D8.12 Security Standardisation Strategy and Policy-Planning

Work Package:	WP8 Dissemination, Impact Creation and Exploitation Plan
Lead partner:	Space Applications Services (SPACEAPPS)
Author(s):	Leslie Gale (SPACEAPPS), Helen Gibson (CENTRIC), Luigi Coppolino (CeRICT), Gerasimos Antzoulatos (CERTH), Orestis Mavropoulos (CLS), Yasmine Boulfani, Yann van Engelandt (CS), Gabriele Giunta, Francesco Durante (ENG), Timo Ryyppo (FMI), Souzana Touloumtzi (NOA), Dimitris Vamvatsikos (RG), Adriana Grazia Castriotta (SERCO) Eftichia Georgiou, Nikolaos Lalazisis (KEMEA)
Due date:	28/02/2023
Version number:	1.0 **Status:** Final
Dissemination level:	Public

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

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	03/01/2023	SPACEAPPS	First release of the Table of Contents
0.2	16/01/2023	SPACEAPPS	Second release
0.3	06/02/2023	SPACEAPPS	Third release
0.4	16/02/2023	SPACEAPPS	Release for internal review from ENG and CERTH
1.0	28/02/2023	SPACEAPPS, ENG	Final release

Quality Control

Role	Date	Who	Approved/Comment
Internal Review	*23/02/2023*	ENG	Approved with minor comments
Internal Review	*22/02/2023*	CERTH	Approved with minor comments

Disclaimer

Executive Summary

The European Parliamentary Research Service briefing PE 698.926 - February 2022 (1) concludes that over the past decade, the Space domain has gained increasing importance as an economic sector offering opportunities for established and emerging markets. Space policies and their applications have also gained in political relevance due to their capacity to tackle global challenges, such as the climate and biodiversity crises, but also due to the growing reliance of the EU economy and society on Space Infrastructure, services and data.

More than ever, today, the Europe Union is confronted by cybernetic warfare with the aim to destabilise the economy and the functioning of a country and community while organised crime knows that very high gains for a minimum of risk and investment can be achieved are carrying out cyberattacks on governments, organisations and companies followed by ransom demands.

Reality is that the complexity of attacks is increasing with new threats emerging including the mixing cyber and physical attacks to counteract the evolution and improvement of the measures taken to protect systems.

In this context, Space Ground Segments increasingly appear as potential "new targets" of "new threats", especially the hybrid ones (e.g., cyber-physical). Indeed, a physical/cyber-attack toward Space Ground Segment installations or communication networks would cause a debilitating impact on public safety and security of European citizens and could affect also other European Critical Infrastructures through cascading effects.

7SHIELD has been developed as a holistic framework covering both cyber and physical protection with cutting-edges technologies for prevention, detection, response and mitigation with the intention to offer commercial services for the protection of Space Ground Segment covering both physical and cyber threats.

One objective of the 7SHIELD project is expressed in the impact objective *IMO3 – Standardisation, strategy and policy-making* that has the aim to standardise and demonstrate strategies and policies to prevent, early detect, response and mitigate of amalgamated attacks in physical and cyber manner.

The intent of this report is to investigate and document how 7SHIELD has addressed IM03. Placing the work performed in 7SHIELD in the context of EU policies, legal frameworks, standards and best practices a concluding goal of this document is to provide policy recommendations for the future of security in Ground Segments and Satellite data assets as well as recommendations for future work on security standardisation.

Table of Contents

List of Figures

List of Tables

Definitions and acronyms

AO	Authorizing Officials
AICPA	Association of International Certified Professional Accountants
ASVS	Application Security Verification Standard
BC	Business Continuity
BCMS	Business Continuity Management System
CENELEC	Comité Européen de Normalisation Électrotechnique; (English: European Committee for Electrotechnical Standardization)
C5	Cloud Computing Compliance Criteria Catalogue
CAIQ	Consensus Assessment Initiative Questionnaire
CCM	Cloud Controls Matrix
CCTV	Closed Circuit Television

CI	Critical Infrastruture
CIS	Center for Internet Security
CIP	Critical Infrastructure Protection
CNSSI	Committee on National Security Systems Instruction
CSA	Cloud Security Alliance
C/P	Cyber/Physical
EC	European Commission
ECSS	European Cooperation for Space Standardization
EDA	European Defense Agency
EGNOS	European Geostationary Navigation Overlay System
ENISA	European Network and Information Security Agency
EO	Earth Observation
EN	From German: Europäische Norm ("European Norm")
ERP	Emergency Response Plan
ESA	European Space Agency
EUSPA	European Union Agency for the Space Programme
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites
EU	European Union
FMI	Finnish Meteorological Institute
GNSS	Global Navigation Satellite System
GSaaS	Ground Segment as a Service
IDEMF	Intrusion Detection Message Exchange Format
IEC	International Electrotechnical Commission
IoT	Internet of Things
IIoT	Industrial Internet of Things
ISAC	Information Sharing and Analysis Centers
ISMS	Information Security Management System
ISS	International Space Station
ISO	International Organization for Standardization
JTC	Joint Technical Commitee (CENELEC)
KR	Key Results
NFPA	National Fire Protection Association
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NOA	National Observatory of Athens
NSS	National Security Systems
MBCO	Minimum Business Continuity Objective
MTPD	Maximum Tolerable Period of Disruption
NFPA	National Fire Protection Association
OWASP	Open Web Application Security Project
PC	Project Coordinator
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PUC	Pilot Use Case
RMF	Risk Management Framework
SCA	Security Controls Assessors
TSC	Trust Service Criteria
SECEF	Security Exchange Format
SGS	Satellite Ground Station
WP	Work Package

1. Introduction

1.1. Scope of the deliverable

The 7SHIELD framework has been realised, guided and influenced by EU policies, legal frameworks and applicable standards, to meet the needs of the Space Ground Segment stakeholders and users.

7SHIELD set itself a number of impact objectives. One objective is *IMO3 – Standardisation, strategy and policy-making* that has the aim to standardise and demonstrate strategies and policies to prevent, early detect, response and mitigate of amalgamated attacks in physical and cyber manner.

The intent of this report is to investigate and document how 7SHIELD has addressed IM03. The work performed in 7SHIELD has been influenced by EU policies, legal frameworks, standards and best practices. It is in this context that a concluding goal of this document is to provide policy recommendations for the future of security in Ground Segments and Satellite data assets as well as recommendations for future work on security standardisation.

This document presents the results of the work performed in *Task 8.4 – Standardisation, strategy (investment measures on new installations) and policy-planning* comprising desktop research, meetings with those responsible at European Space Organisation for Security, attending and presenting at conferences and brokerage events, communication within the 7SHIELD team, including a survey on the influence of standards on the Key Results (KRs) development and implementation in the pilot use cases.

2. Methodology applied to investigating standardisation

Standardisation, strategy and policy are aspects that fit within the context of the dissemination and communication activities of 7SHIELD but have a broader scope than just the promotion of 7SHIELD.

7SHIELD has been developed as a holistic framework covering both cyber and physical protection with cutting-edges technologies for prevention, detection, response and mitigation with the intention to offer commercial services for the protection of Space Ground Segment covering both physical and cyber threats.

With the focus on creating a holistic framework there was the need from the outset to:

- Identify a set of requirements including the security requirements that are applicable for a wide range of Space Ground Segments fulfilling the needs of the stakeholders, but primarily the Ground Segment developers and operators.
- Understand the possible impact of ethics and legal frameworks on both the implementation of the framework as well as its use in the individual pilot use cases.

The 7SHIELD project organisational structure reflected these needs with the inclusion of the dedicated work package, WP2 – User Requirements and Use Case Design and the following related tasks:

- T2.1 – Use case design
- T2.2 – Stakeholder Engagement and User Requirements
- T2.3 – Security Requirements
- T2.4 – Ethics and legal framework

The User Requirements and Use Case Design was very much a forward-looking work package directed towards providing the baseline for developing the 7SHIELD Framework, identifying and performing research and establishing best practices. However, *Task 8.4 – Standardisation, strategy and policy-planning* had a more horizontal mandate in the project, namely, to engage with organisations procuring Ground Segments to understand how their policies and practices influenced the Ground Segments they procured, promote 7SHIELD, and obtain feedback on the 7SHIELD standardisation activities. To gain insight into how 7SHIELD could influence standardisation, the approach taken was to:

1. Perform an initial study on space policy and standards.
2. Establish contact with the security policy making organisations of the main European procuring agencies for Space Ground Segments.
3. Establish contacts with other EU projects with a focus on cyber and physical security.
4. Establish contact with the standardisation authority CEN/CENELEC.

3. Policies driving cyber and physical security measures

3.1. European policy on cyber and physical threats

In Europe, the European Union is leading policy development actions on cyber and physical threats with the objective to ensure the security and resilience of the EU member states' critical infrastructure and networks. EU cyber security policy has been and still is a steady evolution of policies and initiatives designed to improve the EU's cyber security posture and resilience. The EU sees establishing strong policies not only as a means to protect citizens and assets but also for building a competitive and innovative EU security industry.

In 2003, the EC launched the European Network and Information Security Agency (ENISA), a specialized EU agency tasked with promoting network and information security across the EU. In 2016, the EU passed the Network and Information Systems Directive (NIS Directive[1]), establishing the first EU-wide cyber security rules. The NIS Directive requires EU member national governments to implement the directives through their own national legislation. This can involve adapting existing laws or creating new ones to meet the requirements of the directive.

Recently in January 2023, but in the making for a number of years, two key directives on critical and digital infrastructure have entered into force to strengthen the EU's resilience against online and offline threats, from cyberattacks to crime, risks to public health or natural disasters. The two Directives entering into force are the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive[2]) and the Directive on the resilience of critical entities (CER Directive[3])

The NIS2 Directive will ensure a safer and stronger Europe by significantly expanding the sectors and type of critical entities falling under its scope. The new CER Directive replaces the European Critical Infrastructure Directive of 2008. The new rules will strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage. In both directives Space is named as an important entity.

It is of course against the background of a steady evolution of policy that in the H2020 programme the call – *Protecting the infrastructure of Europe and the people in the European smart cities* and specifically *SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe* that the 7SHIELD project was awarded.

3.2. USA Space Policy

The Space Policy Directive-5 (Cybersecurity Principles for Space Systems) of September 4, 2020 states: "The United States considers unfettered freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation". "Space Systems" is defined as "a combination of systems, to include ground systems, sensor networks, and one or more space vehicles that provides a space-based service".

The Five Principles of Section four of Space Policy Directives:

1. Space systems and their supporting infrastructure, including software, should be developed, and operated using risk-based, cybersecurity-informed engineering;

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148
[2] https://eur-lex.europa.eu/eli/dir/2022/2555
[3] https://eur-lex.europa.eu/eli/dir/2022/2557/oj

2. Space system owners and operators should develop and implement cybersecurity plans for their space systems that incorporate capabilities to ensure operators or automated control center systems can retain or recover positive control of space vehicles;
3. Implementation of these principles, through rules, regulations, and guidance, should enhance space system cybersecurity;
4. Space system owners and operators should collaborate to promote the development of best practices, to the extent permitted by applicable law. They should also share threat, warning, and incident information within the space industry, using venues such as Information Sharing and Analysis Centers (ISAC) to the greatest extent possible, consistent with applicable law;
5. Security measures should be designed to be effective while permitting space system owners and operators to manage appropriate risk tolerances and minimize undue burden, consistent with specific mission requirements. United States national security and national critical functions, space vehicle size, mission duration, manoeuvrability, and any applicable orbital regimes.

The principals essentially require a full lifecycle risk-based cybersecurity engineering and the implementation and sharing of best practices and threats.

The recently published NIST Interagency Report NIST IR 8401 Satellite Ground Segment "Applying the Cybersecurity Framework to Satellite Command and Control" maps to 7SHIELD (2). Recognising the importance and critical nature that space systems have in security the report deals with the ground segment of space operations in general with an emphasis on the command and control of satellite buses and payloads. It provides a flexible framework for stakeholders to manage risks. The report expresses similar concerns and actions as the EU NIS directives however what we can perhaps begin to see is the trend that ground segments are no longer either upstream or downstream but are connected systems with increasing overlap that in the future will require new concepts to manage their operation.

3.3. Security policy making organisations of the main European procuring agencies for space ground segments

Policies for cyber and physical security measures for Space Ground Segments are established by the government agencies and organizations responsible for managing and operating Ground Segment Infrastructures or procuring them through open tendering.

An initial desktop analysis of European Union Agency for the Space Programme (EUSPA) and European Space Agency (ESA), the two main agencies responsible for Space Ground Segments, investigated the nature of the ground segments.

Institutional bodies such as ESA and EUSPA have policies but unlike the EU policies where EU Member States have the responsibility to implement the Directives to support the policy, EUSPA and ESA take a more integrated approach of specifying requirements or contractual conditions to be adhered to a contractor/operator when developing and operating a ground segment. Certification processes and accreditation being established to ensure the requirements are met by the operator.

Following up on the desktop analysis, meetings were held with representatives from EUSPA, ESA and SatCen. At the meetings, 7SHIELD was presented followed by a discussion on policy, standards and certification. It should be noted that the classification of 7SHIELD as an EU restricted project literally restricted the information that could be shared. This resulted in a quite a superficial presentation with little detail on how the 7SHIELD capabilities would/are achieved. Despite this, all three organisations expressed interest. Following the meetings further research and discussions were carried out with EUSPA and ESA.

EUSPA manages public interests related to the European Global Navigation Satellite System (GNSS), European Geostationary Navigation Overlay System (EGNOS) and Galileo programmes, the Earth Observation (EO) programme Copernicus, and the European Union Governmental Satellite Communications (GOVSATCOM) programme, while ESA is responsible for Europe's space programme, including scientific missions, space exploration and the development the Sentinel satellites and shared responsibility with EUMETSAT for their operation.

Besides measures to ensure the secure exchange of data between its space systems and ground-based infrastructure, ESA's space security policy covers areas such as the prevention of space debris and the protection of its missions from physical threats, such as space weather and natural disasters.

3.4. Influence of long-time scales for space missions

For Space Ground Segments it is important to understand that ground segments are part of a large development programme to realise a space mission. The development time for a mission can vary greatly depending on several factors such as the scope of the mission, its complexity and funding. Commercial satellite developments for medium-sized satellite mission for instance can range from 2 to 5 years, while larger, more complex institutional led missions, such a science missions, Galileo and Copernicus take upwards of a decade or more to develop and make operational. Even more complex programmes requiring international participation such as the International Space Station (ISS) take decennia to realise.

Another aspect that complicates the whole procurement process is that institutional programmes are procured through a process of industrial tendering. The specification of the tender and the resulting bidding process can be complex. Tendering of a space mission can therefore take many years to prepare which means that a space mission is developed under, at the time of tendering, policies and standards that may already be superseded at the time the tender is issued and certainly by the time the mission is ready to become operational. It is also important to note that the development of a space mission involves several stages, including concept development, design, construction, testing, and launch that can further delay the development time scales and introduce complexity because multiple tendering processes can be required. This could potentially lead to a lack of continuity on how policy, standards and requirements are fulfilled between the various stages because the winning industrial organisation can change for the different stages.

For operational missions the policies and standards applied need therefore not be consistent across missions within an organisation. It is also noticeable that the organisations organise their approach to coordinating how policies and standards are implemented differ.

Taking ESA as an example, where two of the five 7SHIELD PUCs have close links with ESA, we can observe that in ESA there is natural focus depending upon the role of the directorate. This is also noticeable in early publications and documents. In the paper (3), recommendations for security policies to protect sensitive information that is produced or processed were made. This included possible sensitive satellite operational data (house-keeping telemetry) from the spacecraft as well as cryptographic keys that are used for encryption and authentication. The ESA document, ESA EO Ground Segment Security Policy, published in June 2007 stated that the policy was to protect ESA EO Ground Segment information and assets from all threats, whether they be internal or external, deliberate of accidental. Information assets were considered to be data stored on computers, data transmitted across networks, written on paper, sent by fax, stored on tapes and diskettes. It is interesting to note that the EO Ground Segment Security Policy already recognised the need to meet requirements for relevant business, national and international law and the need to report every breach of information security.

More than a decennium later we see at ESA an evolution. ESA Security Regulations (Rev 2) sets out the basic security principles and minimum standards to be applied by ESA and by the ESA Member States,

in accordance with their respective laws and regulations insofar as they provide an equivalent level of protection. An ESA Security Office, ESA Security Authority, DG Service have been created for the coordination, control and supervision of the implementation of the ESA Security measures that includes acting as Security Accreditation Authority for ESA.

The ESA's European Space Security and Education Centre, at Redu in Belgium, a centre of excellence has been established for space cyber security services providing a European reference centre for cyber security services, operated by industry with ESA being the 'catalyser' of the interests in cyber security and the owner of the part related to space.

We do still however see that at procurement level that standards and guidelines are given at project level as requirements or contractual clauses depending upon the nature of the project and the issuing directorate.

4. 7SHIELD standardisation approach

7SHIELD took the position that only through standardisation would it be possible to create a holistic framework. Both the scope, covering cyber and physical threats, and the diversity of the target ground segment systems required the integration of many tools, components and sub-systems. For future exploitation it is important that new users of 7SHIELD can rely on standards to allow integration of 7SHIELD components into their systems or the development of new systems meeting applicable standards.

Figure 1 illustrates how stakeholder requirements, policy and existing standards have influenced the specification and development of 7SHIELD.

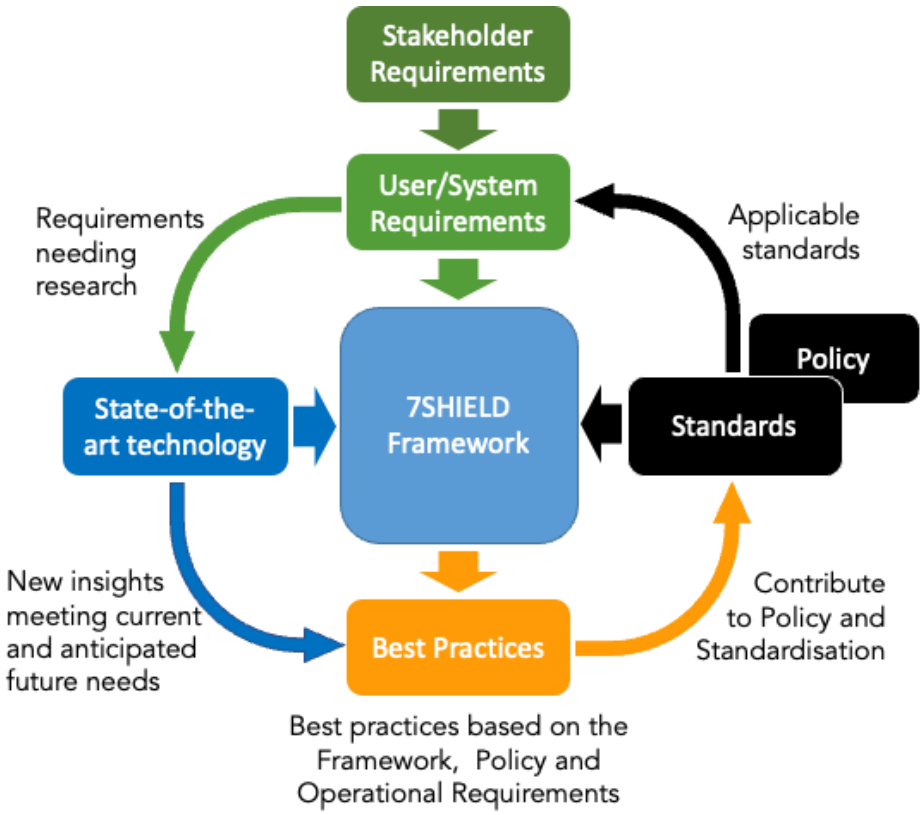

Figure 1: Information flow for 7SHIELD

End-users and stakeholders of the Ground Segments operated by the five Pilot Use Case (PUC) leaders of the consortium were involved to elucidate the user and system requirements. The compilation of user requirements includes the scenario-based and solution-wide functional requirements and their priority per actor, as well as non-functional requirements under various categories, such as performance, reliability, expandability, compatibility, localization, documentation, security, legal, ethical, and safety. Requirements that were insufficiently covered by existing components proposed by the partner(s) for inclusion into the 7SHIELD Framework resulted in starting research and development activities to deliver key results for inclusion into the 7SHIELD Framework.

4.1. International landscape of security standards

To support policies and legislation in the field of privacy and security, standards are developed. Standards have been defined as "technical specifications" defining requirements for products, production processes, services or test-methods. These specifications are voluntary. They are developed by industry and market actors following some basic principles such as consensus, openness,

transparency, and non-discrimination. Standards ensure interoperability and safety, reduce costs and facilitate companies' integration in the value chain and trade".

In the following paragraphs, the cyber and physical security standards and compliance criteria requirements as identified from the normative literature are presented.

ISO-27001 is part of a set of standards developed to handle information security: the ISO/IEC 27000 series. ISO 27001 was developed to help organizations, of any size or any industry, protect their information in a systematic and cost-effective way, through the adoption of an Information Security Management System (ISMS). The ISMS defines and manages controls that an organization needs to implement to ensure that it is protecting the confidentiality, availability, and integrity of its assets from threats and vulnerabilities. The ISM is organised around the concept of information risk management. The basic goal of ISO 27001 is to protect three aspects of information: confidentiality, integrity, and availability.

As part of information security management, an organisation may implement an information security management system and other best practices found in the ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27035 standards on information security. The control objectives and controls listed in ISO 27001, 27002 are directly derived from and aligned with those listed in ISO/IEC 17799:2005 Clauses 5 to 15. The lists are not exhaustive, and an organization may consider that additional control objectives and controls are necessary.

The OWASP Application Security Verification Standard (ASVS) is a list of available security requirements and verification criteria. OWASP ASVS can be a source of detailed security requirements for development teams. The specific standard categorizes the security requirements into different classes based on the security area that they cover. The ASVS security requirements are categorized into 14 different domains based on a shared higher-order security function.

IEC 62443 is an international series of standards that address cybersecurity for operational technology in automation and control systems. The standard is divided into different sections and describes both technical and process-related aspects of automation and control systems cybersecurity. IEC 62443 addresses not only the technology that comprises a control system, but also the work processes, countermeasures, and employees. IEC 62443 takes a risk-based approach to cyber security, which is based on the concept that it is neither efficient nor sustainable to try to protect all assets in equal measure. Instead, users must identify what is most valuable and requires the greatest protection and identify vulnerabilities (4).

The cloud computing compliance criteria catalogue (C5) defines a baseline security level for cloud computing that is used by professional cloud service providers, auditors, and cloud customers. The Federal Office for Information Security in Germany (BSI Germany) initially introduced C5 in 2016. In 2020, the catalogue (C5-2020) was reworked thoroughly adapting to new developments and increasing quality further (5).

The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing aligned to the CSA best practices, that is considered the de-facto standard for cloud security and privacy. The accompanying questionnaire, CAIQ, provides a set of “yes or no” questions based on the security controls in the CCM v4. CCM is mapped to the following: ISO/IEC 27001/27002/27017/27018, CCM V3.0.1, AICPA TSC (2017), CIS Controls V8, NIST 800-53r5, and PCI DSSv3.2.1. These mappings identify the equivalence, gaps, and misalignment between the control specifications of the CCM V4 and other standards (6).

ISO 22322:2015 is an international standard and provides guidelines for developing, managing, and implementing public warning before, during, and after incidents (7). ISO 22320:2018, Security and resilience - Emergency management - Guidelines for incident management, is an international standard that provide guidelines to be used for organizations that helps to mitigate threats and deal

with incidents to ensure continuity of basic function of society (8). The Physical Asset Protection Standard utilizes a management systems approach to provide guidance for assisting organizations in the design, implementation, monitoring, evaluation, and maintenance of a physical asset protection program. It also provides guidance on the identification, application, and management of physical protection systems to safeguard an organization's assets (9). ISO 28000:2022, Security and resilience – Security management systems – Requirements, specifies requirements for a security management system including aspects relevant to the supply chain (10).

4.2. European Space Standards

Europe has a long existing emphasis on creating and maintaining standards for its space industry. Initiated in 1964 the ESA Procedures, Specifications & Standards were created.

In 1993, the European Cooperation for Space Standardization was established. European Cooperation for Space Standardization (ECSS) is an example of a pathway to standardisation that involves ESA, national space agencies and industry represented by Eurospace. It has as observers CEN-CENELEC, EUMETSAT, European Commission (EC) and European Defense Agency (EDA). The Communication from the Commission to the Council and the European Parliament on European Space Policy[4] published on 26 April 2007 initiated the need for space standards.

In July 2009, with anticipation of the provision of the Lisbon treaty (2009), mandate M/496 was generated. This mandate required a set of coherent space standards. In 2017 the CEN-CENELEC Joint Technical Committee 5 'Space' (JTC 5) was kicked-off. Led by ECSS as a representative CEN, CENELEC and ECSS signed a Memorandum of Understanding in May 2013 establishing the intention to transform all ECSS standards into European Standards (ENs). The standards are developed through a series of working groups, which are responsible for drafting and reviewing the standards based on input from experts in the relevant fields.

Although the emphasis on cyber and physical security has changed with policy evolution closer to existing standards there is a lack of Space Specific standards on security. Both the CEN-CENELEC JTC 5 Space and ECSS lack specific standards in this respect, however, ECSS has a working group on security in European Cooperation for Space Standardization and most likely a policy change will be needed. Currently (status February 2023) four standards are in drafting (source: ecss.nl).

Table 1: ECSS Security Standards - Drafting

ECSS-Q-ST-80-10C (aka as 90C)	Space product assurance – Security in space systems lifecycles	Drafting
ECSS-Q-HB-80-xxA	Space product assurance – Security	Drafting
ECSS-Q-HB-80-yyA	Space product assurance – Ground segment security	Drafting
ECSS-Q-HB-80-zzA	Space product assurance – Space segment security	Drafting

4.3. Compliance criteria requirements as identified by the 7SHIELD operators

Because Space Ground Segments are identified as critical infrastructures there is an obligation to take measures to protect them from cyber and physical threats. The obligations are strongly driven by EU, national and regional regulations. Space agencies, national and European must therefore protect their critical infrastructures and assets which flows down to the designers, developers and operators. Also, in increasing numbers, private Ground Segment owners are operating systems that need continuity of service. They too will need to comply with national regulations.

[4] COM(2007)212 final, 26/04/2007, European Space Policy

In order to be used in a significant part of the future customer base, the 7SHIELD framework therefore has to meet both institutional and private legislation needs, creating obligations to protect against cyber and physical threats.

Complementary to the identified and described laws and regulations that should be followed in the context of 7SHIELD, operators were asked to provide any additional regulations and standards that should be considered in the context of each operational scenario. In the following paragraphs, the cyber and physical security standards and compliance criteria requirements as identified by the 7SHIELD operators are presented.

Arctic Space Centre, Finland (PUC1) and ICE Cubes Service (PUC4) mentioned also that an important standard they follow is CNSSI 1200. CNSSI 1200 (National Information Assurance Instruction for Space Systems Used to Support National Security Missions) is an instruction that helps ensure the success of missions that rely on use of space-based National Security Systems (NSS). It elaborates on how to appropriately integrate Information Assurance into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems. It also provides guidance to the Authorizing Officials (AO) and Security Controls Assessors (SCA) for space systems with respect to their roles within the Risk Management Framework (RMF) (11).

Moreover, all the end-users, namely PUC1, PUC2, PUC3, PUC4 and PC5 owners, follow ISO27001 and ISO27002.

The National Observatory of Athens (NOA) Ground Segment, Greece (PUC3) also mentioned the following standards:

- ISO/IEC 15408 standard contains a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.
- ISO/IEC TR 15947 standard defines a framework for detection of intrusions into IT systems. It establishes common definitions for intrusion detection terms and concepts. It describes the methodologies, concepts and relationships among them, addresses possible orderings of intrusion detection tasks and related activities, and attempts to relate these tasks and processes to an organisation's or enterprise's procedures to demonstrate the practical integration of intrusion detection within an organization or enterprise security policy.
- ISO/IEC TR 18044 provides information on the benefits to be obtained from and the key issues associated with a good information security incident management approach, examples of information security incidents, and an insight into their possible causes, description of the planning and documentation required to introduce a good, structured information security incident management approach, and description of the incident management process.
- ISO 22320:2018, Security and resilience - Emergency management - Guidelines for incident management, is an international standard published by International Organisation for Standardisation that provides generic guidelines and a basic roadmap to be used by organisations in order to help them moderate threats and manage disruptive incidents that have the possibility to escalate into a crisis. It provides a set of procedures and advice for the successful response in the framework of the crisis in order to mitigate consequences and reduce the overall impact on the organisation's operations and ensure prompt recovery and continuity of basic functions.

As part of the Pre-Crisis Management phase of 7SHIELD each PUC is required to develop a scenario-based Emergency Response Plan (ERP) based on the attack profile identified in the requirements

gathering of task T2.2 of WP2 – User Requirements and Use Case Design. To assist in the development of the ERP the following guidelines were identified as applicable to the development process:

- ASIS International has published the guideline ASIS GDL BC 01 2005 (12) titled "Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery", the scope of which is to offer a generic guideline that is applicable both to private and public organisation environments and aims at developing, testing, and sustaining an organisation-wide response plan for use in the event of a crisis that threatens the viability and continuity of the operations of an organisation.
- The US Federal Emergency Management Agency published in 2010 (13) a comprehensive set of guidelines on developing emergency operational plans in order to promote a common understanding and help in the creation of integrated and coordinated emergency response plans, based on risk management principles. By following an all-hazards approach in all areas of emergency management (prevention, protection, response, recovery and mitigation) the guide's goal was to streamline the various phases of the emergency management process in all security areas and help emergency stakeholders in developing and maintaining a methodical way of engagement in the life cycle of emergencies/crises.
- NFPA (National Fire Protection Association) 1600 (14) is a standard the scope of which is to establish a common set of criteria for all hazards disaster/emergency management, with the purpose of providing the foundation, to both public and private entities, to develop, implement, assess, and maintain an effective program for the prevention, mitigation, preparedness, response, continuity and recovery of operations and the provision of services. In addition, the standard promotes a common understanding to help the involving entities to produce an integrated, coordinated, and synchronised program for disaster/emergency management and business continuity. Regarding Emergency Response, in particular, this phase is considered part of the implementation section, in which Emergency Operation Response Plans need to have been put in place in order to define the responsibilities for carrying out specific actions. More specifically, according to the standard, ERPs should strive for incident stabilisation by highlighting the protective actions for life safety, warnings & notifications, crisis communications & public information and resource management, including employee assistance and support procedures and provisions. All the above, should be defined in the form of operational procedures to be implemented in case of emergency.
- The NIST 800-61 Guide (15) provides guidelines for cyber incident handling, particularly for analysing incident-related data and determining the appropriate response to each incident. Therefore, the Guide aspires on assisting organisations in mitigating the risks from computer security incidents by establishing computer security incident response capabilities and handling cyber incidents efficiently and effectively to prevent subsequent compromises and minimise their impact on operations and assets. Although this Guide has been prepared for use by Federal agencies, it may, also, be used by non-governmental or private organisations on a voluntary basis. According to the Guide, the establishment of an effective cyber incident response is structured upon two fundamental pillars: a) the organisation of cyber-incident response capabilities, which highlights the need for incident response and highlights other groups of stakeholders within an organisation that may participate in incident handling and b) the actual handling of the cyber incident, which reviews the basic incident handling steps and provides advice for performing incident handling more effectively and finally any other post incident activity.

4.4. 7SHIELD framework standards survey results

4.4.1. Background of the survey

When writing the proposal for 7SHIELD it was anticipated that existing policies and standards could influence the solutions and uptake of 7SHIELD. At the start of the project, an exercise to investigate the policies and standards under which the 7SHIELD Framework would be developed was made and presented to the Advisory Board at the 2nd Plenary Meeting in February 2021. During the work to establish the user requirements a further analysis was performed to identify applicable standards.

During the project at plenary meetings the topic of Policy and Standards was always on the agenda. Contributions to the extension of the IDMEFv1 IETF Standard (RFC 4765) stimulated by 7SHIELD was undertaken, which is discussed later in this document. 7SHIELD, at least from the development point of view, was not suffering from the imposed standards. We do point out that measures for protecting personal data and the concerns raised on legal and ethical considerations raised by the technologies used by 7SHIELD were presented in 7SHIELD deliverable D2.6 Final Ethics and Legal Framework (due at M25). No issues were experienced on personal data or legal and ethical considerations with the PUC demonstrations.

With such a smooth navigation through the policies and standards, we decided that a survey should be held to learn from the 7SHIELD partners how standards had been used, asking if the standards had influenced their work and to what extent they felt an evolution of the standard was/might be needed.

The survey has been performed twice. The initial survey was held in June 2022 and repeated in February 2023 to discover if there were any changes in opinion resulting from the experience gained with the PUC demonstrations.

4.4.2. Survey results

1. **Which standards have you used in your work developing the Key Results?**

We know from the "User Requirements and Use Case Design" work that many standards were considered applicable to 7SHIELD. The survey reported 36 standards as being applicable. An overview of the standards is presented in Annex 1.

2. **How have the standards been used?**
    a. as guidelines for implementing the key result / ground segment
    b. as a means to establish verification and validation criteria
    c. as a means to show compliance as part of your company's certification

a. as guidelines for implementing the key result / ground segment

100% of the development teams acknowledged that standards offered guidelines for implementing Key Results and the PUCs. Standards have been useful in 2 areas: 1) as guidelines to provide a basic foundation model as was the case for Emergency Response Plan model (FEMA CPG 101) and the Generic Operational Model and Business Impact Analysis (ISO22301:2019 and ISO 9001:2008 respectively); 2) defining alerts applying the IDMEF format

b. as a means to establish verification and validation criteria

Only 40% found that standards contributed to establishing verification and validation criteria. This was the case for software standards that set out the process and methodology for specifying and performing verification and validation and for test criteria to assess the impact of a disaster to the operability of a GS, which are based on the concepts of the Maximum Tolerable Period of Disruption (MTPD) and Minimum Business Continuity Objective (MBCO) foreseen by ISO 22301:2019.

c. as a means to show compliance as part of your company's certification

Just 30% agreed that standards helped to show compliance. This was primarily with the IT teams. Management, development, validation and service provision processes are flexible and can be adapted to customer needs. However, IT security policy must be followed strictly. ISO 27001 is used to define IT security policy and has been applied to the deployment of the 7SHIELD framework and the setup of network connectivity between 7SHIELD framework, 7SHIELD remote modules and Ground Segment infrastructure.

Accreditation following procedures specified for the individual PUCs has been followed but not directly aligned with standards but with policy.

3. **Has the availability of standards helped in the process of innovation in creating the Key results?**

It is generally accepted that a systematic application of concept leads to a standardised approach that establishes common interfaces and creates best practices. It has also been suggested that standards either by presenting accumulated knowledge or by setting a high standard to be met encourages innovation. In 7SHIELD, we were interested to know if the developers experienced standards as a positive stimulant, and, in particular, 80% were positive.

The standards helped in the process of innovation in creating the Key Result in the sense that it provided the emergency management and response structure for the development of both strategic and operational guidelines dedicated for the ground segments at hand. In this sense, the standards provided the basis for establishing clear and specific communication channels, specific roles and responsibilities for the ground segment's stakeholders, the definition of specific incident management tasks that need to be performed at each organizational level, as well as provisions for the cooperation between levels within a single ground segment but also between multiple stakeholders outside the ground segment per se (police authorities, ESA etc.). Therefore, the standards formulated the model upon which specific, dedicated and tailor-made emergency response guidelines were created, facilitating timely and effective decision making for the containment of an emergency and leading towards the recovery of a ground segment's operations.

Standards supported the innovation from the technical point of view, given that a) allowed effective distribution of emergency information with improved standardization and ability to be tailored for user needs, and b) allowed the understanding of the complex relationships that exist between organizations, systems, and systems-of-systems, also enabling the analysis of these systems to ensure that they meet the expectations of the end users.

The availability of standards has provided a common framework for the message generation as well as supporting the identification of similar approaches (in other areas of crisis management). It has also led to IDMEFv2 format, developed based on the IDMEFv1 IETF Standard (RFC 4765), it has been employed within our key result to enable the retrieval and display of geolocation and physical assets information.

4. **Do you anticipate that the current standards will have to evolve to allow the application of the innovations introduced in 7SHIELD?**

There was no consensus with a 50/50 split. From an IT security standards perspective, where in fact 7SHIELD applied known standards, it was not felt that current standards need to evolve. However, from the organisational and data exchange perspective evolution is expected that standards will need to evolve.

Within the 7SHIELD project steps have been made to add physical assets to the IDMEFv1 IETF Standard.

5. **Having completed the development of your key result(s) / ground segment infrastructure upgrades do you see the need to investigate further the standards applicable to your work?**

   a. No, we are already aware of the standards needed for our work;

b. Yes, due to 7SHIELD standards have become more relevant;

c. Other: please describe.

The purpose of this question is to gain insight into the benefit gained by the 7SHIELD participant organisations.

Organisations that are active in the Space business domain and significantly involved IT related aspects felt that they were sufficiently aware of the applicable standards for their work. Others (the majority), specifically in the areas where new technologies were being introduced it was felt that review of the standards has made the importance of knowledge of standards more relevant for their work. Particularly to effectively utilise the technologies, a better understanding of standards is needed especially when this applies to legal aspects and ethics as in the case of face detection and recognition.

6. Besides the creation of the Key Result / Ground Infrastructure how would you typify the result?

a. Technology research to deliver a new solution

b. Creation of best practices to implement the 7SHIELD requirements

c. Other

The response to this question was interesting in that it revealed a process of creating new solutions and establishing best practices to use with the PUCs. 75% had as a starting point developing or using new technologies to create solutions for the 7SHIELD Key Results. This however included a group that emphasised that (a) and (b) are complementary and equally important with technology research and development delivering technical solutions and followed by the creation of best practices to use the solutions.

Providing best practices should be considered therefore as a valuable output of 7SHIELD providing a best practice-oriented approach for future projects helping to overcome (avoid) problems encountered in 7SHIELD. The 7SHIELD Training Platform should play an important role in ensuring the best practices remain available after the project is completed.

4.4.3. Survey conclusions

Overwhelmingly the experience of applying standards is positive. The consensus is that considering policies and standards from the outset of the project has provided guidelines to establishing foundation models and supported the process of innovation in creating the key results.

When it comes to deciding if standards would need to evolve to allow the application of the innovations introduced in 7SHIELD, there was no consensus with 50% considering it likely, while 50% felt it was not needed. However, those who considered an evolution was needed cited organisational aspects as probably most needed area of evolution. Currently the ECSS organisation is drafting security requirements in the product assurance branch of the standards.

4.5. Contribution to the IDMEFv2 format

IDMEFv1 is a cyber intrusion detection format specified in 2007 in RFC 4765 at IETF. An update was in progress at the beginning of 7SHIELD in the SECEF (Security Exchange Format) project[5]. The perimeter of the new version IDMEFv2 was not definitely defined but it was supposed to include cyber incidents and availability incidents. IoT, IIoT and Scada were also discussed. 7SHIELD architecture quickly highlighted that the need was larger, and that physical assets and hazards (natural and man-

[5] https://www.secef.net/

made) should also be included. The decision was then taken to define a new version of IDMEFv2 for all kind of incident (wider than intrusion) detection may they be cyber, physical, availability or hazards.

Supporting the development process of a standard requires time and dedication. An individual's past experience and opportunity are strongly contributing factors to the likely success. The combination of the SECEF project and the opportunity offered by 7SHIELD made it possible to pursue the update of the standard.

The need for combined physical and cyber incident detection is increasing with the rise of IoT, IIot, "smart" systems (infrastructure, transport, etc.) but it is still a new and disruptive concept. Defining such a standard needs a wide range of expertise coming from two very different domains. CCTV experts are very rarely anti-virus expert, and vice versa. 7SHIELD gathered in the same project those multiple competencies which were essential to define a common format. The 7SHIELD architecture itself and the five pilots allowed to test the first draft of the IDMEFv2 format in full-scale with close to 30 modules communicating through this format. The collaboration between SECEF and 7SHIELD has been essential.

Having the will and the opportunity is just one part of the process. Procedural steps are required to submit and gain approval for an update of the standard.

The collaboration with another research project on IDMEF has led to the writing of an IETF Draft of IDMEFv2 (https://datatracker.ietf.org/doc/draft-lehmann-idmefv2/). IETF has been chosen as IDMEFv1 has been published in this organisation. There are two major tracks to transform a draft into an official RFC. Either the IETF way with the creation of an official IETF working group working on the standard and proposing a standard RFC, or the individual way which leads to informational or experimental RFCs. We are trying the standard way, but the subject being so new, an experimental RFC would still be a very nice result.

Making recommendations and taking actions to update a standard is difficult. The elaboration of the first IDMEFv2 draft during the 7SHIELD project has needed a lot of alignment work. It would not have been possible without one of the 7SHELD partners working at the same time on a research project for improving IDMEFv1 and that the other partners accepted to "beta test" the first draft. Creating a standard is a full-time project. "Classical" projects can be encouraged to use standards or to contribute to emerging ones but it's complicated to mix in the same project multiple goals and creating a standard is nearly an "exhaustive" goal.

The experience and the difficulties encountered on the "IDMEF" road, suggest there are no real recipe to create a standard. Either it comes from very large companies with no real consensus who can have their choices imposed or it comes from small team of passionate individuals who end up in very few cases creating something that can be widely adopted.

The creation of a first draft at IETF is a very important step although it is still very far from obtaining standardization. Now that there is a formal draft and some code and implementation it is time to create an "IDMEF community" to support the format and convince IETF to create a working group toward a standard track. After draft submission a dedicated web site has been created for community support (www.idmefv2.org). The website hosts documentation and code. There is also a mailing list that anyone interested in the IDMEFv2 initiative can join. The idmefv2.org website hosts a page dedicated to "how to support IDMEF" (https://github.com/IDMEFv2/IDMEFv2-Specification/wiki/IDMEFv2-:-How-to-join-and-support-the-IDMEFv2-initiative-%3F)

5. Influencing future use and policy

7SHIELD provides to the Space Ground Segment security solutions with a focus on increasing the resilience and protection of ground systems and networks against cyber and physical threats.

The developed technologies and 7SHIELD framework have been tested in five pilot use cases, consisting of several scenarios involving physical, cyber or combined cyber/physical attack scenarios. The framework has been tested in training grounds owned by FMI, NOA, DEIMOS, SPACEAPPS and SERCO. 7SHIELD had three demonstrations and four operational tests. By successfully completing the integration of the solutions into the 5 existing ground segments (the 5 PUCs) 7SHIELD has proven the value of the 7SHIELD framework.

In 7SHIELD, we investigated the possible pathways to standardisation. As discussed in section 4, EU and International (mainly USA) directives, EU and International legislation and government regulation has introduced policies and standards to which 7SHIELD has responded. Two possible routes for 7SHIELD to follow are:

1. Industry Consensus: this pathway involves bringing together representatives from various stakeholders within an industry, such as manufacturers, suppliers, customers, and regulators, to reach a consensus on the standards that should be used. This process is often led by industry associations or standards organizations.
2. Market Force: consumer demand for consistent and interoperable products and services. Companies that adopt widely recognized standards may have a competitive advantage over those that do not.

The strategy of 7SHIELD is to build bridges linking existing standards to the development of ground segments and leading by example by providing a framework that systematically applies best practices to meet user demands.

5.1. Standardisation approach – providing solutions that are systematically applied in 7SHIELD.

7SHIELD is created taking into consideration more than 20 standards and good practice guidelines (see Annex 1) and responding to more than 250 Stakeholder (User) requirements. The Key Results components have been designed and implemented to be systematically applied to allow 7SHIELD to be offered as a "use-case-tailored" security framework comprising both software and hardware components. The software part of 7SHIELD will be offered as a service in either in-premise or cloud-based mode while the hardware part (e.g., physical monitoring elements) will be sold on a per-element basis.

The 7SHIELD framework can be considered as a set of standard components and best practices that guide users in customising the components to meet their specific needs.

By promoting and exploiting 7SHIELD, a goal is to drive standardization by offering the consistent and interoperable products and services of 7SHIELD.

5.2. Creating awareness and follow-up to enhance a ground segment system

7SHIELD is organised in three phases: Pre-Crisis Management, Crisis Management and Post-Crisis Management. Pre-crisis management is the means by which 7SHIELD creates awareness and addresses enhancing organizational resilience by defining the Business Continuity (BC) baseline that has to be achieved when faced with an attack. A state-of-the-art approach for risk mitigation is used to define the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

ISO 22301:2019 specifies some general requirements to implement, maintain and improve resilience, there is no single recommended plan for improving BC. Instead, every organization needs to develop its own dynamic Business Continuity Management System (BCMS) based on its unique characteristics. In this process, the identification of the major faced risks along with the development of the corresponding response procedures, the training and the testing of such steps are deemed to be crucial parameters that largely affect the effectiveness of a BCMS. In particular, training and testing is an iterative optimization process that involves initially developing a test methodology, in which the simultaneous testing and training of the disaster recovery team is followed by a BC revision to improve its efficiency, and consequently this is followed by a simultaneous testing and training phase.

Together with a technical assessment a user of 7SHIELD can create a plan to enhance their ground segment to achieve the goals established in the BC.

5.3. Capturing best practices in training

Best practices provide effective and efficient ways to accomplish using 7SHIELD to improve an existing system or create a new system applying the components and methodology of 7SHIELD.

The benefits offered are by applying the best practices are:

1. Consistency: created by experts the best practices present a standardized approach to achieving the purpose for which the component was designed. This ensures when used with other components, or other products adhering to the standards used by the 7SHIELD components for interfacing that the components and other products create a consistent system.
2. Higher quality: used in the PUCs the best practices have been proven to ensure that the end-result meets or exceeds the desired expectations of the user.

By capturing the best practices in training, it provides (potential) users with the opportunity to become familiar with 7SHELD which should:

1. Streamline uptake: best practices are designed to streamline processes and eliminate unnecessary steps, which can result in increased productivity.
2. Reduce risk: best practices are designed to minimize the risk of errors, incorrect use which can help improve the reliability of the resulting system.

To support best practices 7SHIELD provides a training platform (https://7shield.spaceapplications.com)

The purpose of the 7SHIELD Training Platform is to explain to the project's stakeholders the objectives and benefits of the 7SHIELD framework and to provide the SGS operators with more technical information.

For each tool, the Training Platform provides a short description, benefits and relation with the other tools, and concludes with a detailed Operation Manual for the operators.

6. Conclusions and future outlook

The work performed in 7SHIELD has shown that a Space Ground Segment is the merging of many technologies such IT services, face recognition and physical detection devices with very specific space infrastructure and satellite communication needs.

As such, 7SHIELD is subject to a large number of standards with for each specific topic of a "Key Result" one or more standards being applicable and, in some cases, specific space standards being applicable. As discovered in the process of investigating the ECSS and CEN/CENELEC Space standards, the standards cover products, components and production standards. Specific security standards are in drafting by ECSS. For Space missions, security requirements are made applicable and provided as requirements or as annexes to the contractual conditions with the responsibility being with the contractor to demonstrate the requirements are met. Accreditation processes are used to ensure the resulting ground segment meets the required security requirements.

7SHIELD anticipated that there would be gaps in policy and standards and that 7SHIELD would contribute to standards and make recommendations. The expectation did not manifest itself in the project with the exception of the IDMEFv2 format. The side note being that the update of the IDMEFv1 to IDEMFv2 format benefited from already established work in the SECEF project and new needs of 7SHIELD. The conclusion being that without the SECEF team behind the IDMEF v2 it would not have been possible for 7SHIELD on its own to support the effort required to support a standard update. Also, the original project duration of 24 months was considered as too short taking into consideration it would have taken 6 to 9 months to identify a gap. Even with the extension to 30 months the update has only reached a first draft at IETF. This is a very important step although it is still very far from obtaining standardization.

Is then including standardisation in an Innovation Action of just 24 months sensible? We believe it is. It stimulated the search for standards and guided the design to create standardised solutions. It also motivated creating best practices, which is considered one of the valuable results of the project that is now encapsulated in the training platform.

It also assisted in achieving the impact objective of the 7SHIELD to standardise and demonstrate strategies and policies to prevent, early detect, response and mitigate of amalgamated attacks in physical and cyber manner.

The 7SHIELD framework has been tested through five Pilot Use Cases, consisting of several scenarios involving physical, cyber or combined cyber/physical attacks. Four operational tests and three demonstrations have been completed demonstrating that strategy of a holistic approach building customisable standardised components and specific hardware components is successful.

The NIS2 Directive together with the CER introduces new rules to strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage. In both directives Space is named as an important entity.

The Directives requires member states to put legislation in place to ensure critical entities meet the requirements in the Directives which in turn places additional responsibility on the ground segment developers to demonstrate they meet the legislation.

7SHIELD itself is moving to be a cloud-based service joining the growing market of Ground Segment as a Service (GSaaS). Originally offering satellite command and control and data reception GSaaS is now extending to include data links that connect it with its users. Adding to this the concept of processing on-board blurs the line between ground and space segment. With re-programmable satellites and distributed applications residing in space and on the ground security of the end-to-end process becomes complicated.

Technological progress is therefore presenting policy makers, ground segment developers and users with new challenges. A possible approach to address the technological progress would be to establish a New Space working group at CENELEC under JTC 5 to compliment the work being performed by WG6 “Upstream Standards” and WG7 “Future activities in space standardization”.

7. References

1. *EU space policy: Boosting EU competitiveness and accelerating the twin ecological and digital transition.* Evroux, Clément. s.l. : EPRS | European Parliamentary Research Service , February 2022 . PE 698.926.
2. Lightman S, Suloway T, Brule J. *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control.* . (National Institute of Standards and Technology, Gaithersburg, MD),. 2023 : s.n. NIST Interagency or Internal Report (IR) NIST IR 840.
3. *The Operations Security Concept for Future ESA Earth Observation Missions.* Fischer, Daniel & Bargellini, Pier & Merri, Mario. 2008. 9-. 10.2514/6.2008-3594..
4. IEC. Understanding IEC 62443. *Understanding IEC 62443.* [Online] 06 02 2021. [Cited: 10 03 2022.] https://www.iec.ch/blog/understanding-iec-62443.
5. BSI Germany. New Release C5-2020. [Online] 2020. [Cited: 10 03 2022.] https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html.
6. CSA. Cloud Controls Matrix and CAIQ v4. [Online] 2022. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.
7. ISO. ISO 22322:2015 Societal security - Emergency management - Guidelines for public warning. [Online] 2015.
8. —. ISO 22320:2018 - Guidelines for incident management. [Online] 2018. https://www.iso.org/standard/67851.html.
9. Physical Asset Protection Standard. [Online] ASIS, 2021. https://www.asisonline.org/publications--resources/standards--guidelines/physical-asset-protection/.
10. ISO. ISO 28000:2022. Security and resilience — Security management systems — Requirements. [Online] 2022.
11. Committee on National Security Systems. National Information Assurance Instructions for Space Systems used to support National Security Missions. [Online] https://www.cnss.gov/CNSS/openDoc.cfm?yY5LVU3nycwFPGkdyqzoFA==.
12. *ASIS GDL BC 01 2005 (R) titled "Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery".*
13. *FEMA Comprehensive Preparedness Guide (CPG)101: Developing and Maintaining Emergency Operations Plans.*
14. National Fire Protection Association (NFPA). *NFPA 1600 Standard on Disater/Emergency Management and Business Continuity Programs.*
15. National Institute of Standards and Technology. *NIST 800-61 Computer Security Incident Handling Guide- Recommendations of the National Institute of Standards and Technology.*

8. Annex I – Standards used in 7SHIELD

Reference	Description
ASIS GDL BC 01 2005	Business Continuity Guideline - A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery
CEN 60529 (IP Standards)	Degrees of protection provided by enclosures (IP Code) applies to the classification of degrees of protection provided by enclosures for electrical equipment with a rated voltage not exceeding 72,5 kV
ECSS-E-ST-40C	Standard for the software developed as part of a space project
EDXL	Emergency Data Exchange Language Distribution Element
ETSI TS 102 900 v1.3.1 (2019-02)	Emergency Communications (EMTEL) and European Public Warning System (EU-Alert) using the Cell Broadcast System
EU 2016/1148 NIS	European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
FEMA CPG 101	FEMA Comprehensive Preparedness: Developing and Maintaining Emergency Operations Plans.
GDPR	Regulation (EU) 2016/679 (General Data Protection Regulation)
IEC 31010:2019	Risk management — Risk assessment techniques
IEEE 802.11b/g/n standard (2.4GHz)	IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication
ISO 22301:2019	Security and resilience - Business continuity management systems - Requirements
ISO 22320:2018	Security and resilience — Emergency management — Guidelines for incident management
ISO 22322:2015	Societal security - Emergency management - Guidelines for public warning
ISO 22329:2021	Security and resilience - Emergency management - Guidelines for the use of social media in emergencies
ISO 9001:2015	Quality management
ISO Guide 73:2009	Risk management — Vocabulary
ISO/IEC 27001	Information security management systems (ISMS)
ISO/IEC 27017	Information Technology - Security Techniques - Code of Practice for Information Security Controls based on ISO/ITEC 27002 for Cloud Services
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO/IEC 31000	Risk Management - Guidelines
MIL-STD-810G	Test Method Standard, Environmental Engineering Considerations and Laboratory Tests
NIST 800-61	Computer Security Incident Handling Guide- Recommendations of the National Institute of Standards and Technology

OASIS CAP 1.2	OASIS Common Alerting Protocol v1.2 (http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.pdf)
RFC 4765	IDMEF v1 and the related proposed extension and the related extension IDMEFv2 v0.3, https://www.secef.net/idmefv2-first-draft-release/
RFC 7946	GeoJSON - Partially Reliable Stream Control Transmission Protocol (PR-SCTP) extension
RFC 8259	JavaScript Object Notation (JSON) lightweight, text-based, language-independent data interchange format

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