collected from another institution, other than CERTH, and was made publicly available to the web. No formal consent has been requested. The distributor has provided direct access to retrieve all the data through their website using a published download link, without requiring to fill a consent request. The dataset, as distributed originally, includes non-anonymised personal data.
DPIA required	No
Dataset ethics and legal requirements	Legal req.: the photos in the dataset are in the public domain and are free of any copyright restrictions. Proper citation will be added in the project's deliverables in order to credit the creators of the dataset. Ethics req.: • Privacy – the photos found in this dataset contain personal identifiers (i.e., faces) of people that have consented to the public use of their photograph. If withdrawal of this consent is communicated to the dataset provider, CERTH will also ensure the deletion of the indicated photograph from its training model.

	- Data minimisation principle - the data to be processed from this database will be strictly necessary for the training of the face recognition module and will not be used for any other purpose. The dataset's processing will be done in accordance with deliverables produced within the context of WP9 – Ethics requirements.

Table 4-15: Dataset 11 – Chokepoint

Template Field	Description
Overview	
Dataset Name	Chokepoint
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	National ICT Australia Limited (NICTA)
Work Package	WP4
Task/Deliverable	T4.2 Face detection and face recognition from video surveillance D4.1 Video surveillance techniques: Initial release D4.5 Video surveillance techniques: Final release
Details	
Short Description	The video dataset was designed for experimental evaluation of person identification/verification under real-world surveillance conditions. It includes footage from an array of three cameras placed above several portals (natural choke points) that capture subjects walking through each portal. The dataset consists of 48 sequencies with a total of 29 subjects.
Existing already before the 7SHIELD project?	Yes
Use in 7SHIELD	Has been used to evaluate the face recognition module
Use beyond 7SHIELD	This is a well-known public benchmark for face recognition, widely referenced in the related literature. It can be used for research purposes outside the 7SHIELD scope.
Storage and access details	
Is the data open?	Yes

Available to 7SHIELD partners?	Yes, from the original provider.
Access control	The dataset is available to download from the website: http://arma.sourceforge.net/chokepoint/
What kind of processing is involved?	Facial feature extraction has been performed on the images.
What kind of derivative data is produced?	Facial features have been derived from the dataset images, which are then used to evaluate the face recognition component. The features and models exist in the 7SHIELD storage.
How it becomes accessible to stakeholders outside the consortium?	From the original provider.
Data flows and views	The raw data may enter the system as an input to the face recognition component. The raw data will not be forwarded to other modules or system components.
How can be managed after the project?	The acquired dataset will not continue to be stored or managed outside the lifetime of the project.
License	Licensed for non-commercial research purposes (http://arma.sourceforge.net/chokepoint/)
Type and format	JPG images, XML files
Data Size	11.7 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are additional metadata in the form of bounding box annotations of human faces (pixel coordinates) for every image.
Ethics and Data Protection	
Dataset contains personal data?	The dataset contains personal data (i.e., photos of human faces). The data will be used for research purposes within the scope of the 7SHIELD project. The dataset was collected from another institution, other than CERTH, and was made publicly available to the web. No formal consent has been requested. The distributor has provided direct access to

	retrieve all the data through their website using a published download link, without requiring to fill a consent request. The dataset, as distributed originally, includes non-anonymised personal data.
DPIA required	No
Dataset ethics and legal requirements	Legal req.: the photos in the dataset are in the public domain and are free of any copyright restrictions. Proper citation will be added in the project's deliverables in order to credit the creators of the dataset. Ethics req.: • Privacy – the photos found in this dataset contain personal identifiers (i.e., faces) of people that have consented to the public use of their photograph. If withdrawal of this consent is communicated to the dataset provider, CERTH will also ensure the deletion of the indicated photograph from its training model. • Data minimisation principle - the data to be processed from this database will be strictly necessary for the training of the face recognition module and will not be used for any other purpose. The dataset's processing will be done in accordance with deliverables produced within the context of WP9 – Ethics requirements.

Table 4-16: Dataset 11 – Gallery of Authorized People

Template Field	Description
Overview	
Dataset Name	Gallery of Authorized People
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	CERTH
Provider (if different from partner)	The End Users will provide the data
Work Package	WP4
Task/Deliverable	T4.2 Face detection and face recognition from video surveillance D4.1 Video surveillance techniques: Initial release D4.5 Video surveillance techniques: Final release
Details	
Short Description	This dataset will be compiled from volunteers which will appear on CCTVs acting as authorized personnel, during the pilot tests of the 7SHIELD project. The gallery will

	contain high resolution photos of their faces from various angles. In addition, videos captured by the pilot owners from the installed cameras will be used to simulate pilot use cases for integration and testing purposes.
Existing already before the 7SHIELD project?	No
Use in 7SHIELD	During the pilot runs, the face detection and recognition module will continuously monitor specific locations covered by CCTV cameras. Real human volunteers will appear on the CCTV streams which will be either authorized personnel or unauthorized people trying to breach in secure locations. The face recognition module will try to match every detected face to an authorized person from the existing gallery using facial feature similarity metrics. If a match cannot be made with a level of certainty an alert indicating potential unauthorized access will be produced.
Use beyond 7SHIELD	The data will not be available to use beyond the lifetime or outside the scope of the 7SHIELD project.
Storage and access details	
Is the data open?	No
Available to 7SHIELD partners?	Available only to CERTH and the end user volunteers
Access control	The data and all derivatives should be stored in 7SHIELD raw data storage. Access credentials should be granted to CERTH and end user volunteers only.
What kind of processing is involved?	Facial feature extraction will be performed on the images.
What kind of derivative data is produced?	Facial features will be derived from the gallery images, which will be then used to match facial features of unknown detected faces.
How it becomes accessible to stakeholders outside the consortium?	Access of the volunteer image gallery will not be granted outside the consortium.
Data flows and views	The gallery of photos will be provided as input to the specific component of the face detection and recognition module which will be responsible for facial feature extraction. As soon as features are extracted, they will be stored on the same storage space with the images, enriching the gallery. The features and/or images will be available for retrieval from the face recognition component

	whenever a feature comparison of an unknown face to the ones existing on the gallery is required.
How can be managed after the project?	The dataset will not continue to be stored or managed outside the lifetime of the project.
License	Proprietary
Type and format	JPG images, MP4 videos
Data Size	max. 10 GB
Storage location	CERTH local (offline) secure data storage devices as well as in operators secure data storage devices
Storing responsible	CERTH and Satellite Ground Segments owners
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	The data will contain personal data (photos of volunteers) Formal consent will be requested from the volunteers upon the use/reuse of their photos for the pilot tests as well as for research purposes. Personal data will not be anonymised.
DPIA required	No
Dataset ethics and legal requirements	Legal req.: All the photos in this dataset will be used within the scope of testing the 7SHIELD face detection and recognition module during the project's pilot runs. The volunteers' photos will be collected and used only after the volunteer's formal consent is given. Ethics req.: • Privacy – the photos in this dataset will contain personal identifiers (i.e., faces) of people that have consented to the use of their photograph within the scope of 7SHIELD pilot testing. • Data minimisation principle - the data to be processed from this database will be strictly necessary for the evaluation of the face recognition module and will not be used for any other purpose. The dataset's processing will be done in accordance with deliverables produced within the context of WP9 – Ethics requirements.

4.12. DATASET 12: Object detection and activity recognition from video content

Table 4-17: Dataset 12 – Microsoft COCO (Common Object in Context) 2017

Template Field	*Description*
Overview	
Dataset Name	Microsoft COCO (Common Object in Context) 2017
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	Microsoft
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release
Details	
Short Description	COCO is a large-scale object detection, segmentation, and captioning dataset. COCO has several features: • Object segmentation • Recognition in context • Superpixel stuff segmentation • 330K images (>200K labeled) • 1.5 million object instances • 80 object categories • 91 stuff categories • 5 captions per image • 250,000 people with keypoints
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	Is used to train the object detection module
Use beyond 7SHIELD	This is a public dataset which contains objects from the person perspective and is widely used in object detection (and other tasks).
Storage and access details	
Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES

Access control	Can be downloaded from the original publisher
What kind of processing is involved?	Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce labels and bounding boxes around object of interest inside images.
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated objects inside will be forwarded to train the module (s). The annotated output of the inference images and or videos will be propagated to the dashboard and any relevant module for demonstration/informative purposes.
How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any output of the module will not be used outside the projects.
License	Annotations are released under the Creative Commons Attribution 4.0 License. Use of the images must abide by the Flickr Terms of Use.
Type and format	Images in jpeg format, annotations in json format
Data Size	The whole dataset ~20.2 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	Yes, it contains.
DPIA required	No
Dataset ethics and legal requirements	N/A

Table 4-18: Dataset 12 – Pascal VOC (Visual Object Classes)

Template Field	Description
Overview	

Dataset Name	Pascal VOC (Visual Object Classes)
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	PASCAL2 Network of Excellence on Pattern Analysis, Statistical Modelling and Computational Learning
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release
Details	
Short Description	Pascal VOC is an object detection dataset containing images from 20 different classes from mostly first person perspective.
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	Will be used to train the object detection module (and possibly activity recognition module)
Use beyond 7SHIELD	This is a public dataset which contains objects from a first person perspective and is widely used in object detection (and other tasks).
Storage and access details	
Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES
Access control	Can be downloaded from the original publisher
What kind of processing is involved?	Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce labels and bounding boxes around object of interest inside images.
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated objects inside will be forwarded to train the module (s). The annotated output of the inference images and or videos will be propagated to the dashboard

	and any relevant module for demonstration/informative purposes.
How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any output of the module will not be used outside the projects.
License	Use of the images must abide by the Flickr Terms of Use.
Type and format	Images in jpeg format, annotations in xml format
Data Size	The whole dataset ~2.9 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	Yes, it contains.
DPIA required	No
Dataset ethics and legal requirements	N/A

Table 4-19: Dataset 12 – VisDrone

Template Field	*Description*
Overview	
Dataset Name	VisDrone
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	AISKYEYE team at Lab of Machine Learning and Data Mining, Tianjin University, China
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release

Details	
Short Description	The benchmark dataset consists of **400** video clips formed by **265,228** frames and **10,209** static images, captured by various drone-mounted cameras, covering a wide range of aspects including location (taken from 14 different cities separated by thousands of kilometres in China), environment (urban and country), objects (pedestrian, vehicles, bicycles, etc.), and density (sparse and crowded scenes). Note that, the dataset was collected using various drone platforms (i.e., drones with different models), in different scenarios, and under various weather and lighting conditions. These frames are manually annotated with more than **2.6 million** bounding boxes or points of targets of frequent interests, such as pedestrians, cars, bicycles, and tricycles. Some important attributes including scene visibility, object class and occlusion, are also provided for better data utilization.
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	Will be used to train the object detection module (and possibly activity recognition module)
Use beyond 7SHIELD	This is a dataset which contain object from UAV perspective and can be used for similar purposes.
Storage and access details	
Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES
Access control	Can be downloaded from the original publisher
What kind of processing is involved?	Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce labels and bounding boxes around object of interest inside images.
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated objects inside will be forwarded to train the module (s). The annotated output of the inference images and or videos will be propagated to the dashboard and any relevant module for demonstration/informative purposes.

How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any output of the module will not be used outside the projects.
License	Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License
Type and format	Images in jpeg format, annotations in text format
Data Size	~1.8 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	It does not contain personal data and efforts have been made to exclude identifiable information from the data to protect privacy.
DPIA required	No
Dataset ethics and legal requirements	N/A

Table 4-20: Dataset 12- UAV123

Template Field	Description
Overview	
Dataset Name	UAV123
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	The Image and Video Understanding Lab (IVUL) at King Abdullah University of Science and Technology (KAUST), Saudi Arabia
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release
Details	

Short Description	UAV123 contains sequences from an aerial viewpoint, a subset of which is meant for long-term aerial tracking (UAV20L). Our new UAV123 dataset contains a total of 123 video sequences and more than 110K frames making it the second-largest object tracking dataset after ALOV300++. All sequences are fully annotated with upright bounding boxes.
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	It is used to train the object detection module.
Use beyond 7SHIELD	This is a dataset which contain object from UAV perspective and can be used for similar purposes.
Storage and access details	
Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES
Access control	Can be downloaded from the original publisher
What kind of processing is involved?	A sampling of frames was used. Additional annotation of all object of interest was produced for the selected frames. Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce labels and bounding boxes around object of interest inside images.
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated objects inside will be forwarded to train the module (s). The annotated output of the inference images and or videos will be propagated to the dashboard and any relevant module for demonstration/informative purposes.
How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any additional annotation produces can be used for object detection purposes.
License	Unknown
Type and format	Images in jpeg format, annotations in text format
Data Size	Complete dataset **~13.7GB**
Storage location	CERTH local server

Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	The dataset has been annotated for object detection purposes. These annotations will be used to train the object detector.
Ethics and Data Protection	
Dataset contains personal data?	It may contain some personal data but it's a public dataset and the publisher owns the right of the images.
DPIA required	No
Dataset ethics and legal requirements	N/A

Table 4-21: Dataset 12 – UCF Aerial Action

Template Field	Description
Overview	
Dataset Name	UCF Aerial Action Data Set
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	Centre For Research in Computer Vision Lab from University of Central Florida (UCF)
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release
Details	
Short Description	This data set features video sequences that were obtained using a R/C-controlled blimp equipped with an HD camera mounted on a gimbal. The collection represents a diverse pool of actions featured at different heights and aerial viewpoints. Multiple instances of each action were recorded at different flying altitudes which ranged from 400-450 feet and were performed by different actors.
Existing already before the 7SHIELD project?	YES

Use in 7SHIELD	It is used to train the object detection module.
Use beyond 7SHIELD	This is a dataset which contain object from UAV perspective and can be used for similar purposes.
Storage and access details	
Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES
Access control	Can be downloaded from the original publisher
What kind of processing is involved?	Frames were extracted from the videos. Annotations were transformed to xml format. Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce labels and bounding boxes around object of interest inside images.
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated objects inside will be forwarded to train the module (s). The annotated output of the inference images and or videos will be propagated to the dashboard and any relevant module for demonstration/informative purposes.
How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any additional annotation produces can be used for object detection purposes.
License	Unknown
Type and format	Videos in mpg format, annotations in VIPER format
Data Size	Final dataset used ~21MB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	The dataset has been annotated for object detection purposes. These annotations will be used to train the object detector.
Ethics and Data Protection	

Dataset contains personal data?	It may contain some personal data but it's a public dataset and the publisher owns the right of the images.
DPIA required	No
Dataset ethics and legal requirements	N/A

Table 4-22: Dataset 12 – VIRAT v1

Template Field	Description
Overview	
Dataset Name	VIRAT v1
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	VIRAT Video Dataset collection
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release
Details	
Short Description	The VIRAT Video Dataset is designed to be realistic, natural and challenging for video surveillance domains in terms of its resolution, background clutter, diversity in scenes, and human activity/event categories than existing action recognition datasets. It has become a benchmark dataset for the computer vision community. Ground and Aerial Videos: Both ground camera videos and aerial videos are collected released as part of VIRAT Video Dataset.
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	It is used to train the activity recognition module.
Use beyond 7SHIELD	This is a public dataset which contains objects from a first person perspective and is widely used in activity recognition and detection.
Storage and access details	

Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES
Access control	Can be acquired from the original publisher
What kind of processing is involved?	Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce labels for video segments.
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated video segments will be used to train the module. The annotated output of the inference videos will be propagated to the dashboard and any relevant module for demonstration/informative purposes.
How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any output of the module will not be used outside the projects.
License	The V1 data is governed by the VIRAT Video Dataset Usage Agreement. The V1-training annotations are released CC-BY 4.0. DIVA M1 pilot collect dataset by Kitware Inc. is licensed under a Creative Commons Attribution 4.0 International License
Type and format	Images extracted in png format, videos in mp4 format, annotations in yml format
Data Size	The mp4 and annotations files ~52 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	Yes, it contains.
DPIA required	No
Dataset ethics and legal requirements	N/A

Table 4-23: Dataset 12 – CHARADES

Template Field	Description
Overview	
Dataset Name	CHARADES
Dataset Category	Publicly available dataset
Partner	CERTH
Provider (if different from partner)	VIRAT Video Dataset collection
Work Package	WP4
Task/Deliverable	T4.3 Object detection and activity recognition from video content D4.1 - Video surveillance techniques: Initial release D4.5 - Video Surveillance Techniques Final Release
Details	
Short Description	Charades is dataset composed of 9848 videos of daily indoors activities collected through Amazon Mechanical Turk. 267 different users were presented with a sentence, that includes objects and actions from a fixed vocabulary, and they recorded a video acting out the sentence. The dataset contains 66,500 temporal annotations for 157 action classes, 41,104 labels for 46 object classes, and 27,847 textual descriptions of the videos.
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	Will be used to train the activity recognition module.
Use beyond 7SHIELD	This is a public dataset which contains objects from a first person perspective and is widely used activity recognition.
Storage and access details	
Is the data open?	Yes – Public
Available to 7SHIELD partners?	YES
Access control	Can be acquired from the original publisher
What kind of processing is involved?	Deep learning network processing which will involve image classification and regression as outputs.
What kind of derivative data is produced?	A deep network model which will produce **labels for video segments.**

How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	Images with annotated video segments will be used to train the module. The annotated output of the inference videos will be propagated to the dashboard and any relevant module for demonstration/informative purposes.
How can be managed after the project?	The original dataset is publicly available so it will exist after the project life circle end. Any output of the module will not be used outside the projects.
License	License for Non-Commercial Use
Type and format	videos in mp4 format, annotations in csv format
Data Size	Original size ~55 GB
Storage location	CERTH local server
Storing responsible	CERTH
Secure storage procedures	The local sever is protected by the CERTH firewall. No direct access points will be created to access these data.
Metadata	There are no additional metadata.
Ethics and Data Protection	
Dataset contains personal data?	Yes, it contains.
DPIA required	No
Dataset ethics and legal requirements	N/A

4.13. DATASET 13: Cyber-attack detection methods

Table 4-24: Dataset 13 - DDoS Evaluation Dataset (CIC-DDoS2019)

Template Field	Description
Overview	
Dataset Name	DDoS Evaluation Dataset (CIC-DDoS2019)
Dataset Category	Publicly available dataset
Partner	CeRICT
Provider (if different from partner)	Canadian Institute for Cybersecurity

Work Package	WP4
Task/Deliverable	T4.4 - Cyber-attack detection methods D4.4 - Cyber-attack detection methods
Details	
Short Description	CICDDoS2019 contains benign and the most up-to-date common DDoS attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter-V3 with labelled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files).
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	the dataset will be used to test the detection of network patterns in order to trigger alerts and alarms
Use beyond 7SHIELD	The dataset can be used via AI techniques for analysis. A different feature extractor can be used, using raw scanned files (PCAP) to extract features. Data mining techniques can be used to analyse the generated data.
Storage and access details	
Is the data open?	YES
Available to 7SHIELD partners?	Yes, from the original provider
Access control	Can be downloaded from the provider website
What kind of processing is involved?	attack pattern detection using pre-set rules and information correlation
What kind of derivative data is produced?	Alerts and alarms deriving from the detection
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	The dataset will be processed by the cyber-attack detection module and possibly by the cyber-attack correlation solution to be displayed as alerts and alarms
How can be managed after the project?	The dataset is public and will continue to exist even after the end of the project

License	Any use or redistribution of the data must include a citation to the CICDDoS2019 dataset and related published paper.
Type and format	Raw data network traffic (Pcaps) and event logs. Several features were then extracted from raw data and saved in CSV.
Data Size	2.2 Gb
Storage location	CeRICT local server
Storing responsible	CeRICT
Secure storage procedures	N/A at this stage
Metadata	N/A at this stage
Ethics and Data Protection	
Dataset contains personal data?	NO
DPIA required	NO
Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues

Table 4-25: Dataset 13 - ISOT Ransomware Dataset

Template Field	Description
Overview	
Dataset Name	ISOT Ransomware Dataset
Dataset Category	Publicly available dataset
Partner	CeRICT
Provider (if different from partner)	ISOT Research Lab
Work Package	WP4
Task/Deliverable	T4.4 - Cyber-attack detection methods D4.4 - Cyber-attack detection methods
Details	
Short Description	ISOT ransomware dataset is a combination of the behaviour data for a collection of ransomware samples and benign applications.

Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	The dataset is used to detect changes to data due to the effect of ransomware, in order to improve detection
Use beyond 7SHIELD	The dataset is public and can be used for research purposes
Storage and access details	
Is the data open?	YES
Available to 7SHIELD partners?	Yes, from the original provider
Access control	Can be downloaded from the provider website
What kind of processing is involved?	attack pattern detection using pre-set rules and information correlation
What kind of derivative data is produced?	Alerts and alarms deriving from the detection
How it becomes accessible to stakeholders outside the consortium?	From the original provider
Data flows and views	The dataset will be processed by the cyber-attack detection module and possibly by the cyber-attack correlation solution to be displayed as alerts and alarms
How can be managed after the project?	The dataset is public and will continue to exist even after the end of the project
License	The dataset should be used for research purposes only. The dataset must not be passed on to other researchers without the explicit permission of Dr. Issa Traore. The source of the dataset must be indicated in any publications by means of a citation.
Type and format	Network dump of the traffic (pcap) memory dump of the analysis machine (dmp) Meta information about all processes that touched the file, its original file path in the analysis machine, etc. (.json) raw logs (.bson)
Data Size	420 GB
Storage location	CeRICT local server
Storing responsible	CeRICT
Secure storage procedures	N/A at this stage

Metadata	N/A at this stage
Ethics and Data Protection	
Dataset contains personal data?	NO
DPIA required	NO
Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues

4.14. DATASET 14: Infrared and thermal image processing for the detection of man-made disasters

Table 4-26: Dataset 14 - Thermal images with vehicles, people and large animals

Template Field	Description
Overview	
Dataset Name	Thermal images with vehicles, people and large animals
Dataset Category	Publicly/Private available dataset
Partner	INOV
Provider (if different from partner)	FLIR for annotated vehicle and people images and YouTube for large animal images
Work Package	WP4
Task/Deliverable	T4.5 Infrared and thermal image processing for the detection of man-made disasters D4.6 Infrared and thermal image processing techniques
Details	
Short Description	The dataset consists of thermal images containing vehicles, people and large animals. It was collected by FLIR by driving around in a car and collecting images from what was seen. The large animals are collected from YouTube videos posted by several different authors, included also images generated by INOV during the project. All images are annotated for the presence of objects of the classes to be identified in the images.
Existing already before the 7SHIELD project?	YES (FLIR images), No (Large animals' data persons and vehicles)
Use in 7SHIELD	To create deep learning neural networks for detection of vehicles, people and large animals.

Use beyond 7SHIELD	For the same purpose
Storage and access details	
Is the data open?	Yes – Public (for the data set FLIR images) No (for the images generated by INOV during project)
Available to 7SHIELD partners?	YES
Access control	Open access (FLIR data and large animal data)
What kind of processing is involved?	The images are annotated to have the position of the objects from the classes to discriminate. The FLIR dataset was already annotated but the images from YouTube and images generated by INoV during the project are annotated by INOV.
What kind of derivative data is produced?	YouTube annotated images for large animals and INOV generated data.
How it becomes accessible to stakeholders outside the consortium?	The data is mostly available at FLIR site. Remaining data will be available in place yet to be defined.
Data flows and views	The data is used to train, validate and test the networks, it is not used once a neural network is created.
How can be managed after the project?	FLIR dataset is public. Annotated large animals' data is licensed. It is used for deep learning models creation. Where it will be available is yet to be defined.
License	Proprietary for large animals' data.
Type and format	JPEG, JSON, TXT
Data Size	Approximately 30 GB of data.
Storage location	Project Git
Storing responsible	INOV
Secure storage procedures	INOV's data-centre procedures for backup.
Metadata	Image annotations
Ethics and Data Protection	
Dataset contains personal data?	No. Even though people and vehicles are filmed, the faces and license plates were blurred.
DPIA required	Not Required
Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues

4.15. DATASET 15: Laser-based technologies for the detection of ground-based and aerial threat detection

Table 4-27: Dataset 15 – Coordinates of the detected intruder

Template Field	Description
Overview	
Dataset Name	Coordinates of the detected intruder
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	DFSL
Provider (if different from partner)	NA
Work Package	WP4
Task/Deliverable	T4.6 Laser-based technologies for the detection of ground-based and aerial threat detection D4.2 Combined Physical and Cyber Threat detection D4.7 Combined Physical and Cyber Threat detection and correlation
Details	
Short Description	Coordinates (Range, Azimuth) of ground-based intruders, Coordinates (Range, Azimuth, Elevation) of aerial intruder drones; using Laser Based Technologies
Existing already before the 7SHIELD project?	YES
Use in 7SHIELD	Will be shared with 7SHIELD platform via JSON through message broker to 7SHIELD Platform for decision making
Use beyond 7SHIELD	NIL
Storage and access details	
Is the data open?	Yes – but restricted access,
Available to 7SHIELD partners?	YES
Access control	Via JSON
What kind of processing is involved?	NA
What kind of derivative data is produced?	NIL

How it becomes accessible to stakeholders outside the consortium?	NA
Data flows and views	Enters into 7SHIELD Platform via JSON through message broker
How can be managed after the project?	NA
License	NIL
Type and format	JSON
Data Size	Can be recorded, Less than 2 GB,
Storage location	Not on DFSL systems
Storing responsible	NA
Secure storage procedures	NA
Metadata	NA
Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	No
Dataset ethics and legal requirements	NA

4.16. DATASET 16: Combined Physical and Cyber Threat Detection and Early Warning

Table 4-28: Dataset 16 – SPGU

Template Field	Description
Overview	
Dataset Name	SPGU dataset
Dataset Category	Private / Public Dataset
Partner	ENG
Provider (if different from partner)	-
Work Package	WP4

Task/Deliverable	D4.7
Details	
Short Description	The dataset consists mainly of two sets. One dataset describes the Situational Picture and all the events connected to it and another dataset contains all the data describing assets and areas.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The data relating to the assets / areas are data that are recovered from third-party systems and persisted in the system to be recovered via the rest API from CPTMD. The data relating to the SP and all the events related to it are data exchanged through the bus (broker) which are collected by detectors and correlators but are exposed (again through the broker) to third-party systems so that the systems can communicate with each other. and can keep themselves aligned.
Use beyond 7SHIELD	-
Storage and access details	
Is the data open?	YES - The data has restricted access through certificate authentication.
Available to 7SHIELD partners?	YES - Just to those who need access.
Access control	The data on the assets can be accessed only through SSO credentials, instead the data relating to the situational picture can be accessed either through SSO (through rest services) or through the bus (broker) with x509 certificates.
What kind of processing is involved?	Data collecting and data transformation to collect data from all detectors / correlator and expose it on broker / rest API services.
What kind of derivative data is produced?	Properly formatted data is generated (e.g. GPS coordinates with CRS EPSG: 4326) and conventional formats containing an agreed name mapping to allow communication with external systems as well as allowing the dashboard (FE) to retrieve the data as expected.
How it becomes accessible to stakeholders outside the consortium?	Need to be specified.
Data flows and views	The data is captured from the bus and is collected and persisted to update the situational picture. They are then

	exposed on demand from the dashboard or a system update message is published following certain criteria.
How can be managed after the project?	Need to be specified.
License	Proprietary, Apache License 2.0, **GPL**
Type and format	JSON
Data Size	Max ~5MB per message
Storage location	PostGIS
Storing responsible	ENG
Secure storage procedures	Basic authentication (username / password)
Metadata	Any metadata standards used in the dataset. What metadata has been created and how is this managed
Ethics and Data Protection	
Dataset contains personal data?	NO
DPIA required	-
Dataset ethics and legal requirements	The ethical issues related to the 7SHIELD project will be described in WP9.

Table 4-29: Dataset 16 - Cyber, Physical and Availability UAF alerts

Template Field	Description
Overview	
Dataset Name	Cyber, Physical and Availability UAF alerts
Dataset Category	Derived data
Partner	CSNov
Provider (if different from partner)	Cyber: CeRICT Physical: STWS Availability: CSNov

Work Package	WP4
Task/Deliverable	T4.7 Combined Physical and Cyber Threat Detection and Early Warning D4.2 - Combined Physical and Cyber Threat detection D4.7 - Combined Physical and Cyber Threat detection and correlation
Details	
Short Description	The dataset consists of UAF alerts from three different sources: - Cyber UAF alerts for Cyber detection - Physical UAF alerts for Physical detection - Availability UAF alerts for Availability detection These three sources are correlators in their specific domain.
Existing already before the 7SHIELD project?	No
Use in 7SHIELD	To create combined and correlated UAF alerts.
Use beyond 7SHIELD	For the same purpose
Storage and access details	Stored in 7SHIELD storage module
Is the data open?	No
Available to 7SHIELD partners?	YES, but under EU RESTRICTED mark
Access control	Authorized only 7SHIELD partners and end users
What kind of processing is involved?	The metadata of each UAF alerts are correlated together. The aim is to correlate one type of alert (example Cyber Alert) with another type (example: Physical alert) to identify combined attack scenarios/incidents.
What kind of derivative data is produced?	A new UAF alert which reference the correlated alerts
How it becomes accessible to stakeholders outside the consortium?	Not accessible. RESTRICITED alerts
Data flows and views	The data came from 7SHIELD correlators. The data is used to be correlated. The result is showed to the end user.
How can be managed after the project?	To be defined
License	Proprietary 7SHIELD
Type and format	UAF serialized in JSON

Data Size	Few Gigabytes
Storage location	Where 7SHIELD is deployed (on premise)
Storing responsible	TBD
Secure storage procedures	7SHIELD defined procedure
Metadata	Security alerts
Ethics and Data Protection	
Dataset contains personal data?	Final UAF alerts on a 7SHIELD deployment can contain personal data
DPIA required	Not Required
Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues

Table 4-30: Dataset 16 – Physical UAF alerts

Template Field	Description
Overview	
Dataset Name	Physical UAF alerts
Dataset Category	Derived data
Partner	STWS
Provider (if different from partner)	- UAV data: ACCELI - Face detection and face recognition from video surveillance: CERTH - Object detection and activity recognition from video content: CERTH - Infrared and thermal image processing for the detection of man-made disasters: INOV - Laser-based technologies for the detection of ground-based and aerial threat detection: DFSL
Work Package	WP4
Task/Deliverable	T4.7 Combined Physical and Cyber Threat Detection and Early Warning D4.2 - Combined Physical and Cyber Threat detection D4.7 - Combined Physical and Cyber Threat detection and correlation
Details	

Short Description	The component will correlate the physical events detected by sensors on the field. The result of this correlation process is a dataset consisting of the related UAF alerts.
Existing already before the 7SHIELD project?	No
Use in 7SHIELD	The dataset will contain the correlation of the physical events detected by the sensors on the field. Each correlation will be represented as an alert. These alerts will be disseminated to the rest 7SHIELD components, for further analysis.
Use beyond 7SHIELD	For the same purpose
Storage and access details	Stored in 7SHIELD storage module
Is the data open?	No
Available to 7SHIELD partners?	YES, but under EU RESTRICTED mark
Access control	Authorized only 7SHIELD partners and end users
What kind of processing is involved?	The physical sensors (UAV, cameras etc) on the field will survey the area, searching for unusual and critical situations. The detected events will be combined and correlated, producing actionable information that will be useful for the rest components. The dataset will be consisted by that actionable information.
What kind of derivative data is produced?	A new UAF alert that references the correlated physical events.
How it becomes accessible to stakeholders outside the consortium?	Not accessible. RESTRICITED alerts
Data flows and views	The data came from 7SHIELD physical sensors on the field. The physical events will be correlated. The correlated alerts will be disseminated to the rest 7SHIELD components for further analysis.
How can be managed after the project?	To be defined
License	Proprietary 7SHIELD
Type and format	UAF serialized in JSON
Data Size	Few megabytes
Storage location	The same as the main 7SHIELD platform.
Storing responsible	-

Secure storage procedures	7SHIELD defined procedure
Metadata	-
Ethics and Data Protection	
Dataset contains personal data?	No. The dataset contains the correlation among the different physical events. The dataset will contain only the information that is related to the correlation. The real physical events will be stored on the resalted sensors datasets. So, it is agnostic to the personal data that each physical event may contain.
DPIA required	Not Required
Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues

4.17. DATASET 17: Semantic Representation

Table 4-31: Dataset 17 – Semantic Representation

Template Field	Description
Overview	
Dataset Name	Semantic Representation
Dataset Category	Metadata
Partner	CERTH
Provider (if different from partner)	-
Work Package	WP5 Post-Crisis management for response and mitigation of physical and cyber threats
Task/Deliverable	Task 5.1 Semantic representation and linking for decision-making
Details	
Short Description	The dataset will contain the semantic representation of the annotations that are generated by the various 7SHIELD modules. The vocabulary follows the ontology that will be developed in the T5.1
Existing already before the 7SHIELD project?	No
Use in 7SHIELD	This dataset will be used in order to map the incoming data into 7SHIELD KB and to develop the reasoning mechanism
Use beyond 7SHIELD	The ontologies that will be developed with the use of this dataset will be available for further use in other projects in this domain of interest
Storage and access details	
Is the data open?	With restricted access
Available to 7SHIELD partners?	If it's necessary for their services
Access control	The dataset will be stored in 7SHIELD's KB repository. Only authorized users can have access to it.

What kind of processing is involved?	Input data from other 7SHIELD modules (JSON) will be formulated into RDF triples and stored in a native RDF triple store.
What kind of derivative data is produced?	The derivative data will help with the formulation of the 7SHIELD knowledge base.
How it becomes accessible to stakeholders outside the consortium?	Need to be specified
Data flows and views	The data are uploaded to the KB in order to upgrade it with new knowledge.
How can be managed after the project?	Need to be specified
License	Apache v2.0
Type and format	RDF
Data Size	Need to be specified
Storage location	Triple Store: GraphDB
Storing responsible	CERTH
Secure storage procedures	Basic local authentication (username/password)
Metadata	-
Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	No
Dataset ethics and legal requirements	The ethical issues related to the 7SHIELD project will be described in WP9.

4.18. DATASET 18: Data Severity Level

Table 4-32: Dataset 18 – Data Severity Level

Template Field	Description
Overview	
Dataset Name	Data Severity Level
Dataset Category	Derived data (e.g., output from processing by 7SHIELD module)
Partner	CERTH
Provider (if different from partner)	7SHIELD modules: • Situational Picture Generation and Update (SPGU) • 7SHIELD Knowledge Base • Tactical Decision Support System
Work Package	WP5 Post-Crisis management for response and mitigation of physical and cyber threats
Task/Deliverable	T5.3 Security Risk Assessment Algorithms for Decision Support (KR13 Crisis classification module)

Details	
Short Description	This dataset encapsulates characteristics that are derived from the outcome processes of other 7SHIELD modules. In particular, features that describe the current situational picture, semantically information that is stored in Knowledge Base, and other information from the field obtained from TDSS are integrated.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The Crisis Classification module will use this dataset in order to assess the current severity level of the ongoing crisis event.
Use beyond 7SHIELD	Need to be specified
Storage and access details	
Is the data open?	Yes – but restricted access
Available to 7SHIELD partners?	Yes, by Integrated Command Control and Coordination System
Access control	The dataset will be stored in 7SHIELD's data storage repository. Only authorised users can have access to it.
What kind of processing is involved?	The dataset will be annotated in terms of the severity level. The annotated dataset will be used to train a machine learning model enabled to assess the severity level of a crisis event.
What kind of derivative data is produced?	The derivative data present the severity level of a crisis. It will comply with Common Alerting Protocol (CAP) severity code values: • "Extreme" - Extraordinary threat • "Severe" - Significant threat • "Moderate" - Possible threat • "Minor" – Minimal to no known threat • "Unknown" - Severity unknown
How it becomes accessible to stakeholders outside the consortium?	Need to be specified
Data flows and views	The dataset is used in order to train and test (evaluate) a machine learning model which will be enabled to assess the severity level of a P/C crisis.
How can be managed after the project?	Need to be specified

License	Creative commons The algorithmic part is public. However, in case this module needs to process and analyse EU RES input, then the output will be of type EU RES too
Type and format	CSV or JSON, need to be specified
Data Size	Depends on the frequency that generated data will be obtained from the 7SHIELD ecosystem. However, a rough estimation could be less than 100 MB.
Storage location	Need to be defined
Storing responsible	Need to be defined
Secure storage procedures	It will be stored in the project repository which is hosted in a server of the project coordinator's IT infrastructure. The repository supports version control which should be enough to ensure data recovery in case of accidental deletions. Data back-ups will be done according to the internal IT policy of the project coordinator as applicable to all other relevant digital data of the company. Access to the data will only be possible through authenticated access to the repository.
Metadata	Metadata standards would be determined in the 7SHIELD project
Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	No
Dataset ethics and legal requirements	The ethical issues related to the 7SHIELD project will be described in WP9 deliverables.

4.19. DATASET 19: 7SHIELD Space Ground Segment Cyber / Physical Dataset

Table 4-33: Dataset 19 – 7SHIELD Space Ground Segment Cyber / Physical Dataset

Template Field	Description
Overview	
Dataset Name	7SHIELD Space Ground Segment Cyber / Physical Dataset
Dataset Category	Secondary (derived) data not publicly available
Partner	CERTH

Provider (if different from partner)	Created by Satellite Ground Segment operators and CERTH
Work Package	5
Task/Deliverable	5.3
Details	
Short Description	The dataset was collected using "Annotation Tool", a web application developed in order to enable the experts from each pilot site to quickly annotate random generated C/P attack scenarios with pilot specific parameters. Each scenario is classified concerning the severity level of a potential crisis.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The data were used as a training and testing dataset for the Machine Learning algorithms developed for the Crisis Classification module (task 5.3)
Use beyond 7SHIELD	No foreseeable future use for the data collected since they are specific to the 7SHIELD pilot sites
Storage and access details	
Is the data open?	NO
Available to 7SHIELD partners?	NO, only to Satellite Ground Segment operators (members of the consortium)
Access control	The data are stored in a MongoDB database and in order to gain access an account with credentials is needed
What kind of processing is involved?	In order to generate the "Severity level" of each random generated attack scenario described in the data, the two inputs of the end users, "Potential Consequences" and "Likelihood" were processed using a custom Risk Matrix
What kind of derivative data is produced?	The Severity Level (Low, Medium, High, Very High) of a potential P/C attack derived by the analysis of detected items (attributes)
How it becomes accessible to stakeholders outside the consortium?	The access is not permitted to stakeholders outside the consortium
Data flows and views	Data is only used for the training of the Machine Learning algorithms used by Crisis Classification module, so it can't be seen in the system

How can be managed after the project?	N/A
License	Proprietary
Type and format	XML
Data Size	Depends on the number of annotated C/P hypothetical attack scenarios (order few MBs)
Storage location	MongoDB
Storing responsible	CERTH
Secure storage procedures	Network encryption available with MongoDB allows the protection of the database through an industry-standard encryption methodology
Metadata	No Metadata created since the data that were used are restricted
Ethics and Data Protection	
Dataset contains personal data?	NO
DPIA required	Not Required
Dataset ethics and legal requirements	The dataset does not raise any ethical or legal issues

4.20. DATASET 20: Emergency Response Plan

Table 4-34: Dataset 20 – Emergency Response Plan

Template Field	Description
Overview	
Dataset Name	Emergency Response Plan
Dataset Category	Primary data collected by partner (KEMEA) in 7SHIELD Synthetic / generated data (Data generated from bibliographic research; Data generated in collaboration with 7SHIELD operators regarding the actions to be taken while handling an incident; analysis deriving from processed public data such as papers, documents, standards etc.)
Partner	KEMEA
Provider (if different from partner)	FMI, SPACEAPPS, SERCO, NOA, DEIMOS, HP
Work Package	5
Task/Deliverable	T5.4/D5.7
Details	

Short Description	Answers retrieved from questionnaires distributed to the 7SHIELD operators and stakeholders alongside with relevant stakeholders' interviews (i.e. operators' security department, third party companies involved in security, Police, technical teams, building managers, etc.). The data collected is relevant to the general and local regulations per each 7SHIELD Ground Segment Pilot site as well as the best practices and methodologies followed while handling an incident.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	To draft a generic Emergency Response Plan (ERPs) and further adapt it per Pilot Site, tailored to the specific needs of each scenario per pilot site as developed in Task 2.1. The ERPs are visualized to the end-users though the STWS Engage platform providing several functionalities for the management of the ERP to them.
Use beyond 7SHIELD	NONE
Storage and access details	
Is the data open?	No (Classified Information: RESTREINT UE)
Available to 7SHIELD partners?	YES (the D5.7 report)
Access control	EUCI procedures (e.g. usage of encryption software to exchange and read the report)
What kind of processing is involved?	In case processing of classified information is involved, then processes on EUCI handling, based on Commission Decision 2015/444/EC and the developed PSMP by the SAB in order to support the consortium (e.g. encryption/decryption process through approved software, in order to exchange the classified deliverable between the involved partners). Additionally, no technical processing on the collected data has been performed.
What kind of derivative data is produced?	No derivative data.
How it becomes accessible to stakeholders outside the consortium?	Only after need-to-know basis and approval by the SAB
Data flows and views	Emergency Response Plan model describing the strategies, techniques systems and practices widely applied for the effective response during an emergency incident and the containment of its impacts on an organization's assets, property, and people as well as its offered services Emergency Response Plans tailored to each Pilot site describing the steps and methods to mitigate specific attacks (cyber,physical, and cyber-physical) under discussion. STWS Engage platform visualises the ERP steps and provided several functionalities for the management of the ERP to the end-user.
How can be managed after the project?	Only generic data that are not linked to CIs and are not contradictory with the Commission Decision 2015/444/EC

	and the developed PSMP will be managed after the project. The ERP model can be further exploited and adopted by Cis in order to ensure the smooth continuity of Critical Infrastructures, even in cases of serious disruptions, preventing fatalities and injuries, reducing damage to buildings, stock, and equipment, protecting the environment and the community, accelerating the resumption of normal operations.
License	Proprietary
Type and format	.pdf, .doc
Data Size	~5mb
Storage location	Partners' PCs and project MS TEAMS
Storing responsible	KEMEA
Secure storage procedures	Classified information in electronic format will be stored encrypted through ZED! or following any other procedure indicated by the PSMP (e.g. secure room/administrative area for hardcopies)
Metadata	N.A.
Ethics and Data Protection	
Dataset contains personal data?	• Deliverable to be submitted in December 2022. • Data expected to be collected: name/surname & email. • Informed consent will be given for use/reuse in case dataset contains personal data. So far, no personal data have been contained in the datasets • Personal data will be anonymised.
DPIA required	Data Privacy Impact Assessment Required - NO
Dataset ethics and legal requirements	D9.1, Recruitment of participants, Informed Consent. Requirement respected.

4.21. DATASET 21: Social Awareness

Table 4-35: Dataset 21 – Social Awareness

Template Field	Description
Overview	
Dataset Name	Social Awareness (official and public)
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	CENTRIC
Provider (if different from partner)	
Work Package	WP5
Task/Deliverable	T5.5 / D5.4
Details	

Short Description	This dataset contains information from social media services and pages – namely – Twitter and Facebook (the latter via the CrowdTangle platform). The datasets include data from public authorities, GSS operators and other organisations communicating in an official capacity.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	The data will be used to inform the development of guidelines for crisis communications and be analysed to understand what makes certain methods of communication more effective.
Use beyond 7SHIELD	The data could be used by other researchers in the field of crisis communications.
Storage and access details	
Is the data open?	Not currently. Further dissemination of CrowdTangle data is restricted via their terms of service. Twitter only allows the publication of Tweet IDs. In addition, data would require strict anonymisation procedures.
Available to 7SHIELD partners?	YES
Access control	Data will be available in a tabular format (e.g., csv, xlsx or similar)
What kind of processing is involved?	Statistical processing and text processing techniques
What kind of derivative data is produced?	Keywords, potential warning indicators and similar may be extracted
How it becomes accessible to stakeholders outside the consortium?	N/A
Data flows and views	Data is not part of the formal 7SHIELD system, it is for research and analysis purposes
How can be managed after the project?	Any dataset will be managed and stored by CENTRIC
License	TBC
Type and format	CSV or similar tabular format
Data Size	Per PUC: - Finland (Arctic Space Centre): 8058 records - Athens (National Observatory): 3261 records - ICE Cubes Service: 685 records

	- ONDA DIAS: 550 records - Spain (DEIMOS): 3222 records
Storage location	Sheffield Hallam University Research Data Archive
Storing responsible	Task Leader in CENTRIC
Secure storage procedures	Strict access procedures will be defined on deposit
Metadata	Data source: Twitter account / Facebook page / Instagram Account Data columns / headings Date collected
Ethics and Data Protection	
Dataset contains personal data?	Dataset may contain personal data (e.g. names / usernames). Such information will be at least be pseudonymised, although full anonymisation would be sought before any wider sharing of datasets beyond the task.
DPIA required	Originally a DPIA was envisioned; however, ultimately only data from organisational accounts/pages was collected which significantly reduced the incidence of processing of personal data.
Dataset ethics and legal requirements	Ethical approval for the research has been obtained through the Sheffield Hallam University Research Ethics Committee under application number ER27797704

4.22. DATASET 22: Pilot Critical Operation

Table 4-36: Dataset 22 - Pilot Critical Operation

Template Field	Description
Overview	
Dataset Name	Pilot Critical Operations Dataset
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	KEMEA, ENG, INOV, and RG as needed
Provider (if different from partner)	FMI, NOA, DEIMOS, SPACEAPPS, SERCO
Work Package	WP5
Task/Deliverable	T5.6
Details	

Short Description	Data in standardized format on (i) how operations are conducted by each pilot case study, (ii) available infrastructure (cyber and physical), (iii) available man-power, (iv) available on/off-site physical & cyber resources that can be leveraged to mitigate impacts
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	Data will be employed to determine optimal business continuity scenarios per partner in T5.6
Use beyond 7SHIELD	This primary data cannot be used beyond 7SHIELD due to its highly sensitive nature.
Storage and access details	
Is the data open?	No
Available to 7SHIELD partners?	YES, subject to end-user confidentiality requirements
Access control	Verified access only to partners through project data curation platform.
What kind of processing is involved?	Standardization of data through the adoption of a common taxonomy for operations, resources and infrastructure.
What kind of derivative data is produced?	Business continuity scenarios per T5.6
How it becomes accessible to stakeholders outside the consortium?	Only the end-user to which each dataset pertains can provide access to it
Data flows and views	Data enters the system via detailed surveys and interviews with key personnel of each end user
How can be managed after the project?	None
License	Proprietary
Type and format	CSV, JSON
Data Size	Maximum 10MB per end-user
Storage location	Project internal data curation platform
Storing responsible	ENG, RG
Secure storage procedures	Encrypted storage, access only via verified login
Metadata	None

Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	None
Dataset ethics and legal requirements	Confidentiality per end-user requirements

Table 4-37: Dataset 22 - Pilot Critical Operations - Anonymized

Template Field	Description
Overview	
Dataset Name	Pilot Critical Operations Dataset - Anonymized
Dataset Category	Primary data collected by partner in 7SHIELD
Partner	KEMEA, ENG, INOV, and RG as needed
Provider (if different from partner)	FMI, NOA, DEIMOS, SPACEAPPS, SERCO
Work Package	WP5
Task/Deliverable	T5.6
Details	
Short Description	This is data similar in nature to the "Pilot Critical Operations Dataset", only anonymized & virtualized to remove any references and information that pertain to any specific partner, thus becoming a benchmark generic dataset, applicable to all but specific to no end-user.
Existing already before the 7SHIELD project?	NO
Use in 7SHIELD	Data will be employed for dissemination of the findings of T5.6
Use beyond 7SHIELD	This primary data is fully usable beyond 7SHIELD to help researchers and other operators derive business continuity scenarios and optimize their operation and emergency response planning.
Storage and access details	
Is the data open?	Yes – Public;
Available to 7SHIELD partners?	YES

Access control	How can the data be accessed? (software, techniques, credentials, key pair, etc.)
What kind of processing is involved?	Standardization of data through the adoption of a common taxonomy for operations, resources and infrastructure. Anonymization of data to avoid any relation with specific end-users
What kind of derivative data is produced?	Business continuity scenarios per T5.6
How it becomes accessible to stakeholders outside the consortium?	Through public archives and project website
Data flows and views	Data provided by anonymization and virtualization of he "Pilot Critical Operations Dataset"
How can be managed after the project?	Data to be fully and publicly available after the project
License	Creative commons
Type and format	CSV, JSON
Data Size	Maximum 10MB
Storage location	Zenodo, GitHub
Storing responsible	ENG, RG
Secure storage procedures	None
Metadata	None
Ethics and Data Protection	
Dataset contains personal data?	No
DPIA required	None
Dataset ethics and legal requirements	None

5. 7SHIELD IPR Plan

The management of IPR is strictly ruled by the Consortium Agreement (CA) which includes all provisions related to the management of IPR including ownership, protection and publication of knowledge, access rights to knowledge and pre-existing know-how as well as questions of confidentiality, liability and dispute settlement. The IPR Management focuses on the careful handling of IPR issues in 7SHIELD project, that are of strategic importance. It aims to create a favourable environment for respecting intellectual property rights (IPR) and ensuring a uniform approach by the Consortium, in conjunction with a permanent IPR monitoring during the project.

5.1. IPR Strategy

For a successful project, it is important to have an **IPR strategy** in place, so that all partners of the consortium work collaboratively towards the achievement of common objectives. The 7 SHIELD IPR strategy is focused and concise with the aim to protect the results developed within the timeframe of the project with a set of agreements that are planned (D8.6, D8.11) to clearly identify:

1) IPR ownership;
2) Exploitation rights (and royalties) by owners and co-owners;
3) IPR protection (e.g. copyright law, patent law, trademarks law, etc.) and filing of applications where applicable;
4) IPR exploitation strategy at consortium and partner level.

This will help in maximizing the returns on the human, capital and intellectual investments.

Regarding the management of knowledge, intellectual property and other aspects of innovation two types of activity are foreseen:

1) IPRs for new systems and solutions that are prepared by consortium partners;
2) Information disseminated within the project and to external bodies, such as publications, presentations and regulatory and standards bodies, only after the necessary steps for ensuring the protection of IPRs have been made. This ensures that IP will be secured in the interest of project partners. Contributions to external bodies will have an impact on global harmonisation of concepts and systems. The dissemination of information and the influence, e.g., on standards bodies, are the prerequisites for the economic success of IPRs.

5.2. IPR Management

IPR will be handled in line with general EU policies regarding ownership, exploitation rights, confidentiality and commercial utilization of results to other EU funded projects and disclaiming rules. Specific actions will be taken in order to satisfy the basic intellectual property regime: IPRs are attributed to those who generate the results, and results are owned by those who generate them); publications will be made by the owners of the background or results for their background or results and publications are owned by those who write the article; 7SHIELD will aim at open access publications; Some of the project software modules will be Open Source, allowing operators to start using the 7SHIELD services without a major up-front investment.

Following the CA, the Results are owned by the Party that generates them. Background remains with the respective party.

In case of **Joint Ownership** the joint owner shall be entitled to use the jointly owned Results for non- commercial research activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s), and each of the joint owners shall be entitled to otherwise Exploit the jointly owned Results and to grant non-exclusive licenses to third parties (without any right to sub- license), if the other joint owners are given a 45 calendar days advance notice (at least) and Fair and Reasonable compensation.

Access Rights to Results and Background are granted on a non-exclusive basis (sublicensing is excluded) and on a royalty-free basis, if they are used for the performance of the work of a Party under the Project (implementation). After the completion of the project, Access Rights to Results for exploitation are granted on Fair and Reasonable conditions (unless access is made for internal research activities in which case access is granted on a royalty-free basis). Access Rights to Background for Exploitation, including for research on behalf of a third party, shall be granted on Fair and Reasonable conditions.

The CA also foresees clauses in relation to rights and obligations for affiliated entities of a party; such entities shall enjoy the access rights on Fair and Reasonable conditions, upon written bilateral agreement and under the condition that they all confidentiality and other obligations accepted by the Parties under the GA and CA (Article 9.5). Access may be refused if such granting is contrary to the legitimate interests of the Party which owns the Background or the Results.

Specific IPR agreements will be released later in the project but before its end to ensure the exploitation strategy is identified before the exploitation activities will begin.

5.3. Background Data

Background means any data, know-how or information – whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights – that is:

- Held by the beneficiaries before they acceded to the Agreement

- Needed to implement the action or exploit the results.

In relation to access rights to Background, the consortium will comply with the H2020 default rules (European IPR helpdesk 2015); it means that:

- On the one hand, the partners/beneficiaries will provide each other access — on a royalty-free basis — to Background needed to implement their own tasks under the action/project;
- On the other hand, the partners will give each other access — under fair and reasonable conditions — to background needed for exploiting their own results.

At proposal stage it has been confirmed that all partners have the access they need to each other background; in the Consortium Agreement (CA) signed between partners, the conditions regarding the need to implement exploitation actions are outlined.

5.4. Results

In relation to protection of the results, the partners will aim to protect all results that can be commercially or industrially exploited as appropriate (i.e. the form which offers the most adequate and effective protection for each type of result). In particular:

- Results shall be owned by the participant generating them,
- Results generated jointly (e.g. 7SHIELD platform), will be jointly owned,
- Access rights to Results. In keeping with the H2020 default rules the partners will give each other access — on a royalty-free basis — to results needed for implementing their own tasks under the action. The partners will give each other — under fair and reasonable conditions — access to results needed for exploiting their own results.

6. Conclusions and Future Outlook

This deliverable constitutes the final version of the Self-assessment & Data Management Plan (DMP) of the 7SHIELD project. D1.4 outlines the evolution of project requirements and objectives and the datasets which have already been collected / generated in 7SHIELD with detailed information about their content and their FAIR ability. Specifically, the updates provide information related to the objectives' achievements and implemented activities to reach the objectives and include new sets of data and changes in consortium policies and datasets management. It is fundamental to report the project achievements in terms of objectives realisation underlining all thee implemented activities carried out to reach the aforementioned objectives. A revised assessment plan, based on the experience gained until M24, and the monitoring of the evolution of project requirements and objectives along with the implementation of the plan and activities per objective have been reported. Moreover, it provides the description of data types and sources, explains how the FAIR principles will be respected in the project, explores the security measures, allocation of resources, ethical and legal issues related to the data collection and generation in the project. It describes in more details the procedures to be applied in the 7SHIELD project to efficiently manage its research data in terms of storage and backup (backup provision, recovery procedure), selection and preservation (which data will be retained/shared/preserved, length of time data to be preserved and preservation preparation time). It also provides a clearer vision on the data management with respect to the technologies developed in the project. Moreover, the 7SHIELD IPR plan that focuses on the careful handling of IPR issues in the project has been also illustrated. Moreover, the assessing plan of the project objectives has been illustrated. The specific objectives for the project as described in section 1.1 of the DoA have been listed and the work carried out towards the achievement of each listed objective has been assessed, considering also the expected KPIs and target value.

This DMP has been created to serve as guidance to the project partners as to the requirements and legislation that the project should follow in the delivery of the project activities with regards to the management of data. The DMP is a document that can evolve along the project, and this is the final version that includes the updates and new sets of data and changes in consortium policies and datasets management.

7. References

[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.

[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.

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

Annex I - Dataset Management Template

The following template has been developed (in line with the DMP H2020 template requirements) to specifically gather information on the various 7SHIELD datasets.

Table 8-38: Dataset Management Template

Template Field	Description
Overview	
Dataset Name	A unique and descriptive name for the dataset
Dataset Category	A category the Dataset: - Project management data - Primary data collected by partner in 7SHIELD - Secondary data (not publicly available) - Derived data (e.g., output from processing by 7SHIELD module) - Publicly available dataset (e.g. training / benchmark data) - Synthetic / generated data
Partner	The responsible partner for the dataset
Provider (if different from partner)	
Work Package	
Task/Deliverable	If applicable
Details	
Short Description	A short description for the dataset and how it was collected
Existing already before the 7SHIELD project?	YES/NO
Use in 7SHIELD	How the data is/will be used in 7SHIELD
Use beyond 7SHIELD	How the data could be useful to other researchers beyond 7SHIELD
Storage and access details	
Is the data open?	Yes – Public; Yes – but restricted access, No TBC
Available to 7SHIELD partners?	YES/NO

Access control	How can the data be accessed? (software, techniques, credentials, key pair, etc.)
What kind of processing is involved?	
What kind of derivative data is produced?	
How it becomes accessible to stakeholders outside the consortium?	
Data flows and views	Describe the data flows and views, i.e. how the data enters the system
How can be managed after the project?	Specify which part of the data can be made publicly available beyond the project end, for which purpose, under which license, and through what kind of infrastructure.
License	Specify license (e.g. Creative commons, Proprietary, etc.)
Type and format	e.g. CSV, TSV, XML, JSON, etc.
Data Size	Can be records, GB, etc.
Storage location	Where will it be stored; (if open, specify repository)
Storing responsible	Who is responsible for storing the data
Secure storage procedures	Which secure storage procedures are used for storing the dataset?
Metadata	Any metadata standards used in the dataset. What metadata has been created and how is this managed
Ethics and Data Protection	
Dataset contains personal data?	Does the dataset contain personal data, and if YES, which? (For details about personal data please see: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en) Was informed consent given for use/reuse? Is personal data anonymised?
DPIA required	Data Privacy Impact Assessment Required
Dataset ethics and legal requirements	Please describe any Ethics and/or legal requirements relevant to the dataset - If you want you can refer to relevant Ethics deliverables.

Annex II – Participant Consent Form

7SHIELD: Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats

I volunteer to participate in this research conducted as part of the research project 7SHIELD, coordinated by Engineering Ingegneria Informatica and funded by the European Commission. The information sheet has been made available to me.

Please place an "X in the boxes" to affirmatively consent to the following statements.

☐ I confirm that I have read and understood both this form and the accompanying Information Sheet. I had the time and opportunity to ask questions as needed.
☐ I understand that I am free to withdraw my consent at any time without giving reason.
☐ My personal data can be gathered to be used, stored and shared in the ways described on the accompanying Information Sheet.
☐ Data from my participation can be used to inform 7SHIELD system requirements, revise design, develop 7SHIELD technologies and subsequent evaluation activities.
☐ Data from my participation may be used to in articles for peer-reviewed journals and relevant industry magazines, for presentations at conferences and workshops,
☐ *Data from my participation may be used in the promotion of 7SHIELD in general.
☐ *7SHIELD may take research notes or audio recordings of my activities
☐ *I give my consent to be identified in any public reports.
☐ *I consent to having photos or videos taken of me for research purposes.
☐ *I consent to having photos or videos taken of me for communication purposes.
☐ *I agree to be quoted directly.
☐ I would like to receive updates on the progress and findings of the project.
☐ I agree to voluntarily take part in the 7SHIELD research.
☐ I agree to voluntarily take part in the 7SHIELD research.

*Optional

Participant Name		Participant Signature	
Participant Email*		Date	

Researcher Name		Researcher Signature	
Researcher Email		Date	
Researcher Organization			

Project Coordinator		Coordinating Organization	
Coordinator Email		Date	

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