D6.1 – Exploitation, Dissemination, Standardisation Report- 1st Release

Editor(s): ED, GSH, HSE

Contributors: All Partners

Reviewed by: ED, JRCC

Quality Review by: ED

Official Submission Date: 2023-09-30

Actual Submission Date: 2023-09-30

Dissemination Level: Public

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073985

Copyright notice - Disclaimer

EURMARS project is funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or REA. Neither the European Union nor the granting authority can be held responsible for them.

Executive Summary

This Deliverable, titled "D6.1 Exploitation, Dissemination and Standardization Report," marks the initial release among the three planned for this project, focusing on the Exploitation, Dissemination and Standardization facets. It is rooted in Task 6.1, Task 6.2 and Task 6.3 with the following objectives:

First and foremost, its primary aim is to provide an overview of the exploitation plan that will be implemented both during and after the project's completion. This involves presenting the Key Exploitable Results of the project and attempting to discern individual exploitation strategies.

Secondly, the standardization aspect is multifaceted. On one hand, it seeks to investigate whether the project complies with, or should comply with, pertinent international and European standards. In addition to these standards, it was deemed highly advisable to ensure project's compliance with relevant regulations and directives, which are outlined in the respective annexes alongside the standards. On the other hand, project partners will explore the potential for participation in standardization initiatives in appropriate organizations, with the ultimate goal of contributing to ongoing standardization efforts and, ideally, creating a new standardization item or project.

Lastly, the Dissemination and Communication section offers a comprehensive overview of past and future activities in this domain. Its objective is to ensure that the project as a whole, or its individual components, reach as many target groups as possible and become established as promising solutions in maritime and border surveillance.

Table of Contents

Table of Figures

Table of Tables

List of Abbreviations

Terms	Description
ACM	Association for Computing Machinery
AI	Artificial Intelligence
AIS	Automatic Identification System
BNAE	The Aeronautics and Space Standardization Bureau
BT	Technical Board
CCMC	CEN-CENELEC Management Centre
CEN	European Committee for Standardization
CENELEC/CLC	European Committee for Electrotechnical Standardization
CEO	Chief Executive Officer
CIRAM	Common Integrated Risk Analysis Model
CSIRT	Computer Security Incident Response Team
CWA	CEN Workshop Agreement
DCP	Dissemination and Communication Plan
DG-JRC	The Joint Research Centre Initiative of the European Commission
DSS	Decision Support System
EARSC	The European Association of Remote Sensing Companies
ELOT	Hellenic Organization for Standardization
EN	European Standard
ENISA	The European Union Agency for Cybersecurity
ETSI	The European Telecommunications Standards Institute
EU	European Union
GA	Grant Agreement
GNSS	Global Navigation Satellite System
HE	Horizon Europe
IEC	The International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standardization
JTC	Joint Technical Committee
LEA	Law Enforcement Agency
ML	Machine Learning

NSB	National Standardisation Body
NWI	New Working Item
PIU	Passenger Identification Units
PNT	Positioning, Navigation and Timing
R&D	Research and Development
SDO	Standards Development Organization
SME	Small-medium Enterprise
SOC	Security Operations Centre
SoTA	State-of-the-art
TC	Technical Committee
TR	Technical Report
TS	Technical Specification
UAT	User Acceptance Tests
UAV	Unmanned Aerial Vehicle
UxVs	Any type of unmanned vehicle
WG	Working Group
WI	Working Item
WP	Work Package
WS	Workshop
UK	United Kingdom

1 Introduction

1.1 Overview

The EURMARS initiative, spanning three years (2022 - 2025), is a European Union supported endeavour undertaken by a group of 18 partners hailing from 13 different countries. Its primary objective centres around improving the observable efficacy of border surveillance systems during both singular and collective authority missions at Europe's offshore and coastal operations. This will be achieved through the creation, implementation, and validation of a revolutionary round-the-clock surveillance platform.

While the overarching goal of the EURMARS initiative seeks to augment the safety and governance of Europe's external boundaries, it is essential to accomplish this while adhering to a robust and eco-friendly methodology, in tune with the escalating border management market. Highlighting the novel facets of EURMARS is crucial as it simultaneously showcases the project's clear progress compared to existing market solutions. EURMARS, being a technologically superior border management system, will offer an agile, modular, and flexible solution capable of enhancing existing border management mechanisms. EURMARS, grounded in both technical and commercial scalability and sustainability, is poised to maintain its competitive edge while offering high-end services well into the foreseeable future.

Throughout the project's initial phase, a range of research, engagement, and development activities were conducted concurrently across all work packages, producing several results. The emphasis during the project's remaining duration will be on further fine-tuning these outputs, making them accessible to pertinent stakeholders and underlining their advantages in the context of border management. As per the definition provided by the European Commission, "Exploitation" implies the utilization of project outcomes in additional activities not covered by the project itself.

To ensure durability and sustainability, it's essential that EURMARS adopts and upholds a bespoke exploitation strategy designed to bring about tangible societal impacts. It's anticipated that the results obtained will continue to be applicable beyond the project's lifespan. Hence, for a successful exploitation strategy, it's crucial to recognize and categorize exploitable results within EURMARS, enabling an assessment of the project's overall impact. Additionally, identifying the project's most innovative outcomes and ways to leverage them will further boost interest, commercial viability, and marketability. However, it's acknowledged that not all project outcomes will be exploitable or reach the market; only those with the highest scientific, economic, or societal potential will.

In this context, comprehensive reports detailing both finished and upcoming exploitation activities are necessary, including the creation of the EURMARS exploitation framework and its three core phases. Additionally, a thorough strategic analysis will aid in understanding the exploitation landscape, identifying and characterizing key exploitable results, and discerning individual exploitation plans as defined by all consortium members. This analysis will form the groundwork for impending intellectual property rights and standardization activities, and establish future actions to ensure the long-term success of the EURMARS project.

Ongoing refinement of the exploitation strategy will allow the consortium to gain insights into definitive outcomes and potential opportunities for exploitation. This will be achieved through continuous engagement, allowing the consortium to collaboratively tweak and enhance the strategy towards the project's conclusion. The research methodology used to define the initial exploitation strategy considered multiple information sources, with the most valuable inputs coming from the consortium partners via a shared online document. This document followed a structured approach with guidelines, examples, and expected information to understand key exploitation aspects and derive conclusions. Other sources included the project grant agreement, other project deliverables submitted thus far, literature reviews, project meetings, communication with work package leaders, and knowledge gathered from similar projects.

1.2 Structure

The document is organised as follows:

Section 2 provides an overview of the exploitation strategy and its 3 main phases. Here, the objectives are to identify and transform EURMARS services and individual components into marketable products and as such to create profitable outcomes. These outcomes will be exploited via different routes by different stakeholder groups.

Section 3 addresses the challenges faced by Europe's border management systems in the maritime domain, including increased threats like smuggling and human trafficking, the need for information sharing and cooperation, technological advancements, surveillance and detection capabilities, and the legal and political complexities surrounding border management.

Section 4 provides the identification of the Key Exploitable Results (KERs). Here, the generated list represents most innovative results which have been achieved or will be delivered by the end of the project. Their exploitation potential is expected to have either a commercial, social or a scientific value.

Section 5 provides individual exploitation plans of all consortium partners. This includes results that are going to be exploited, market sector and customer segments, preliminary plans for exploitation channels, expected sales, and current achieved exploitation goals.

Section 6 provides an initial basis of an IPR strategy which is an essential requirement for a successful exploitation. This includes an overview of the background technologies and know-how that the consortium partners are bringing in the project, as identified in the Consortium Agreement, as well as an overview of foreground technologies and know-how generated by partners.

Section 7 provides an overview of the EC provided HORIZON Results Booster services provided by the EC, as EURMARS will take advantage of this initiative and explore the possibilities to boost its impact.

Section 8 provides a general description of standards, regulations and directives, offers an overview of the standardization landscape and outlines the activity plan and future steps related to standardization.

Section 9 covers core dissemination and communication activities, including past actions and future planning in these domains. Dissemination activities encompass scientific publications, clustering with related European projects, participation in relevant events, meetings with policy makers and regulators, and the potential for thematic workshops. Additionally, the section presents the main communication channels, such as the website, social media, newsletters, etc. Finally, it contains all relevant dissemination and communication materials and the evaluation plan.

2 EURMARS exploitation strategy

The primary aim of the exploitation strategy is to recognize and convert the services and individual elements of EURMARS into market-ready products, thereby generating profitable returns. To introduce the EURMARS solution to the market, a systematic and methodical strategy must be established and executed. This custom-made commercialization plan will enable the maximization of the project's impact through suitable business models. The primary objective here is to formulate strategies for leveraging the project outcomes and investigating their broader application, sustainability, and business viability.

Moreover, given the project's complexity and the consortium's size, it is crucial to effectively coordinate and distribute the partners' efforts, track progress, and plan activities throughout the project's duration. It is also important to lay out future actions to ensure the successful continuation of the EURMARS project beyond its lifespan. A well-organized consortium, like that in EURMARS, significantly influences the project's commercialization outcomes, where suitable and relevant stakeholders will assist in gaining a better market understanding. Consequently, it will simplify the definition and commercialization of key EURMARS products and services, and include additional stakeholders such as decision-makers, governments, etc.

2.1 Exploitation routes

EURMARS will generate various scientific, research, engagement, and development outcomes, which hold high potential for commercialization in different ways by different stakeholder groups. The EURMARS consortium has identified the following initial commercialization pathways: scientific, commercial, and exploitation by/through networks, associations, initiatives, policy groups.

2.1.1 Scientific exploitation

Researchers can contribute to advanced border management solutions, the development of innovative ideas and tools as the key to enhancing the dynamics of awareness methods to manage security risks in the maritime domain. The identified scientific commercialization objectives of the knowledge produced by EURMARS are:

- Promote awareness of the project's outcomes and their benefits by reaching both academic and practitioner target groups.

- Establish trust in the EURMARS brand and all the solutions and services derived from this project.

- These objectives can be achieved through the execution of several scientific commercialization activities, such as academic publications and conference participation. EURMARS partners have been very active. They have participated, and plan to participate in several venues.

- Other potential scientific commercialization measures are currently being explored: blog posts, action plans/research roadmaps, policy papers/recommendations, informative pieces/news and press releases, internal and external newsletters, handbook, etc.

2.1.2 Commercial exploitation

The objective of commercial exploitation is to convey the accomplishments and insights gained from EURMARS, as well as to stimulate interest and market demand for the final products of EURMARS. The industrial collaborators will leverage their extensive networks at both the European and national levels to disseminate the outcomes of the EURMARS project, attract attention, and enhance its prominence. The groups targeted in this process include:

- **European industry:** Marketing campaigns and in-house presentations to increase public awareness and commercialise the results of EUMARS.

- **Strategic Partners:** Identify and collaborate with strategic partners who can help in the distribution, implementation, or integration of EURMARS solutions. These could be other technology companies, consulting firms, or organizations in the maritime industry.

- **End Users:** Conduct training and awareness programs for end users to ensure they understand the benefits and functionality of EURMARS solutions. This could include security personnel, maritime operators, and other relevant stakeholders in the maritime domain.

2.1.3 Networks, associations, initiatives, policy groups

Partners of EURMARS are affiliated with or collaborate with various networks and initiatives, in addition to their involvement in several ongoing projects. They will establish connections with potential external collaborators and projects, ensuring that any outcome or strategy from EURMARS related to interoperability, standards, and security, along with business validation and sustainability, can be grouped together. The outputs of EURMARS will be leveraged through other networks and by engaging with policy makers to amplify the reach and impact of the primary project results. This will have a beneficial effect and will shape the future innovators in the cyber security industry;

scholarly debates and discussions may provide fresh perspectives for the project results, fostering innovation and leading to job creation throughout Europe.

EURMARS aligns with the European Commission's objective of providing security for all EU citizens, by pooling all accessible resources and intelligence and by fostering collaboration among completed and ongoing projects and initiatives, which will generate inventive security solutions.

On the list to follow we identify several potential areas of collaboration, where EURMARS will be able to align with its primary objectives regarding security for all EU citizens by synergies with completed projects that bring their gained knowledge and documented experiences, such as:

- **algorithms sharing, fusion and data analysis** (where FOLDOUT, IPATCH, EFFECTOR, I2C and ANDROMEDA can share their lessons learned and know-how on information fusion and sensory data augmentation, on object detection and classification, and on high level modelling of behaviour analysis, with FOLDOUT's ML predictors, when combined with all aforementioned competencies, can enhance EURMARS's ability to effectively detect, classify and predict/prevent threats).

- **the shared intelligence, situational awareness and threat assessment** (where IPATCH and FOLDOUT monitor around and outside the immediate border area pre-events and provide alerts using DSS tools, EFFECTOR and ANDROMEDA emphasize the use of platforms like CISE and EUROSUR and have the primary objective of monitoring and assessing real-time threats, and OCEAN2020 uses the "system-of-systems" approach to enhance situational awareness. All these projects include technologies that can be leveraged by EURMARS to enhance efficiency and effectiveness on all three of the aforementioned project's aspects).

- **insights on sensor integration** (where IPATCH operators and experts may offer more comprehensive tips regarding the installation, capabilities and challenges related to multispectral sensor suites used as surveillance solutions).

- **counter-piracy measures and recommendations** (where IPATCH, given its in-depth analysis on counter-piracy measures, can provide insights for EURMARS's specific challenges regarding ways to deal with developing threats at the maritime borders).

- **hybrid architecture** (where ANDROMEDA's hybrid architectural approach can offer EURMARS the flexibility to utilize existing CISE nodes/gateways while also testing and validating newer data models and solutions).

- **interoperability** (where OCEAN2020 emphasizes on synergetic compatibility to align with EU/NATO standards, and ANDROMEDA with CISE-compatible command and control systems, EUMARS can benefit by adapting universally designed solutions to integrate seamlessly with existing surveillance systems).

- **enhanced search & rescue scenarios** (where, besides border surveillance, FOLDOUT's focus on such scenarios can benefit EURMARS, especially in maritime rescue missions).

- **past trials, demonstrations and impact assessment** (where OCEAN2020, EFFECTOR and ANDROMEDA can offer real-world pilot insights – including the leveraging information gained from research projects like PERSEUS, CloseEye, MARISA, and RANGER) as they emphasize in diverse maritime environments, and thus provide EURMARS with important lessons-learned regrading live and simulated trials as well as in translating results into scientific and commercial exploitation approaches).

- **user involvement, human factor and barriers removal** (where OCEAN2020 can be addressed as a manual serving with its guidelines for EURMARS, taking into consideration the operator HUI needs, operational, functional and responsiveness obstacles, creating a tailored system specifically on the evolving maritime security challenges, while establishing trust on the project's brand and ensuring effective utilization of the respective solutions on the maritime personnel).

Furthermore, EURMARS partners are participating in several other projects, to further enhance interoperability and intelligence and, subsequently, to increase the quality of outcomes by collectively streamlining the factors that guarantee security for all EU citizens. The EURMARS results will be utilized in collaboration with policymakers, amplifying the reach and effect of the project's objectives. On an academic level, all available resources will be consolidated to create directions towards innovation spurring and the creation of employment opportunities throughout Europe.

2.2 Exploitation phases

The exploitation strategy comprises the EURMARS consortium, which consists of partners from industry, academia, and research. These partners collectively contribute to the overall EURMARS exploitation effort. The strategy relies on the utilization of technologies and solutions that serve as the foundation for EURMARS. These encompass a range of products, services, and knowledge, referred to as Key Exploitable Results (KERs).

Through the acquisition of results and experiences, the core of the exploitation strategy is further developed. This strategy is executed through three continuous phases: A, B, and C, which are implemented throughout the project's duration. Each of these exploitation phases is meticulously structured and planned, incorporating predefined meta-activities such as pre-marketing, exploitation ramp-up, and market penetration. The primary objective is to establish a robust market position for EURMARS' innovative border management solutions and services, aligning them with

the needs of the target exploitation groups. Consequently, all exploitation actions are carefully defined to ensure timely contributions from partners and efficient utilization of resources.

The overall EURMARS exploitation framework will be executed through three main exploitation phases, meticulously designed based on market analysis, business planning, exploitation actions, and continuous monitoring. These three phases are as follows:

Phase A | Initial pre-marketing activities: This phase involves technology mapping, market analysis, and trend identification. Through market analysis, the border management landscape, existing suppliers, available products and services, impactful trends, competitors, and relevant stakeholders are assessed. Based on these insights, initial business models are proposed, which will be further developed as the EURMARS platform progresses.

Phase B | Exploitation ramp-up: This phase focuses on identifying values, strengths, competencies, and potential issues. As the project advances, results and the overall direction become clearer. Strategic analysis, identification of key exploitable results, initiation of interoperability and standards, as well as mapping of intellectual property rights (IPR) are carried out during this phase. The primary objective is to establish a strong market position for EURMARS' innovative border management solutions while aligning them with the needs of the target exploitation groups. The exploitation actions involve identifying the project's key exploitable assets and exploring challenges and gaps in border management systems. Additionally, each partner develops and updates their individual exploitation plans and defines pre-commercial agreements through the identification of background and foreground technologies.

Phase C | Market penetration: This phase encompasses business scenarios, joint exploitation, promotion, and future planning. The activities planned for this phase are subject to change based on the project's progress and maturity. Currently, Phase C includes the definition of potential business scenarios, creation of a business model canvas, customer targeting through brochures, digital marketing materials, and online promotion, financial planning and pricing models, licensing and IPR considerations, joint exploitation activities, and planning for follow-up projects. Simultaneously, the EURMARS project will fully embrace the Horizon Results Booster initiative to maximize its exploitation potential.

During the initial phase of the project, some crucial information required for a comprehensive exploitation strategy may not be available. As a result, the development of the initial strategy will be deferred to the second reporting period. During this phase, partner exploitation activities will be intensified whenever possible, and all consortium partners interested in the project will collaborate to define a joint business plan.

In this context, the exploitation actions aim to identify the main exploitable assets of the EURMARS project, which will serve as a foundation for targeted communication and dissemination efforts. By utilizing various communication channels such as the project’S website, news outlets, social media

platforms, infographics, publications, and live demonstrations, the project will effectively reach its main interest groups, potential customers, and target audiences, including EU industry stakeholders, academia, industry customers, end-users, experts, policy makers, networks, and relevant projects and initiatives.

3 Strategic analysis

Border management systems play a critical role in safeguarding national security, facilitating trade, and managing the movement of people across international borders. In the context of Europe, with its extensive coastline and reliance on maritime trade, effective border management in the maritime domain is of utmost importance. However, this area presents unique challenges that require careful attention and innovative solutions. This analysis aims to identify the current challenges faced by Europe's border management systems, with a specific focus on the maritime domain.

3.1 Increased Maritime Threats

Europe's maritime domain is susceptible to various security threats, including smuggling of drugs, and human trafficking. Criminal organizations take advantage of the vastness and complexity of the maritime environment to carry out illicit activities, often evading detection and interception by border management agencies.

The extensive coastline of Europe, coupled with numerous ports and multiple entry points, presents a significant challenge for effectively monitoring and controlling maritime borders. Criminal networks exploit these vulnerabilities by using small vessels, fishing boats, and other means to transport illegal goods and individuals across borders.

Human trafficking, is another pressing issue in Europe's maritime domain. Desperate individuals seeking better lives or fleeing conflict often resort to dangerous sea crossings. Smugglers exploit their vulnerability, endangering lives and profiting from human misery. These irregular migration flows put a strain on border management agencies, as they need to balance the responsibility of ensuring border security with the humanitarian aspect of the migration crisis.

Addressing these increased maritime threats requires robust and coordinated efforts by border management agencies. Enhanced surveillance capabilities, including radar systems, coastal patrols, and aerial surveillance, are necessary to monitor maritime borders effectively. Collaboration with international partners and intelligence agencies is vital to gather timely and accurate information on criminal networks involved in maritime smuggling activities. Moreover, investing in training and capacity building for border control officers is crucial to improve their ability to identify and respond to maritime security threats.

3.2 Information Sharing and Cooperation

Effective border management requires seamless cooperation and sharing of accurate information. However, there are significant challenges in achieving this goal. One major obstacle is the differences in systems, procedures, and legal frameworks across European Union (EU) member states. These differences often hinder smooth cooperation, resulting in gaps in intelligence sharing and coordination efforts. The lack of harmonization and standardization in information sharing processes can impede the ability to respond effectively to maritime threats. Without a cohesive framework for sharing information, it becomes challenging to identify patterns, track criminal activities, and prevent illicit actions in the maritime domain.

To address these challenges, it is necessary to establish mechanisms that facilitate information sharing and cooperation among relevant stakeholders. This may involve developing common platforms, protocols, and procedures for sharing intelligence in real-time. Additionally, there is a need for greater coordination in the collection, analysis, and dissemination of information related to maritime security threats. By improving information sharing and cooperation, border management agencies can enhance their situational awareness, respond more effectively to maritime security threats, and mitigate risks to national security and public safety. It requires a collaborative approach, involving the alignment of legal frameworks, standardization of procedures, and the development of interoperable systems that enable seamless communication and information exchange between relevant agencies.

3.3 Technological Advancements

Advancements in technology, are being utilized by criminal networks. This requires border management agencies to adapt and develop sophisticated technological solutions to effectively address these emerging threats. The pace of technological advancements often outpaces the capabilities of existing border management systems. This misalignment poses several challenges for border management agencies. One of the challenges is resource allocation. Keeping up with rapidly evolving technology requires substantial investments in acquiring new equipment, upgrading infrastructure, and implementing advanced systems. Limited resources can hinder the ability of agencies to adopt and integrate these technologies effectively. Another challenge is training. Border management personnel need to be trained in operating and maintaining new technologies. Training programs must be developed and implemented to ensure that the staff has the necessary skills and knowledge to utilize these advancements effectively.

Furthermore, the integration of new technologies with existing border management systems can be a complex task. Legacy systems may not be compatible with the new technologies, requiring agencies to invest in system upgrades or develop customized solutions. Seamless integration is essential to ensure the smooth functioning of the overall border management system.

However, technological advancements also have the potential to enhance border management in Europe's maritime domain. Advanced surveillance technologies can improve the monitoring and detection capabilities of border management agencies. These technologies can aid in the identification and tracking of small vessels engaged in illicit activities, thereby strengthening security measures. To overcome the challenges posed by technological advancements, continuous improvement and collaboration among stakeholders is of utmost importance. Investment in advanced surveillance technologies is recommended, along with capacity building initiatives to enhance the skills and expertise of border management personnel. Additionally, harmonization of legal frameworks is crucial to facilitate the integration of new technologies across different European Union (EU) member states and ensure a coordinated approach to border management.

3.4 Surveillance and Detection Capabilities

Limited resources and outdated equipment hinder the ability to detect and track vessels engaged in illicit activities. The lack of real-time situational awareness further compounds these challenges. Border management agencies may not have sufficient coverage of remote or less frequented areas, which can be exploited by criminal organizations.

To address these challenges, border management agencies require advanced surveillance technologies. These technologies could include optical sensors, UAVs, and satellite surveillance. These tools can enhance the ability to detect and track vessels engaged in illicit activities, providing crucial situational awareness to the authorities.

However, the pace of technological advancements often outpaces the capabilities of existing border management systems. This creates a challenge in terms of resource allocation and training. Agencies need to invest in acquiring and integrating new technologies while ensuring that their personnel are trained to effectively use and interpret the data provided by these systems.

Overall, improving surveillance and detection capabilities in Europe's maritime domain is crucial for effective border management. By investing in advanced technologies, expanding coverage, and providing adequate training to personnel, border management agencies can enhance their ability to detect and intercept illicit activities, ensuring the safety and security of maritime borders.

3.5 Legal and Political Complexities

In the context of border management, legal and political complexities arise from several factors:

- Disparities in Legal Frameworks: European Union (EU) member states often have different legal frameworks and approaches to border management. These disparities can create challenges in harmonizing border management practices across the region. Varying laws and regulations regarding immigration, asylum, and border control make it difficult to establish consistent procedures and guidelines.

- Differing Approaches to Immigration Policies: European countries may have different perspectives and approaches to immigration. Some countries may prioritize strict border control measures, while others may adopt more lenient or humanitarian-oriented policies. These differing approaches can lead to challenges in achieving a unified and coordinated approach to border management.

- Political Sensitivities: Border management issues can be politically sensitive, especially in the context of migration. Public opinion, political ideologies, and electoral considerations can influence decision-making processes and policy formulation. Political sensitivities surrounding immigration and border control can hinder the development and implementation of effective border management strategies.

- Human Rights and International Obligations: Border management systems must navigate the complex intersection of border security and the protection of human rights. Respecting international obligations, such as the right to seek asylum, non-refoulement (protection against returning individuals to a place where they may face harm), and the principle of non-discrimination, is crucial. Policymakers and border management agencies face the challenge of upholding security, while ensuring compliance with human rights standards and international legal obligations.

Addressing these legal and political complexities requires a comprehensive and coordinated approach. Policymakers need to strike a balance between ensuring border security and protecting human rights. This may involve harmonizing legal frameworks and procedures across EU member states, fostering greater cooperation among relevant stakeholders, and promoting dialogue and information sharing to develop effective and inclusive border management strategies.

By proactively addressing the legal and political complexities, European countries can enhance their border management systems and ensure the safety and security of their maritime borders while upholding human rights standards and international obligations.

4 EURMARS Key Exploitable Results

During the initial phase of the project, the consortium conducted a preliminary identification of the Key Exploitable Results (KERs), which are listed in Table 1. This list comprises the most innovative outcomes that have been achieved or are expected to be delivered by the project's completion. These results possess potential for commercial, social, or scientific exploitation. Exploitable results encompass various forms such as equipment, hardware, processes, products, services, knowledge and intellectual property (including publications and patents).

Table 1. Key Exploitable Results

No.	KER	Partner(s)
1	EURMARS Integrated System	Technical developers (ED, AIT, UREAD, VTT, GSH, HSE, SKYLD, SPACE-SI,TASF, ONERA, HSE)
2	EURMARS Systems	Technical developers (ED, AIT, UREAD, VTT, GSH, HSE, SKYLD, SPACE-SI, TASF, ONERA, HSE)
2.1	Coastal Ground Altitude Sensing Systems	AIT
2.2	Low Altitude Sensing Systems	SKYLD
2.3	earthLive Simulation Platform	TASF
2.4	High Altitude Sensing Systems	ONERA, TASF
2.5	Satellite Based Systems	GSH, SPACE-SI
2.6	Common Data Hub	HSE
2.7	Multimodal Data Fusion Platform	UREAD
2.8	Registration, Communication & Coordination of Subsystems	ED
2.9	Collaborative C2, Visualization & Alarming	ED
2.10	Data-Driven Risk Assessment Tool	UREAD
2.11	Decision Support System	HSE
3	Secure interoperable architecture	ED

4	Stakeholder requirements supporting use case and technical development, validation and user acceptance	All partners
5	EURMARS platform blueprint operationally validated in real life scenarios and three Pilot Use Cases	All partners
6	Benchmark dataset	UREAD, end-users
7	AI Foresight Report and Blueprint, PIA, EIA and SIA assessment	TRI
8	Contribution to international standards	GSH

Next step is to carry out the characterisation of the identified results using a systematic approach. Here, the characterisation focuses on the assessment of the results' technological maturity using the Technology Readiness Level (TRL) framework, as shown in Table 2. In any case, after the end of the project, the identified results will potentially need further development, refinement, optimisation, or investment before they can be fully exploited commercially. Furthermore, several additional parameters are used to define the results in context of innovation, uniqueness, market potential, IPR measures:

- **Description:** Brief description about the result.
- **What problems are solved:** What problems does the result solve? / Why has this result been achieved in EURMARS?
- **Innovativeness/new approach:** What is the new element/approach/innovation of the result that distinguishes it from the state of the art?
- **Unique selling point:** In what way is the solution better (faster, cheaper, more reliable, more efficient, with less undesired effects)?
- **Competitors (solutions):** Who are the main competitors of the result?
- **Target users / customers:** Who will potentially use the result?
- **Benefits for users / customers:** What benefit will the result bring to end users? Why should the end users invest in or adopt the result?
- **TRL level:** Estimation of the result's technology maturity.

- **Main technical challenge(s):** What are the main technical challenges, which need to be or were solved?
- **Legal / ethical requirements:** Legal, normative, or ethical requirements (Is there a need for authorisations, compliance to standards, norms, etc.?).
- **Involved partners:** Who are the principal partners involved in the delivery of the result?
- **IPR protection:** Does the result need to be protected? How? When?

Table 2. Technology Readiness Level (TRL) framework

TRL	Description
TRL 1.	basic principles observed
TRL 2.	technology concept formulated
TRL 3.	experimental proof of concept
TRL 4.	technology validated in lab
TRL 5.	technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 6.	technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
TRL 7.	system prototype demonstration in operational environment
TRL 8.	system complete and qualified
TRL 9.	actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

4.1 EURMARS Integrated System

KER 1: 4.1 EURMARS Integrated System	
Description	EURMARS Integrated System is a ground-breaking innovation that enhances sensor and platform capabilities to detect critical objects of interest. It integrates a set of high-altitude and ground-based sensors deployed by consortium members, simulations of upcoming high-altitude sensors, along

	with integrated services by accessing EU services. It also includes a modular architecture enabling a plug and play concept.
What problem(s) are solved	■ Limited coverage and endurance of existing surveillance systems: Current systems rely on ground-based or lower altitude aerial assets with constrained geographic reach and operation time. EURMARS introduces higher altitude and satellite platforms for persistent wide area coverage. ■ Data isolation and lack of interoperability: Existing systems tend to have proprietary data formats and interfaces that restrict information sharing and joint operations. EURMARS integrates diverse data sources into a common architecture. ■ Gaps in detection capability: No single system currently provides robust detection across all vessel types and sizes, especially smaller boats involved in illegal activities near the shoreline. EURMARS fuses data from multiple sensors to fill these gaps. ■ Lack of continuity between maritime and land operations: Most systems focus on either the maritime or land domain. EURMARS supports handover between sea, coastline and inland surveillance. ■ Limited autonomy and poor reliability: Current systems have high maintenance needs and poor resilience. EURMARS redundancy and advanced analytics aim to enhance autonomy and reliability. ■ Insufficient situational awareness: Existing systems do not provide a comprehensive common operational picture accessible to all relevant authorities. EURMARS collaborative platform addresses this.
Innovativeness / new approach	Integration of High-Altitude Sensors: The system integrates high-altitude sensors, including existing satellite-based systems and sensors, existing drones/UAVs equipped with multimodal sensors, and simulated Stratobus stratospheric airship enabling long endurance, long range, high fidelity multimodal imaging. This integration enhances the system's ability to detect critical objects of interest from long distances. State-of-the-Art Multimodal Data Fusion and AI-Based Sensor Analytics: The system leverages state-of-the-art multimodal data fusion and AI-based sensor analytics to improve the performance of classical thermal/RBG

	sensors which are severely lowered by certain environmental conditions (e.g., fog, dust).
Unique selling point	■ Wider geographic coverage and scope of surveillance spanning maritime, coastal and inland domains. ■ Longer endurance and persistence from high altitude aerial and space-based platforms enabling 24/7 monitoring. ■ Enhanced reliability and complementarity of detection across multiple sensor types and altitudes. ■ Increased autonomy and resilience provided by redundancies in the system architecture and analytics. ■ Interoperability and seamless data integration from the diverse sensor network and external systems. ■ Advanced AI and data fusion capabilities for improved detection, classification, tracking, risk assessment. ■ Comprehensive common operational picture accessible securely to multiple authorities and users. ■ Flexibility and modularity to readily integrate with next-generation platforms and national systems. ■ Cost-effectiveness from efficiently clustering existing platform investments and open standards. ■ Accelerated capability development and deployment by building on proven technologies.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	Border and coast guard authorities responsible for maritime and land surveillance
Benefits for users / customers	Enhanced situational awareness and common operating picture from the fusion of diverse data sources. Provides a more complete real-time view of the surveillance domain.

	Improved detection, especially of smaller vessels involved in illegal activities, through the layered sensor network. Earlier discovery of potential threats. More accurate analytics and reduced false alarms via advanced AI and algorithms applied to aggregated data. Increased autonomy, permanence, and reliability of surveillance from high altitude aerial and satellite platforms with long endurance orbits. Reduces costs of conventional air/sea patrols. Easier coordination between authorities and handing over of events between land and maritime domains. Flexibility to readily integrate new sensors, data sources and analytics modules via open architecture. Future-proofs investment. Interoperability with existing national systems like EUROSUR via standard interfaces. Leverages legacy platforms. Enhanced evidence collection by recording data from multiple sensors. Supports prosecution of illegal activities. Modular and scalable architecture allows incremental adoption and spreading of costs over time.
TRL level (1-9)	5-7
Main technical challenge(s)	Achieving effective integration and interoperability between the heterogeneous sensor platforms and external systems. This includes handling different data formats, interfaces, update rates, etc. Developing robust detection, classification and tracking algorithms that can leverage the diverse multi-modal sensor data. Algorithms need to be accurate in complex maritime environments. Implementing advanced sensor fusion that can handle uncertainty, conflicting data, and variability in sensor coverage and quality. Meta-fusion with external data sources also needs to be addressed. Enabling efficient information sharing and handover between the different authorities involved in land and maritime monitoring. This includes role-based access control and filtering. Developing user-centric interfaces and visualization that provide actionable intelligence to operators and assist multi-agency collaboration. Achieving reliable operation and fault tolerance given the mix of aerial, ground and space segments. Communication links are also vulnerable, especially to UAVs.

	Handling large amounts of heterogeneous streaming data from the multitude of sensors and platforms. Scalability of data ingestion, fusion and analytics. Protecting platform and information security given the involvement of multiple stakeholders across land and maritime domains. Planning and executing complex field deployments involving diverse assets across sea, air and land. Logistic challenges.
Legal / ethical requirements	Compliance with data protection laws like GDPR for any collection or processing of personal data. Necessitates privacy by design and data minimization. Adherence to ethical principles and human rights laws regarding use of surveillance technologies. Requires transparency, accountability, and oversight mechanisms. Implementation of cybersecurity measures to protect systems and data from unauthorized access or misuse. Relevant standards like ISO 27001 should be followed. Acquiring necessary authorizations for operation of remote sensing platforms like UAVs. Ensuring non-discrimination and avoidance of bias when using algorithmic analytics for detection and risk assessment. Conducting prior impact assessments on human rights, societal risks, and dual-use concerns. Adapting operations based on judicial rulings and legal opinions that may emerge on surveillance technologies. Following best practices like security and privacy by design and building ethics capacity of practitioners. Updating procedures continually as regulations and standards evolve around security technologies and data usage.
Involved partners	All Partners
IPR protection	Cannot be estimated at current stage

4.2 EURMARS Subsystems

4.2.1 Coastal Ground Sensing Systems

KER 2.1: Coastal Ground Sensing Systems	
Description	The coastal ground sensing systems consists of **2 dedicated optical smart sensing solutions** integrating automated object detection, tracking and classification for different target areas: ■ Maritime Smart Sense Camera Sub-System responsible to generate geo-referenced detection events for ships and small vessels and to track them as long as they are in the field of view of the camera (up to 800m). A classification of the type of the ship is also foreseen. The camera system is a mast mounted, steerable camera system, controlled by an operator, with AI detection and short term-tracking and will automatically scan (sweep over) a sea or costal area following a predefined path. ■ Land Smart Sense Camera Sub-System responsible to generate geo-referenced detection events for persons and vehicles and track them, as long as they are in the field of view of the camera. A classification of the type of the vehicle is also foreseen. The camera system is a mast mounted, steerable camera system, controlled by an operator, with AI detection and short term-tracking for land observation (up to 200m); ■ Vessel/Vehicle Classification Sub-System responsible to identify and classify the detections provided by the camera systems, through the use of deep learning techniques; ■ Behaviour Analysis/Anomaly Detection Sub-System responsible to automatically recognise defined behaviours of detected and tracked objects, by generating a series of behaviours based on analysing the movements of the targets. The focus of behaviour detection will be on anomalous behaviours that have been manifested from the end-user requirements. It will make use of object detection and tracking information provided by the camera systems; **Additional to the optical sensing solutions, a Behaviour Analysis/Anomaly Detection Sub-System** is developed and responsible to automatically

	recognise defined behaviours of detected and tracked objects, by generating a series of behaviours based on analysing the movements of the targets.
What problem(s) are solved	The 2 dedicated optical smart sensing solutions are able to trigger the initial georeferenced alarms of target objects of the EURMARS system from the coast. The behaviour detection system extracts the anomalous behaviours that have been manifested from the end-user requirements. It will make use of all georeferenced alarm information.
Innovativeness / new approach	The innovation on the optical smart sensing solutions is that the combination of sub-sensors is selected in the way that they provide relevant raw data to achieve the best performance with the chosen detection/ tracking/ classification algorithms for most weather conditions. E.g., high performance in foggy situations, high performance for day and night situation in land scenarios. Additionally, to the sensor innovation the algorithmic frameworks are chosen and trained for the target use cases, e.g., improved performance for vessel-detection/tracking/classification. The sensing solutions are designed in that way that they are transportable to chosen selected areas and can cover a bigger monitoring area by scanning with an automated PT unit. Abnormal behaviour algorithm is designed for specific end-user requirements. The algorithm can detect abnormalities based on historical data and on the different types of data sources.
Unique selling point	■ Affordable and transportable target detection systems, providing high performance for bad weather conditions for land and maritime scenarios ■ Detection of abnormal behaviour based on historical data
Competitors (solutions)	■ Maritime system: Flir Triton, Axis Q87, Hikvis. DS-2TD6266 ■ Land: Bertin Exensor (Scout Mk3)
Target users / customers	Border Guard Authorities, Sensor developers, System integrators
Benefits for users / customers	Transportability of systems improve scalability options for surveillance systems and therefore this reduces costs. High performance of automated detection systems improves the security at the relevant areas because the end-users get better support.

	All data will be in digital form, therefore it can be stored easily for reporting.
TRL level (1-9)	7
Main technical challenge(s)	Systems should work in difficult weather situations and different types of objects at different distances
Legal / ethical requirements	Algorithms should work well for all persons and should not be biased Compliance with data protection regulations like GDPR when handling any personal data
Involved partners	AIT: HW of the Optical Smart Solutions; object detection & tracking UoR: Object classification, Abnormal behaviour algorithm
IPR protection	Innovation is integrated in a closed SW and has to be protected by copyright; interfaces are open. Patent and brand are foreseen for the future.

4.2.2 Low Altitude Sensing Systems

KER 2.2: Low Altitude Sensing Systems	
Description	Aerial Video Surveillance – through UAV - generating reliable geo-referenced detections and tracking of ships and small vessels, persons in distress in real-time under marine environment, away from the costal line (up to 15km).
What problem(s) are solved	■ **Verification and confirmation of** abnormal events (ships/ vessels, oil spill) triggered from other components of EURMARS Solution (coastal ground sensing systems, high altitude sensing systems) ■ Further **identification and classification** of detected objects/events ■ **Tracking of** their evolution as long as the UAV flies above of the targeted sea area ■ **Surveillance of wide sea areas** providing Situational Awareness and actionable data, enhancing decision support.
Innovativeness / new approach	■ **AI and Machine Learning Integration:** Incorporating Artificial Intelligence (AI) and Machine Learning (ML) algorithms into low altitude sensing systems (airborne video processing) enables real-time data analysis and decision-making. This allows for adaptive, abnormal

	events detection, track and trace the annotated objects at the sea terrain in real time. ■ **Edge Computing:** Edge computing involves processing data locally on the sensor or device rather than sending it to a centralized server. This approach reduces latency and allows for faster decision-making, critical in applications like autonomous vehicles and drones. ■ **Non-Invasive Sensing:** Advancements in non-invasive sensors, such as passive optical sensors or hyperspectral imaging, enable the collection of data without physical contact with the target object.
Unique selling point	■ **Precision and Accuracy:** Drone's Sensing Systems offer high levels of precision and accuracy in altitude or height measurements, making them essential for applications where precise height information is critical, such as surveying. ■ **Real-time Data:** Provision of real-time processed data feedback, allowing operators to make informed decisions quickly. This is crucial for applications like search and rescue, where time is of the essence. ■ **Cost-Effective Solutions:** Some sensors and systems offer cost-effective alternatives to more complex technologies, making them accessible to a wide range of industries and applications. ■ **Ease of Use:** User-friendly interfaces and integration capabilities make these systems accessible to a wide range of users, from novice drone operators to experienced professionals.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	Border and coast guard authorities, LEAs, Security companies
Benefits for users / customers	■ **Search and Rescue Operations:** More effective search and rescue missions by rapidly locating missing individuals or disaster survivors using low altitude sensing systems equipped with thermal imaging and night vision capabilities. ■ **Data-Driven Decision-Making:** Access to real-time and high-resolution data for informed decision-making, helping organizations/end users

	optimize processes, allocate resources, and respond to changing conditions effectively. ■ **Customization and Versatility:** Flexibility to tailor low altitude sensing systems to specific needs and applications, making them adaptable for a wide range of use cases. ■ **Remote Sensing and Surveillance:** Remote monitoring and surveillance capabilities, enabling end users and security personnel to maintain awareness and respond to incidents promptly. ■ **Cost-Effective Solutions:** Some sensors and systems offer cost-effective alternatives to more complex technologies, making them accessible to a wide range of end users. E.g., is rather low cost to survey a wide sea with a drone rather with a boat, which is more expensive and demands more human assets with specific skills.
TRL level (1-9)	5-7
Main technical challenge(s)	■ **Environmental Conditions:** Adverse weather conditions, such as rain, snow, fog, and strong winds, can affect sensor performance and navigation accuracy. Developing sensors and algorithms that can function effectively in a variety of weather conditions is a significant challenge. ■ **Sensor Integration:** Drones operation rely on multiple sensors, such as cameras, radar, and GPS, to gather data for navigation and obstacle avoidance. Integrating these sensors and fusing their data in real time while minimizing errors and redundancies is complex. ■ **Data Processing and Computation:** The vast amount of data collected by sensors, especially in high-resolution mapping and surveillance applications, requires significant processing power. Efficient data processing and onboard computation are crucial for real-time decision-making.
Legal / ethical requirements	Flying drones, is subject to a range of legal and ethical requirements to ensure safety, privacy, and responsible use. These requirements may vary by country or region, but some common legal and ethical considerations include: ■ Safety Regulations:

	○ Compliance with aviation authorities: Depending on the country, drones and other low altitude vehicles may need to adhere to regulations set by aviation authorities, such the European Union Aviation Safety Agency (EASA) in Europe. ○ Altitude limits: There are often altitude limits imposed on unmanned aircraft to prevent interference with manned aircraft and ensure safe operations. ○ Collision avoidance: Systems must incorporate collision avoidance measures to prevent accidents and collisions with obstacles or other aircraft. ○ Emergency procedures: Operators must have procedures in place for emergency situations, such as equipment failures or loss of control. ■ Privacy Regulations: ○ Data collection and storage: Collection and storage of data, including images and videos, must comply with privacy laws and regulations. Consent may be required for data capture in certain scenarios. ○ Avoidance of sensitive areas: Some jurisdictions may prohibit or restrict the use of drones and other low altitude systems near sensitive locations, such as military bases, nuclear facilities, or private properties. ■ Ethical Considerations: ○ Respect for privacy: Operators and users should respect the privacy of individuals and property when capturing images or conducting surveillance at low altitudes. ○ Responsible use: Users should operate low altitude sensing systems responsibly, avoiding harassment or intrusion into private spaces. ■ Data Security and Cybersecurity:

	○ Protection of data: Measures should be in place to protect data from unauthorized access, including encryption and secure storage. ○ Cybersecurity: Systems should be secure against hacking or unauthorized control, as vulnerabilities could lead to safety risks. ■ Liability and Insurance: ○ Operators and manufacturers may be required to have liability insurance to cover potential damages or accidents caused by the use of low altitude sensing systems. ■ Training and Certification: ○ Operators and pilots may need to undergo training and certification to demonstrate competence in operating low altitude systems safely and responsibly.
Involved partners	SKYLD / other consortium partners
IPR protection	Innovation is integrated in a closed SW and has to be protected by copyright. Patent and brand will be foreseen in near future.

4.2.3 earthLive Simulation Platform

KER 2.3: earthLive Simulation Platform	
Description	With earthLIVE, TASF is exploring a paradigm shift in Earth Observation, with combined persistent detectability and tracking capabilities based on an optical telescope payload hosted on a telecom satellite in geosynchronous orbit. In the frame of EURMARS, will be developed a component, core of the ground segment, to demonstrate the capability thanks to the AI algorithms, to detect and track vessels for maritime and coastal surveillance missions as part of the global EURMARS system. The earthLIVE component will be fed by the Nemo-HD LEO Satellite (From SPACE-SI) with short videos reflecting “permanent” monitoring (video during proximate 2 minutes). The earthLIVE will then process videos to simulate a geostationary satellite image, and provides primary vessels plots (with direction and speed). This output will feed the fusion component from

	the EURMARS platform contributing to the global situation awareness for end-users.
What problem(s) are solved	The core operational problem is to have the capability to monitor permanently an area of interest.
Innovativeness / new approach	The innovative approach is to install an optical sensor on a geostationary satellite to have continuous images, coupled with AI algorithm detecting and tracking vessels.
Unique selling point	The key point is to have a permanent monitoring that is not possible with LEO satellites.
Competitors (solutions)	Current solutions consist in a multitude of LEO satellites with revisit from 6 days up to 1 hour in best cases.
Target users / customers	Target customers are multiple, National and EU level for public administrations/agencies; national defence, and *export customers* requiring civil security and defence solution.
Benefits for users / customers	The main benefit is to have a "continuous" area monitoring, that could be up to 10s for example for an 200km x 200km size.
TRL level (1-9)	4
Main technical challenge(s)	The main challenge for the ground segment is to be able to detect and track vessels with low resolution images (between 15 and 40m) and with a low latency.
Legal / ethical requirements	Cannot be estimated at current stage
Involved partners	SPACE-SI will provide videos as inputs (for the detection and tracking solution).
IPR protection	IPR on Detection and Tracking solution will be owned by TAS-F.

4.2.4 High Altitude Sensing Systems

KER 2.4: High Altitude Sensing Systems	
Description	Simulation of a 3D-LiDAR payload for a High-Altitude Platform (Stratobus) to provide enhanced surveillance capabilities.
What problem(s) are solved	Provides wide area maritime surveillance not possible with existing lower altitude aerial platforms. Long endurance and persistence over target areas.

Innovativeness / new approach	Integration of a novel high-altitude platform (Stratobus) with advanced 3D-LiDAR not previously used for maritime surveillance.
Unique selling point	Stratobus operates at altitudes up to 20km with the ability to stay on station for over a year, providing continuous monitoring over wide areas. The 3D-LiDAR provides detailed imaging and object identification.
Competitors (solutions)	Lower altitude aerial surveillance platforms like fixed wing aircraft and drones which have limited endurance and coastal based sensors.
Target users / customers	Maritime authorities and border agencies needing enhanced maritime domain awareness over wide areas.
Benefits for users / customers	24/7 monitoring capability over wide maritime areas enabling improved detection, tracking and identification of vessels not possible with existing systems.
TRL level (1-9)	4
Main technical challenge(s)	Integrating and optimizing the 3D-LiDAR on the Stratobus platform. Processing and exploiting the volumetric LiDAR data for surveillance.
Legal / ethical requirements	Ensuring lawful, ethical and privacy compliant use.
Involved partners	ONERA, TASF, AIT, UREAD, GSH
IPR protection	Technical aspects of the integrated Stratobus/LiDAR surveillance solution could be protected by patents or copyright if deemed necessary.

4.2.5 Satellite Based Systems

KER 2.5: Satellite based systems	
Description	The system utilizes multiple satellite-based infrastructures to provide remote sensing solutions, leveraging a combination of freely available and commercial satellite data. Its primary purpose is to effectively monitor various marine tasks, including ship detection, environmental indices and phenomena such as oil spills and infrastructure resilience monitoring. It employs cutting-edge software for data acquisition, preparation and pre-processing. The data processing incorporates state-of-the-art AI and ML techniques to efficiently, reliably, and rapidly detect events.

What problem(s) are solved	1) The system will monitor marine tasks and actions, with particular emphasis on detecting vessels and dark vessels. The latter can help identify illegal fishing, irregular migration, human trafficking, smuggling, drug and arms trafficking, thereby preventing economic losses resulting from illegal commerce and enhancing security throughout Europe. 2) Monitor environmental indicators and subsequently propose immediate actions and advisory guidelines to enhance security and safety. Specifically, satellite data will be utilized to detect oil spills caused by either platforms or ships. 3) The system works in conjunction with other sensors and technologies to achieve the optimal solution for continuous monitoring of vessels and to record any suspicious actions and changes in their courses. Moreover, satellite imagery containing oil spills can serve as the main input for other systems used to predict the movement of oil spills.
Innovativeness / new approach	• The system will be built in open-source software (code, libraries, etc.), which provides the following advantages not only for the system itself but also for the complete platform: i. Transparency: Open-source software provides access to its source code, allowing users to inspect, modify, and enhance it. ii. Longevity: Open-source projects tend to have a longer lifespan compared to proprietary software. iii. Compatibility and interoperability: Open-source solutions can be more easily migrated to different systems and are much more compatible in complex architectures, compared to proprietary software. iv. Security and debugging: With open-source software, security vulnerabilities can be identified and addressed more quickly. A large number of developers scrutinizing the code can discover and fix issues promptly, ensuring enhanced security and reducing the risk of malicious exploits. • Utilize multiple satellites, including both data available in open hubs and commercial satellite data. Additionally, the data sets will vary in terms of their nature (optical and SAR data), spatial analysis and temporal analysis.
Unique selling point	• Offers a significantly advanced solution compared to traditional means, which primarily relied on operational methods. This

	innovative system will streamline bureaucracy and provide cost efficiency. • Various data, differing in nature, spatial resolution, and temporal analysis, will be harmonized to provide a comprehensive solution to the end-users. • Offered as "dockerized" product, it can be incorporated optimally in the whole platform, but also be migrated to other systems if needed.
Competitors (solutions)	Capella Space, ImageSat International (ISI), Earth-i, Orbital Insight
Target users / customers	Coast Guards, relevant Ministries, shipping companies, No-Govermental Organizations
Benefits for users / customers	Users/customers will benefit from a comprehensive surveillance platform equipped with state-of-the-art solutions and capabilities. Specifically, • All data will be in digital form, reducing bureaucracy and costs. • Data, results, detection events, and other materials will be stored in a common data storage, allowing users to access historical data and track the evolution of events. • The integration of various sensors and technologies enhances efficiency, reliability, and precision.
TRL level (1-9)	7
Main technical challenge(s)	• Adapt the algorithms to handle data of varying nature, including optical and SAR data, as well as different spatial resolution requirements. Harmonize all diverse data sources to generate and present comprehensible output in every case. • Improve temporal resolution based on the available satellite observation at each time, trying to achieve optimal coverage above the AOIs. • Improve the performance of the algorithms by measuring appropriate metrics such as mean Average Precision (mAP), Localization Loss, F1 curve, etc. • Reduce pipeline time from the time that data are acquired until the detection event.
Legal / ethical requirements	NA

Involved partners	GSH
IPR protection	The software design for the detection of vessels and oil spills using satellite data has to be protected by copyright.

4.2.6 Common Data Hub

KER 2.6: Common Data Hub	
Description	A software component that is responsible for retrieving information from external data sources. Data from these sources includes information about the weather and vessel tracking information. It consists of two major components, one offline and one online component. The online component is responsible for serving the information from the external data sources in near real-time or as soon as they arrive, while the offline component is responsible for storing the information and serving it when asked from the other EURMARS components. Hence, the offline component serves historic data.
What problem(s) are solved	Lack of a common data hub for retrieving information. Each EURMARS component will have a single point of retrieving the data from the external sources taking the burden of each partner or EURMARS component of developing software for retrieving the data.
Innovativeness / new approach	■ Real-Time Access: The platform can provide data in near real-time, which is essential for applications requiring timely data, such as weather forecasting and vessel tracking. ■ Integration with External Data Sources: The ability to integrate and retrieve data from various external data sources increases the richness and diversity of the data available through the platform. ■ API Access: Offering API access to the data hub could facilitate integration with other systems and promote broader use of the data available through the platform.
Unique selling point	EURMARS components will have the ability to retrieve information from a common data hub rather than developing software tools for retrieving data

	from different APIs. One API can serve the data needs of all EURMARS components.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	Developers of EURMARS components
Benefits for users / customers	One API for all external data sources
TRL level (1-9)	7
Main technical challenge(s)	The integration of multiple different APIS into a unified seamless API.
Legal / ethical requirements	No legal / ethical requirements have been identified for this component
Involved partners	HSE, ED, AIT, THAL, CDBP, GDBP, JRCC, GMD, GIRBP, UKH
IPR protection	Cannot be estimated at current stage

4.2.7 Multimodal Data Fusion Platform

KER 2.7: Multimodal Data Fusion Platform	
Description	The EURMARS Multimodal Data Fusion Platform is an advanced system which takes advantage of the SoTA ML and AI tools to harness multimodal data, transforming it into actionable intelligence. It enhances the capabilities of detecting, classifying, and tracking small vessels at sea/shoreline and persons/vehicles in inland areas from aerial platforms. Data fusion happens at two distinct levels: sensor-level fusion and higher-level fusion that incorporates external IT services.
What problem(s) are solved	■ Integration of diverse data sources and modalities. ■ Scattered and uncorrelated data.

Innovativeness / new approach	■ Cutting-edge AI and ML techniques for data fusion. ■ Two-tier fusion processes that enhance data correlation both at the micro (sensor) and macro (external IT services) levels.
Unique selling point	The platform's ability to iteratively update fused estimates with confidence measures, allowing for continuous improvement and refinement.
Competitors (solutions)	■ Traditional centralized fusion systems. ■ Platforms based on singular data modalities. **Solution:** Results and methodologies found in the FOLDOUT project.
Target users / customers	■ Surveillance and security agencies. ■ Defence forces. Coastal and border security authorities.
Benefits for users / customers	■ Consolidated and correlated intelligence from diverse data sources. Real-time actionable insights.
TRL level (1-9)	7
Main technical challenge(s)	■ Ensuring real-time processing and fusion with no significant lag. ■ Achieving high levels of accuracy in detection and classification. ■ Integrating vast amounts of data from disparate sources.
Legal / ethical requirements	■ Data protection and privacy laws related to processing individual(s) or vehicle tracking. ■ Obtaining licenses and permissions for 3rd party software. ■ Periodic ethical reviews to ensure the platform remains ethically sound after updates and data source changes. Measures for: data and platform misuse, data breaches, unauthorized personnel access, data processing with malicious intent.
Involved partners	UREAD and all that can provide useful sensory and data input.

IPR protection	Cannot be estimated at current stage

4.2.8 Registration, Communication & Coordination of Subsystems

KER 2.8: Registration, Communication & Coordination of Subsystems	
Description	The Registration, Communication & Coordination of Subsystems will enable the integration of diverse sensing systems like coastal sensors, UAVs, satellites, and simulation systems into the EURMARS platform. It will provide: ■ A registry containing technical specs, interfaces, data formats etc. for all connected subsystems. This will aid discovery and usage. ■ Standardized interfaces and adapters to handle interoperability between subsystems using different protocols. ■ A communication framework with robust connectivity including security features tailored to EURMARS. ■ Tools to simplify registration, configuration, testing and monitoring of subsystem integration. ■ Future-proofing via loose coupling and ability to expand registry for new subsystems. By handling the complexity of integrating many heterogeneous systems, the framework will allow developers to seamlessly leverage the array of sensors and data sources in the EURMARS platform.
What problem(s) are solved	■ Manual integration of new sensors and data sources into the platform is cumbersome and time-consuming due to diversity of formats, interfaces, etc. The framework simplifies this via standardized adapters. ■ Lack of central registry containing technical specs and metadata for available subsystems makes discovery and usage difficult. The registry addresses this.

	■ Proprietary interfaces of subsystems restrict interoperability and modular growth. Open standardized interfaces promoted by the framework improve flexibility. ■ Limited monitoring and diagnostic capability regarding connected subsystems. The framework provides better testing and debuggability. ■ Brittle integration pathways between subsystems prone to breakages and latency. The framework delivers robust connectivity and performance. ■ Constraints in leveraging legacy subsystem investments. Loose coupling approach provides adaptability to utilize existing systems. ■ Difficulty supporting emerging technologies, data sources, and user needs. The framework's expandable approach future-proofs integration capability.
Innovativeness / new approach	■ It goes beyond a static registry to provide active adapters that can handle interoperability between diverse subsystems and external systems like CISE. ■ The framework is customized to the specific needs of EURMARS in terms of sensors, data formats, interfaces etc. rather than a generic solution. ■ It incorporates robust connectivity features like dynamic configuration, redundancy, and security tailored to EURMARS operational requirements especially for aerial assets. ■ The modular loose coupling design allows flexible expansion as new subsystems and data sources emerge without having to re-engineer core integration pathways. ■ Advanced monitoring, debugging and simulation capabilities are incorporated to simplify testing and reduce integration risk of upgrades. ■ It is designed to promote open standards and interfaces to avoid vendor lock-in and leverage community innovation in areas like maritime data sharing.

	■ By handling complexity of integration, it allows developers to focus on core surveillance analytics rather than interoperability problems. ■ Tools for automated registration and configuration minimize overhead of adding new subsystems.
Unique selling point	■ Greatly reduced integration effort and time to add new sensors and data sources to the surveillance platform. ■ Loose coupling and open standards enable flexibility to leverage legacy systems and future technologies. ■ Robust connectivity features specially designed for reliability in maritime operations. ■ Improved scalability to handle growth in sensors, data volumes, and users as operations expand. ■ Better coordinated management of connected subsystems via centralized monitoring and control. ■ Cost-effectiveness from reuse of proven building blocks enhanced for EURMARS. ■ Opens up innovation ecosystem by avoiding vendor lock-in.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	Border and coast guard authorities responsible for maritime and land surveillance
Benefits for users / customers	■ Discovers and leverages sensors/data relevant to surveillance needs. ■ Visualizes relationships between integrated subsystems. ■ Centralized monitoring and control. ■ Near real-time exchange of threat data between linked authorities. ■ Scalability to support operations growth and evolution.
TRL level (1-9)	7

Main technical challenge(s)	■ Handling the diversity of data formats, interfaces, protocols, and technologies across the various subsystems and external systems that need integration. ■ Achieving robust and responsive interconnectivity between subsystems especially for aerial assets like UAVs and satellites with constrained communication. ■ Providing security features like access control, encryption, and cyber threat monitoring tailored to EURMARS operational needs across multiple agencies. ■ Enabling scalability of the framework to support growth in sensors, users, data volumes etc. as operations expand over time after initial capability deployment. ■ Simplifying registration and configuration processes given multitude of parameters across heterogeneous subsystems. High degree of automation needed. ■ Delivering requisite performance especially for real-time tracking and anomaly detection analytics operating on integrated data. ■ Developing adapters for legacy subsystems and future technologies in a rapid, low-effort manner. ■ Handling semantics of multimodal data fusion and analytics output so integrated subsystems have common operational picture. ■ Planning complex field trials and testing scenarios to validate the integrated platform comprising many subsystems.
Legal / ethical requirements	■ Compliance with data protection regulations like GDPR when handling any personal data as part of subsystem integration. ■ Implementation of access controls and cybersecurity measures to prevent unauthorized access to sensitive surveillance data. ■ Following technical standards for subsystem communication protocols, maritime data exchange, interfaces etc.

	■ Building capabilities like metadata tagging to allow appropriate data handling restrictions to be enforced. ■ Adapting as regulations around maritime/aerial surveillance systems and data sharing evolve.
Involved partners	All Partners
IPR protection	Cannot be estimated at current stage

4.2.9 Collaborative C2, Visualization & Alarming

KER 2.9: Collaborative C2, Visualization & Alarming	
Description	A software platform that enables a common operational picture and real-time collaboration between multiple authorities responsible for border surveillance. It consists of a GIS-based web interface that can be accessed remotely from anywhere through a standard web browser. This allows relevant authorities to log in and view a unified visualization of the deployment area, including layers of information such as vessel locations, tracks, anomalies, risks, and alarms. The software integrates services and applications for processing and visualizing content in a customized way based on user rights and needs. The platform architecture is designed to integrate the outputs of EURMARS analytics modules like anomaly detection and risk assessment into the decision support views. This enables an enhanced common operational picture.
What problem(s) are solved	■ Lack of a common operational picture. Existing maritime surveillance systems used by different authorities often cannot interoperate or share information seamlessly. This leads to fragmentation, lack of coordination, and inability to see the full picture. The C2 platform provides a unified visualization bridging systems. ■ Situational awareness. Without a shared view of the situation, anomalies or emerging threats may be missed as information resides in silos. The C2 platform enhances awareness by integrating analytics outputs.

	■ Cooperation difficulties. Authorities face difficulties cooperating in real-time when using disjoint systems and data formats. The virtual workspace features of the C2 platform enables real-time collaboration. ■ Inflexible platforms. Current platforms can be rigid and not customizable to user needs. The C2 platform allows configuring information layers and views based on user rights and operational needs.
Innovativeness / new approach	■ Integration of AI analytics. A key innovation is the integration of outputs from EURMARS AI-based analytics like anomaly detection and risk assessment into the decision support views of the C2 platform. This provides an enhanced common operational picture. ■ Unified architecture. The platform unifies disparate systems used by different authorities into a common architecture for information sharing and situational awareness. ■ Adaptive information layers. The ability to configure information layers and system views based on user rights and specific operational needs provides flexibility not present in existing rigid systems.
Unique selling point	■ Faster response. By improving situational awareness and collaboration, the C2 platform enables authorities to respond more quickly to emerging border incidents. ■ Cost-efficient. The C2 platform reduces costs compared to authorities having to develop customized standalone systems. It provides a shared architecture and tools. ■ Interoperability. The platform enables interoperability between diverse systems and data sources not achievable today. ■ Versatility. The highly configurable architecture can be readily adapted to different multi-authority use cases and operational needs. ■ User-centric. Features like mobile access, virtual workspace, and adaptive views make the platform tailored to end user and mission needs.

	■ Enhanced detection. Integration of AI analytics enhances the detection and response capabilities compared to traditional approaches. ■ Compliance. The design ensures regulatory compliance for aspects like data protection and privacy.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	Border and coast guard authorities responsible for maritime and land surveillance
Benefits for users / customers	■ Improved situational awareness - Integrated view of events and threats enables better assessment. ■ Enhanced detection - Incorporation of AI analytics improves detection of anomalies and small vessels. ■ Real-time collaboration - Virtual workspaces allow seamless cooperation between authorities. ■ Efficient information sharing - Common architecture enables sharing relevant data timely. ■ Quicker response - Shared situational awareness and collaboration enables faster reaction. ■ Interoperability - Platform bridges diverse systems and data formats used by authorities. ■ Versatility - Configurable platform can address a wide range of multi-authority use cases. ■ User-centric access - Features like mobile access improve utility for end users in the field. ■ Cost-efficiency - Shared C2 architecture reduces costs vs. separate systems. ■ Future-proofing - Open architecture can integrate future technologies and systems.
TRL level (1-9)	7

Main technical challenge(s)	■ Integrating diverse systems and data formats into a unified architecture. A key challenge is enabling interoperability between the disparate systems and data. Required development of adapters, APIs and middleware. ■ Scalability. The platform needs to scale to handle large volumes of real-time data from multiple sensors and systems across a wide area. ■ Heterogeneous data fusion - Fusing real-time and archival structured and unstructured data from diverse sources into an integrated operational picture posed data engineering challenges. ■ Customizability - Allowing dynamic configuration of information views based on user needs and contexts involved complex authentication, authorization and filtering techniques. ■ Cybersecurity - Addressing cybersecurity vulnerabilities and threats across interconnected systems and new attack surfaces required rigorous security software engineering. ■ User acceptance - Getting adoption and buy-in from end users accustomed to legacy interfaces required incorporating human-centred design principles.
Legal / ethical requirements	■ Data protection laws. Compliance with regulations like GDPR on protecting personal data privacy and security. ■ Authorization. Legal clearance for sharing of information between government authorities. ■ Licensing. Usage restrictions for proprietary systems and data sources integrated into the platform. ■ Transparency. Ethics requirements for explainability and transparency of AI systems used for decision support. ■ Oversight. Ethical obligation for human oversight and control over autonomous analytics-based systems. ■ Non-discrimination. Avoidance of bias, stereotyping and exclusion.

	■ Security. Legal duties to secure systems and data shared between authorities. ■ Accountability. Record-keeping and audit trails for compliance demonstration and incident investigation.
Involved partners	All Partners
IPR protection	Cannot be estimated at current stage

4.2.10 Data-Driven Risk Assessment Tool

KER 2.10: Data-Driven Risk Assessment Tool	
Description	A tool that focuses on potential threat analysis by situation evaluation outputting possible future states. It works in tandem with end-users (authorities) to rank threats based on current state and probability estimations. Leveraging FRONTEX's CIRAM, it ensures uniformity in risk assessment.
What problem(s) are solved	■ Analysing and ranking real-time cross-border threats. ■ Streamlining collaboration between multiple authorities. ■ Identifying threats with significant humanitarian impacts. Guiding operators on the subsequent action steps based on analysed risks.
Innovativeness / new approach	■ Incorporation of FRONTEX's CIRAM for standardized risk assessment. ■ Proactive risk evaluation considering potential future state evolutions. Data-driven approach replacing traditional subjective analysis.
Unique selling point	Ability to integrate real-time data fusion with standardized risk analysis models, keeping the human in the loop, allowing for immediate and forward-looking surveillance and risk evaluation.
Competitors (solutions)	Risk assessment tools that may not adapt in evolving cross-border threats.
Target users / customers	■ Authorities

	■ Defence agencies ■ Border protection units ■ Humanitarian organizations
Benefits for users / customers	■ Enhanced situational awareness. ■ Streamlined decision-making processes. ■ Better inter-agency collaboration by applying standardized assessment models.
TRL level (1-9)	4
Main technical challenge(s)	■ Integration of data sources. ■ Adapting to rapidly escalating threat scenarios (distinguishing between false positives and real suspects/events). ■ Ensuring compatibility with various legacy systems.
Legal / ethical requirements	■ Protecting sensitive data related to threat assessments. ■ Discouraging discrimination or inadvertently highlighting bias. ■ Complying with international regulations.
Involved partners	UREAD and end-users (authorities)
IPR protection	Cannot be estimated at current stage

4.2.11 Decision Support System

KER 2.11: Decision Support System	
Description	A software platform that aids relevant authorities in their decision-making during incidents or threats. The Decision Support System (DSS) platform consists of two major components. The first one is responsible for consuming vessel tracking data from the Automatic Identification System (AIS) that are considered low level events and generating high level events. Examples of

	these high-level events include detections of vessels not transmitting their position or vessels that entered an area of interest for the authorities. The second component is responsible for recommending to the relevant authorities' possible courses of actions when a threat or an incident is detected.
What problem(s) are solved	Taking the right course of action at the time an incident takes place, can be overwhelming for the responsible user employed by the relevant authority. The DSS can aid the users in taking better decisions and faster.
Innovativeness / new approach	The use of AI analytics in the decision-making process. A key innovation is the use of a smarter mechanism for recommending actions or operational steps to the authorities.
Unique selling point	The DSS will receive feedback from the end users in order to learn and improve its recommendations.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	The relevant maritime authorities.
Benefits for users / customers	Improved decision-making.
TRL level (1-9)	7
Main technical challenge(s)	The user's acceptance is the major technical challenge. While the DSS can recommend actions per incident, the end-user is responsible for implementing them and providing feedback.
Legal / ethical requirements	No legal requirements have been identified
Involved partners	HSE, ED, GSH, BDI
IPR protection	Cannot be estimated at current stage

4.3 Secure interoperable architecture

KER 3: Secure interoperable architecture

Description	This is an open, standards-based system architecture that enables the integration of diverse surveillance platforms, sensors, databases and legacy systems into a common interoperable framework. The architecture adopts a modular plug-and-play approach allowing different components and systems to connect seamlessly through well-defined interfaces. This facilitates the rapid integration of new sensors, analytics modules, visualization platforms etc. to extend system capabilities.
What problem(s) are solved	■ Integration difficulties. The architecture addresses the problem of integrating diverse sensors, platforms, databases and systems used by different authorities into a unified architecture. This enables interoperability. ■ Vendor lock-in. Proprietary non-interoperable architectures result in vendor lock-in. The standards-based open architecture approach of EURMARS avoids this. ■ Scaling constraints. Legacy architectures often cannot handle the scale of data and users needed for wide area border surveillance. The distributed scalable architecture of EURMARS overcomes these limits. ■ Inflexibility to new technology. Rigid legacy architectures cannot readily adopt new innovations like AI analytics, sensors etc. The modular design of EURMARS allows integrating this flexibly.
Innovativeness / new approach	■ Modular plug-and-play design. This allows flexible integration of diverse new systems and evolution of capabilities. ■ Open standards base. Basing the architecture on open standards avoids vendor lock-in and aids adoption. ■ Compliance-by-design. Mapping regulatory compliance requirements like privacy into architectural safeguards.
Unique selling point	■ Future-proofing. The modular design protects user investments in new technology and avoids vendor lock-in. ■ Faster integration. Plug-and-play approach enables rapid integration of new platforms and upgrades.

	■ Enhanced security. Comprehensive cybersecurity coverage beyond piecemeal legacy protections. ■ Operational agility. Standards-based architecture allows dynamically assembling solutions for diverse missions. ■ Compliance assurance. Architecture designed to address regulatory compliance requirements proactively. ■ Total cost savings. Shared interoperable architecture reduces costs compared to fragmented systems.
Competitors (solutions)	Cannot be estimated at current stage
Target users / customers	Border and coast guard authorities responsible for maritime and land surveillance
Benefits for users / customers	■ Interoperability. Integrates diverse systems into a unified architecture to improve information sharing. ■ Enhanced security. Comprehensive cybersecurity protections reduce vulnerabilities. ■ Operational agility. Standards-based architecture allows dynamic mission reconfiguration. ■ Faster upgrade cycle. Plug-and-play approach enables rapid integration of new technologies. ■ Compliance assurance. Architecture designed to facilitate regulatory compliance. ■ Cost savings. Shared architecture drives efficiencies compared to separate systems. ■ Vendor flexibility. Avoidance of vendor lock-in provides freedom to adopt new innovations. ■ Future-proof investment - Modular design protects sunk costs in new capabilities.
TRL level (1-9)	7

Main technical challenge(s)	Heterogeneous systems integration. Developing adapters and common interfaces to bridge diverse systems and data formats used by authorities. Cybersecurity. Engineering comprehensive security spanning applications, networks, systems and physical infrastructure. Access control. Fine-grained mechanisms to enable lawful, need-to-know data sharing between agencies. Legacy compatibility. Integrating legacy systems and data which were not built on open standards. Sensor discovery. Mechanisms for automated discovery and integration of sensors into the architecture. Compliance assurance. Embedding mechanisms throughout the architecture to facilitate regulatory compliance.
Legal / ethical requirements	Cannot be estimated at current stage
Involved partners	All Partners
IPR protection	Cannot be estimated at current stage

4.4 Stakeholder requirements supporting use case and technical development, validation and user acceptance

KER 4: Stakeholder requirements supporting use case and technical development, validation and user acceptance	
Description	This is the main description for considering and implementing identified and specified stakeholder requirements in EURMARS platform and technology development. The requirements help EURMARS technology developers to comprehensively understand the expectations and capabilities of border authorities and other relevant stakeholders in using future border security technologies in their respective operational environments. Stakeholder requirements support the validation of the project's outcomes, enacted through various use cases, also ensuring high user acceptance for and overall relevance of the development efforts performed in the project.

What problem(s) are solved	To ensure that developed system features match genuine user needs, specified as functional and non-functional system requirements
Innovativeness / new approach	The requirements were collected, analysed, specified, and categorised through an iterative, co-creative process engaging end-users in various ways to EURMARS research work. The process included for example data collection, iteration and validation through survey and several virtual and physical workshops.
Unique selling point	Extensive requirements knowledge in border security domain from several MSs and third countries
Competitors (solutions)	Other EU projects, Research institutes and commercial actors in the security domain
Target users / customers	EU border security organisations, security research units, Commercial actors providing border security solutions
Benefits for users / customers	User validated systems meet best genuine user needs
TRL level (1-9)	Not applicable
Main technical challenge(s)	Not applicable
Legal / ethical requirements	The requirements include also legal and ethical issues.
Involved partners	All partners
IPR protection	Not applicable

4.5 EURMARS platform blueprint operationally validated in real life scenarios and three Pilot Use Cases

KER 5: EURMARS platform blueprint operationally validated in real life scenarios and three Pilot Use Cases	
Description	The real-world effectiveness of the project will be estimated using three Pilot Cases which will encompass diversified situations in the maritime and

	geographical domains. UAT will check the system's robustness and adaptability using at least five critical user groups from the boarder and coast guard community.
What problem(s) are solved	The platform can address the escalating complexity of various maritime security incidents ranging from irregular migration flows, human and/or drugs and/or arms trafficking, and smuggling to illegal fishing. Tackling such issues can be achieved with the facilitation of an integrated surveillance approach which merges UxVs, ground-based sensors, satellite imagery and high-altitude platforms to extend situational awareness.
Innovativeness / new approach	The operational validation of converging multi-authority collaboration that is enhancing (through data-fusion) the joint surveillance capability of the system.
Unique selling point	Fostering closer collaboration between national, regional, and EU-level authorities, ensuring that all diversified stakeholders (whether military, surveillance, or civilian security forces) receive near real-time, high-quality data and thus support a more streamlined and effective response to diverse security risks.
Competitors (solutions)	■ Established systems that rely on isolated (standalone), singular technology platforms Systems leveraging matured C5ISTAR systems (without the added advantage of a comprehensive, integrated surveillance approach)
Target users / customers	The operational validation of the platform blueprint will eventually benefit ■ Industrial partners, ■ service providers, ■ SMEs, ■ LEAs, ■ PIUs, ■ Ministries and, ■ Leading research and technological development institutions.

Benefits for users / customers	This unified surveillance mechanism can act as a game-changer, especially in high-stakes zones where multi-authority cooperation is pivotal for maintaining security and mitigating threats.
TRL level (1-9)	7
Main technical challenge(s)	Difficulty to replicate during the demos: ■ Integration complexity (single coherent platform aspiring towards seamless communication over diverse, and independent in most cases, systems) ■ Operational Resilience in adverse conditions (storms, high-sea states) ■ Cybersecurity Risks (checking cyber-secure protocols) ■ Data Overload (number of data types, data rates, and volume of data)
Legal / ethical requirements	The Legal, Ethical, Societal (LES) impact work performed within EURMARS ensures adequate consideration of the risks that data analytics could pose to key societal and ethical values, privacy, data protection, societal wellbeing and fundamental rights, including the freedom of movement in particular.
Involved partners	All partners
IPR protection	Cannot be estimated at current stage

4.6 Benchmark dataset

KER 6: Benchmark dataset	
Description	The EURMARS benchmark dataset is expected to provide the necessary data on vessel tracking, behaviour analysis and anomaly detection, linked to the use cases, which will be used for performance assessment. These will be made publicly available, contributing to international benchmarking / standardization advancement in maritime surveillance.
What problem(s) are solved	■ **Inconsistent data standards**: In surveillance operations that involve various agencies and multiple technologies, there is high chance that there will be lack of uniformity in data standards. This is where a

	benchmark dataset can establish a consistent and standardized set of data parameters that enhances coherency and interpretation universality. ■ **Training and testing discrepancies**: Training and testing new data-driven surveillance tools requires a standardized and well-defined dataset to ensure repeatability and predictability of results. A standardized dataset can provide a reliable foundation for algorithm development and validation. ■ **Inter-agency collaboration**: the disconnection between agencies in the defence sector or the absence of a shared data framework. The benchmark dataset can stand as an attempt towards a unified data reference. ■ **Quantitative assessment of proposed solution**: the efficacy assessment could be subjective without a standard comparison point. The benchmark dataset can provide a reference of objective evaluation. **Data gaps and redundancies**: In many cases sensory data may be overlapping or missing values or translate into weak information load. The establishment of a benchmark can identify and also rectify gaps and redundancies, leading to a comprehensive and sufficient coverage.
Innovativeness / new approach	■ **Unified multidisciplinary framework**: The approach of structuring data (for maritime, land and aerial surveillance) is rare in conventional datasets and their fusion can provide useful emerging properties in situational awareness. ■ **AI-optimized recognition**: Real-time threat detection with a human in the loop for supervised learning can lead to rapid and efficient algorithm training and enhance predictive analysis. ■ **Contextual metadata integration**: the benchmark dataset might incorporate rich metadata which introduce semantical and contextual meaning to the data structure, facilitating situational understanding (thus series or combination of events can lead to stories and then to tactics and emerging agendas). ■ **Accumulating data assimilation**: on top of the other two points, the benchmark can assess the extent of relevance and richness of the data

	and to provide a sensitivity analysis in respect to its accumulated information content. ■ **Inter-agency collaboration**: A novel aspect on the tactical defence preparation is bridging information silos and benchmarking the results of the multi-parameter data fusion. Feedback Loop Integration**:** On a similar note, to the ones discussed previously, an advanced aspect of the proposed system is the ability of developing constant dataset refinements during the incorporation and highlighting of the most dominant or frequent events (and their conditional aspects per case), providing useful feedback for future-ready provision without major overhauls.
Unique selling point	The unique selling point relates to EURMARS capacity to integrate rich contextual metadata that enable agencies to derive semantical and strategic insights. This effect is further enhanced when the derived intelligence is combined with the inclusion of dataset benchmarking.
Competitors (solutions)	The large-scale surveillance and reconnaissance competitors are not expected to disclose benchmark datasets, algorithms or tactics of use, due to security, proprietary and competition issues involved. However, EURMARS has a diversified generalized scope from most of the strong competitors of the markets. C5ISTAR Systems: EURMARS differentiates by a multidisciplinary dataset, AI optimized, enabling faster and real-time threat detection. **LANDGUARD Integrated Surveillance Systems, Global Maritime Surveillance Systems,** AeroWatch Surveillance Systems: EURMARS uses a holistic approach, integrating aerial, maritime and land surveillance data.
Target users / customers	As EURMARS ushers in a new era, the benchmark datasets are transformed into invaluable marketable tools of great importance for various target users / customers. ■ **Military and Defence Agencies:** they require sophisticated datasets to train their surveillance and monitoring systems to ensure readiness and effective response. ■ **Civilian Security Forces:** benchmark datasets can elevate the efficacy of their monitoring tools, enhancing the safety of national territories.

	■ **Surveillance System Manufacturers:** Companies developing surveillance technologies, especially those reliant on AI and ML, can benefit from a standardized dataset for testing and refinement. ■ **Research and Development Institutions:** new detection algorithms can use the benchmark datasets as a tool for research and progress evaluation results. ■ **Multi-agency Taskforces:** Collaborative groups, especially those working across both military and civil domains, can utilize the dataset to harmonize their operations, to benchmark interoperability and to gain a shared understanding of causes (threats) and responses. **Private Security Companies:** Firms offering monitoring and surveillance for critical infrastructures like ports, airports, and strategic facilities can leverage the dataset to improve their product / service offerings.
Benefits for users / customers	■ **Standardization:** Users can rely on a unified data standard. ■ **Improved Situational Awareness:** The benchmark dataset offers data-driven insights, allowing for quicker decision-making and proactive responses based on real-time analysis. ■ **Efficient Resource Allocation:** For both civilian security forces and the army, the dataset provides clarity on areas of concentration, ensuring optimal distribution of assets and personnel. ■ **Enhanced Training Modules:** As mentioned on the previous table cell, with a standardized dataset, training programs can be more structured, leading to better-prepared algorithms and personnel in both conventional and asymmetric warfare scenarios. ■ **Reliable Decision-making Framework:** The benchmark dataset, through its consistency, suggests the management of reliable data sources and thus provides a dependable foundation for strategic and tactical decisions.
TRL level (1-9)	7
Main technical challenge(s)	■ **Interoperability with Legacy Systems:** Military and security forces often operate with legacy systems. Ensuring the benchmark dataset is

	compatible and can communicate effectively with these older systems can be technically challenging. ■ **Data Integration (data fusion):** Guaranteeing the integration of heterogeneous data types and sources can be quite challenging. ■ **Data Security & Integrity:** Requires the implementation of robust security protocols. ■ **Scalability and Relevance Concerns:** Data evolve and their volumes grow, as do the scenarios that need to be identified as threats, so the benchmark dataset system needs to ensure that it can handle these issues without compromising efficiency and performance. ■ **Real-time Processing:** Speed of processing and analysing data in such sets is crucial. **Data Normalization & Standardization:** As already discussed, ensuring that data from varied sources adheres to a common standard is crucial, yet challenging due to the diversified operational methodologies of the various agencies involved.
Legal / ethical requirements	■ **Data Privacy & Protection:** Adhering to data protection laws, such as GDPR, AI Foresight Report and Blueprint, PIA, EIA and SIA assessment. Personal data, if any, should be anonymized and encrypted. ■ **Intellectual Property Rights:** Respect to copyrights, patents, and licenses. Credits to be attributed where necessary. ■ **International Data Sharing:** Compliance with international data sharing agreements, concerning sensitive defence-related data. ■ **Data Retention Policies:** Relevant for surveillance and defence. ■ **Transparency & Consent:** Transparency in data collection methods and obtaining necessary consents can be paramount. ■ **Bias & Discrimination:** To ensure dataset does not introduce or perpetuate any (positive or negative) bias. ■ **Use Limitations:** Clear and concise attribution of credentials and user rights/restrictions and for what purposes. Clear guidelines and protocols applied according to justified quality assurance processes.

	■ **Feedback & Redress Mechanisms:** If a misinterpretation or misuse of the dataset is identified, it needs to be a clear mechanism for the affected parties to provide feedback or seek redress.
Involved partners	UREAD and all partners that contribute sensory or data input.
IPR protection	Cannot be estimated at current stage

4.7 AI Foresight Report and Blueprint, PIA, EIA and SIA assessment

KER 7: AI Foresight Report and Blueprint, PIA, EIA and SIA assessment	
Description	The purpose is to ensure that EURMARS is compliant with EU legislation and requirements for border management projects, and develop a blueprint for a responsible research and innovation approach (RRI) of other border management surveillance projects. As part of this task, we will conduct foresight compliance work anticipating the entry into force of the proposed AI Act, as well as monitoring and assessing the impact of the EURMARS platform on privacy, security, and the environment. Partners will be continually informed of their corresponding obligations along the complete supply chain from design through manufacturing to deployment.
What problem(s) are solved	As border security and management projects are classified as “high risk” by the AI Act due to their potential impact on safety and human rights as a whole, this task aims to ensure that the EURMARS platform can be taken up and deployed upon the project’s termination.
Innovativeness / new approach	A pivotal component of this foresight assessment is employing a socio-technical approach to identify and include explainability (xAI) components into the development of the EURMARS platform. This is be achieved by collecting end-users' requirements via end-user engagement (workshop, survey, ethics requirements meetings) which will feed backward into the design of suitable xAI indicators. The deliverable report will be written to serve as a blueprint for other border management surveillance projects.
Unique selling point	NA

Competitors (solutions)	NA
Target users / customers	Border and coast guard authorities responsible for maritime and land surveillance
Benefits for users / customers	Ensuring compliance with the AI Act and other relevant EU regulatory frameworks, and thus facilitating the EURMARS platform's easy integration for end-users.
TRL level (1-9)	NA
Main technical challenge(s)	The AI Act has not yet been adopted officially and the document is at this stage open for amendments proposed by EU member states. As such, we are currently working on the latest published draft of the AI Act, yet we will need to monitor any changes throughout the project and adapt requirements as necessary.
Legal / ethical requirements	■ Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. ■ 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). Comprehensive legal and ethical framework TBD
Involved partners	NA
IPR protection	NA

4.8 Contribution to European / international standards

KER 8: AI Foresight Report and Blueprint, PIA, EIA and SIA assessment	
Description	Participation in existing standardisation Working Groups or creating new standardisation Working Items:

What problem(s) are solved	■ Identify standardisation gaps observed in the development of the project and incorporate them in standardisation items. ■ Propose good practices or methodologies followed by any partner in the project that are not part of any existing standard, and incorporate them into standardization items.
Innovativeness / new approach	NA
Unique selling point	NA
Competitors (solutions)	NA
Target users / customers	NA
Benefits for users / customers	NA
TRL level (1-9)	NA
Main technical challenge(s)	NA
Legal / ethical requirements	NA
Involved partners	GSH, ED, BDI, VTT, AIT, UREAD (potentially the whole consortium)
IPR protection	NA

5 Individual exploitation plans

This section presents the individual exploitation plans of all consortium partners, which have been updated based on the initial plans outlined in the EURMARS proposal phase. It is important to note that some partners may have declared similar exploitation strategies without any new elements. However, as the project progresses, partners may identify different opportunities and goals for exploitation. This reporting activity will be repeated in D6.2 and D6.3, incorporating only significant changes in partners' individual exploitation plans.

The individual exploitation plans include the results that each partner intends to exploit, the specific market sectors and customer segments they will target, as well as preliminary plans for exploitation channels, expected sales, and current achievements in exploitation goals. To assist partners in drafting their individual exploitation plans, the following guiding questions were provided:

- Results to exploit: What aspects of EURMARS (technology, services, knowledge, experience, know-how, network, etc.) do you plan to exploit and for what purpose?
- Market Sectors: Are you currently collaborating or planning to collaborate with local, national, EU, or international sectors? Which stakeholders (research, industry, academia, authorities, decision-makers, etc.) are you connected with? How many people can potentially be reached?
- Channel/Actions: Which channels and actions will you employ to exploit EURMARS results?
- Expected Sales: How will EURMARS provide added value to your organization? This can include financial gains, acquired know-how, development portfolio, expanded networks, etc.
- Achieved exploitation goals: What exploitation goals have been accomplished thus far in the project? This may include the number of publications, organized events, bachelor/master/PhD theses, employed personnel, developed entities, gained know-how, etc.

By following these guidelines and addressing the proposed questions, consortium partners have laid the foundation for establishing their exploitation plans for EURMARS outputs at this stage of the project. Each partner has defined the primary exploitable items and outlined the appropriate business strategy, as detailed in the subsequent sections.

5.1 European Dynamics Luxembourg SA (ED)

Results to exploit: European Dynamics aims to maximize the potential of the Registry of Sensing & External Interfaces Subsystems and Agents. This will involve transforming it into a standalone

registry system or incorporating it into ED's wider platform offerings. Additionally, the customized Collaborative C2 System, developed for this specific project, will be utilized in other research endeavours and commercialized by offering licenses to border authorities or system integrators. Lastly, the technical expertise acquired from designing the EURMARS architecture will be applied to various other commercial and research projects.

Market Sectors: National, EU-level and international public administrations or agencies working in the civil security and defence domains.

Channel/Actions: ED will exploit the results of EURMARS by enlarging its products and services with genuinely needed solutions for cyber security. ED will exploit the project results in three ways**:**

- will enlarge its technical know-how and services within the cyber security sector with new products and services that are complementary to its own,
- will obtain new and innovative as well as competitive services that can reach public organisations where ED mainly provides services, and
- will expand its alliances with other global players of the consortium in the cyber security market.

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be estimated at current stage.

5.2 Austrian Institute Of Technology GMBH (AIT)

Results to exploit: AIT Austrian Institute of Technology GmbH plans to exploit the results of EURMARS in various ways:

- Research: AIT focus is on research and therefore cooperative research projects by national or European funding are an important pillar of our activities. AIT will further pursue to achieve multilateral projects cooperation involving industry, infrastructure operators and public authorities in the field of visual surveillance, protection and of border surveillance in particular.
- Consulting and management: In the same fields, AIT aims to perform support and consulting towards stakeholders in politics, government and industry. Furthermore, AIT can provide management of deployments for pilots and implementation of the future EURMARS platform, also in the form of a network of multiple platforms.

- Licensing and product development: AIT will provide industry with algorithms, methods, software and hardware to provide future products on the market.

AITs main contributions are part of T3.1 and T3.5, therefore AIT aims to develop a commercial solution for object detection and tracking in maritime areas in the form of a standalone sensors, combining SWIR, UV and Thermal, RGB with advanced computer vision algorithms to fuse and process the data. Additionally, AIT plans a commercial solution for its georeferenced fusion technology which improves detection qualities from different sensors. The major area of exploitation is coastal surveillance of maritime areas with detection and tracking of vessels and remote land border areas with detection of persons/vessels.

Results:

- EURMARS transportable sensing platform (combining optical sensors) at coastlines for surveillance of maritime areas close to the coast.
- Tracking and detection of vessels/vehicles/persons from a distance using advanced sensors with combined optical sensors.
- Fusion of georeferenced detections results.

This will occur in coordination with all RTOs and industrial project partners that are involved in research and technical development. Requirements and needs of the end users drive the development process since the very beginning, so that we expect a strong interest of the end users to deploy the final solution.

Market Sectors: AIT has developed over the years as a knowledge and network hub for border surveillance and can count many contacts in the field. EURMARS technological insight will be exploited by AIT to advise major players in government and industry, who will benefit from an in-depth knowledge. AIT will provide future services in research and technology in the field with highest quality and impact.

Therefore, the AIT market is on National- and EU-level for public administrations/agencies or industry partners working in the civil security and defence domains.

Channel/Actions: AIT will foster to establish liaisons with industry partners and border organisations (e.g., Frontex) to explore the developed technologies in public tenders and active sales towards our current and prospective customers.

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.3 Teknologian Tutkimuskeskus VTT OY (VTT)

Results to exploit: The EURMARS project will generate results for VTT that can be exploited in future research projects and in commercial activities that we provide for a multitude of customers in the security field, both governmental organizations and the private sector. Although VTT is an RTO, we have contracted research work in our offering portfolio.

The research results relating to the understanding of practitioner needs/requirements, processes and operational environments (WP2 and WP5 research work) provide valuable insights for future commissioned work. Humans, in other words end-users, may often form the bottleneck of excessive and effective utilisation of new technological solutions and systems. The EURMARS results can be used in bridging the gap between border security personnel and technology in the future ways of working in security domain. The human factors knowledge can be exploited for services that relate to for example operational concept designs, standardization, business process development, feasibility studies, technology forecast studies or requirements specification in support of enhanced border management. Supporting WP4 activities in user interface development also provides synergies for both jointly funded and commercial projects that focus on developing situational awareness systems for security-critical applications.

At the general level, participation in EU funded border security projects opens new business opportunities for VTT also in the research and innovation consulting area. The EU added value from these projects is the comprehensive overview together with the grassroots level intake from different border environments of EU MS with distinctive national variants and characteristics, affecting key processes at the local level.

Market Sectors: National, EU-level and international public administrations or agencies working in the civil security and defence domains.

Channel/Actions: Participation in national and EU-level public funding tenders and active sales towards our current and prospective customers. VTT is an active partner in many national and international level security networks and research communities. Project outcomes such as publications and white papers strengthen our visibility and role as a border security expert organisation.

VTT will be participating in national and EU funding programmes serving similar aims as EURMARS.

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.4 Geosystems Hellas It Kai Efarmoges Geopliroforiakon Systimaton Anonimi Etaireia (GSH)

Results to exploit: GSH will develop a complete module that provides novel and state-of-the-art solutions in remote sensing by utilizing both free and commercial satellites. The processing of these various data sets will be done using open-source software, which offers the opportunity to function as an autonomous part that can be easily migrated to different systems and architectures. This product can contribute significantly to defence and security by detecting dark vessels and monitoring the activities related to them. Additionally, with the inclusion of more satellite sources, the final product can be used for constant monitoring of maritime events, such as oil spills, and tracking suspicious ships. It can also serve as a complementary component to other systems for continuous monitoring.

Moreover, the development of appropriate AI/ML models for the detection tasks enhances the expertise in using pattern recognition algorithms, their training process, and setting them up to match specific needs and requirements. The performance and reliability of the designed systems will be measured using traditional metrics and tests, leading to enhanced knowledge in optimization for such tasks.

Market Sectors: GSH is a member of European Association of Remote Sensing Companies (EARSC) and intends to present the EURMARS platform and find possible audiences via this channel. In addition, interconnections with European and national industries will be examined as possible audiences.

Channel/Actions:

Channels:

- **Physically:** In-person meetings with appropriate audience, participation in commercial exhibitions and in conferences related to security and defence.
- **Digitally:** Website of Geosystems Hellas, GSH's social media.

Actions:

- Dedicated Sales Team: Establish a specialized sales team with people who are informed about the features, advantages, and value proposition of EURMARS. Reaching out to potential consumers, such as defense and security companies.

- Presentations and Product demos: Hold presentations and product demos to highlight EURMARS features and advantages. Describe how the tool may contribute to. Make presentations and demos specific to the wants and needs of potential clients.

Expected Sales: EURMARS will lead not only to financial gains for GSH but also to expand its network. Additionally, GSH will enhance its position in the defence and security sector.

Achieved exploitation goals: NA.

5.5 Hardware And Software Engineering EPE (HSE)

Results to exploit: The primary aim is to strategically present the culmination of technological advancements, innovative services, knowledge, and extensive experience that have been cultivated through the EURMARS project. Our intention is to meticulously showcase the success and multifaceted benefits of the developed solution to a wide-ranging network of clients, resellers, and collaborators. By spotlighting these outcomes, we seek to demonstrate not only the project's technical prowess, but also its real-world applications, positioning it as a transformative solution capable of addressing the most pressing challenges within the targeted domains.

Market Sectors: Collaborate with a wide network of clients, resellers, and collaborators across local, national, EU, and international sectors. Connect with stakeholders in research, industry, academia, and decision-making authorities to reach a diverse audience.

Channel/Actions:

- Explore integration possibilities with existing systems and solutions to enhance effectiveness and efficiency across relevant domains.
- Develop comprehensive documentation, case studies, and reference materials highlighting successful implementations.
- Organize workshops, seminars, or webinars to share insights and lessons learned, fostering knowledge exchange.

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.6 Thales Alenia Space France SAS (TASF)

Results to exploit: The EURMARS project will generate for us valuable technical results, coming from research level to a pre-operational component level for detecting and tracking vessels. The component will be then part of our ground segment features portfolio. Moreover, this corresponding to a first level in AI tracking technology mastering, while the next step would be to extrapolate a wide resolution range, and also to a wide object types of range that could make sense for different applications in civil or defence domains. Since the component could be fed with images provided by a telescope onboard a geostationary satellite, but also any other platforms such as UAV, a wide business perspective could be open.

Market Sectors: National and EU level for public administrations/agencies; national defence, and *export customers* requiring civil security and defence solution.

Channel/Actions: Demonstration to potential customers as part of our ground segment solution.

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.7 Center Odlicnosti Vesolje, Znanost In Tehnologije (SPACE-SI)

Results to exploit: Space-SI will develop New Earth Observation concepts by combining video from space with multispectral and panchromatic imaging. The agile multi-payload Nemo-HD satellite platform enables highly innovative EO acquisitions from a variety of precisely guided observation angles where different combinations of payloads can be activated for low latency EO missions.

Nemo-HD microsatellite is providing cutting-edge space video with accurate and stable point targeting. This feature enables monitoring of maritime traffic allowing for video analytics with ship detection and movement tracing options. Space-SI will develop satellite observation scenarios dedicated to marine monitoring using multi-sensor, multi-scale satellite imaging and video recording, agile tracking, near-real-time data download through our ground station and data processing using our data processing chain. Such scenarios can be adjusted also for other sectors and areas of interest.

Market Sectors: National, EU-level and international public administrations or agencies including maritime authorities, civil protection and ecosystem services.

Channel/Actions: B2B meetings, presentations at conferences and symposiums, public tenders, private (sub)contracting, new national and international research and development projects.

Expected Sales: 0,75 MEUR.

Achieved exploitation goals: Agile multi-payload satellite acquisitions for EO services.

5.8 Trilateral Research Limited (TRI)

Results to exploit: The results generated by the EURMARS project can be exploited by TRI in future research project and commercial activities in the security field.

As Ethics lead for EURMARS, TRI deepened and demonstrated its competency and expertise in the security space. TRI established the Ethics and Innovation Management plan for the project, and created an Ethics Risk Assessment Tool (ERAT) designed to facilitate the identification, assessment, mitigation, and monitoring of any potential Ethics risks impacting the project throughout its entire cycle (pre-deployment, deployment, post-deployment stages). In addition, TRI will demonstrate additional thought leadership and expertise.

TRI will deliver a blueprint for a responsible research and innovation approach (RRI) of other border management surveillance projects in the incipient regulatory environment of the European AI Act (T2.4 on AI ACT Foresight Compliance, Social and Ethical Impact Assessment). TRI will also create a training programme that will outline how border guards can use the system developed while ensuring ethical awareness & knowledge are increased (T5.7 on Training & Ethics Monitoring).

Given their nature and consideration for EU and national regulatory frameworks, TRI's project outputs demonstrate thought leadership, establish our competence as a research partner and can be adapted to other border management projects TRI and/or its partners are running in the foreseeable future.

Market Sectors: National, EU-level and international public administrations or agencies, NGOs and other research institutions working in the civil security and defence domains**.**

Channel/Actions: B2B meetings, presentations at conferences and symposiums, new research project in the security sphere

5.9 Glavna Direktsia Granichna Politsia (GDBP)

Results to exploit: GDBP will harness new knowledge and technological insights in border surveillance, incorporating AI and ML integrations into its operational protocols. This will facilitate a more robust monitoring system that allows for the rapid detection and prevention of illicit activities across borders. The data assimilated during the project will be instrumental in creating dynamic response strategies, enhancing collaboration with other agencies, and fostering a culture of innovation and foresight in border management.

Market Sectors:

- National and EU-level public administrations or agencies.
- International public administrations or agencies working in the civil security and defence domains.

Channel/Actions:

- B2B meetings to foster collaborations and partnerships for technology sharing and implementation.
- Hosting and attending conferences and symposiums to present the findings and technological advancements obtained through the EURMARS project.
- Participating in public tenders to facilitate the acquisition of state-of-the-art technologies and knowledge garnered through the project.
- Collaborative research and development projects to further the goals achieved in the EURMARS project and to explore new avenues of technological advancements in border management.
- Training programs and workshops to disseminate knowledge and to foster skill development in utilizing the new technologies.

Expected Sales: While GDBP is primarily focused on enhancing security rather than revenue generation, it is envisaged that the incorporation of the technological advancements from the EURMARS project will lead to more streamlined operations, potentially attracting investments and funds for further developments.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.10 Ministry Of Transport, Communications And Works (JRCC)

Results to exploit: EURMARS general system and the ability to integrate sensors**.**

Market Sectors: National, EU-level and international public administrations or agencies working in the civil security and defence domains.

Channel/Actions: Through JRCC official website and social media accounts.

Expected Sales: Not applicable.

Achieved exploitation goals: Can't be determined at this stage.

5.11 General Maritime Directorate (GMD)

Results to exploit: GMD will study the possibility of expanding digital systems for monitoring different navigational areas by increasing the distance of maritime monitoring. In maritime security monitoring, there are several aspects where GMD will expand the possibility of using dedicated satellite systems. Primarily among these in the prevention of illegal acts are the attack on criminal activities related to clandestine movements, the transport of prohibited items and weapons, etc. Also, monitoring marine pollution is a very important objective for the surveillance of marine areas. The main goal of achieving the profitable objectives of EURMARS is the creation of a system which can determine the polluted area and follow the traces of the vessel/ship which is supposed to have created the pollution. In terms of monitoring marine pollution, GMD has a high sensitivity since these activities have a profound national and international impact.

The satellite connections, which after tests and exercises will be effective with their conclusions, will be an achievement in improving the main goals of GMD such as security in maritime areas and protection of the marine environment.

Market Sectors: GMD intends to implement the system in its activity through the Inter-institutional Maritime Operational Center (IMOC) through which the monitoring of the maritime areas of the Republic of Albania and the connection with the neighboring countries is carried out. Also, the effectiveness of the system will be the subject of promotion by agencies related to maritime safety and environmental protection activities such as The National Environmental Agency, Department for Borders and Migration and other stakeholders etc.

Channel/Actions: Workshop meetings with appropriate audience, participation in commercial exhibitions and in conferences related to maritime security and marine environment protection.

Systematically, it will proceed with the updating and conclusions of the effectiveness of the system on the official website of GMD and on social networks.

Expected Sales: Not applicable at this stage.

Achieved exploitation goals: Not applicable at this stage.

5.12 Inspectoratul General Al Politiei De Frontiera (RBP)

Results to exploit: RBP intends to utilize the operational capabilities and technical expertise gained through participation in the EURMARS project. Specifically, RBP aims to exploit:

- Knowledge and experience in deploying advanced surveillance technologies.
- Improved situational awareness and common operating picture from integrating diverse sensing systems.
- Enhanced inter-agency collaboration and information exchange capabilities.
- New skills in utilizing multimodal data fusion and decision support systems.

RBP will seek to incorporate these into its border security operations to augment detection, interdiction and response capabilities.

Market Sectors: As a public sector agency, RBP's primary market is the government sector responsible for border security in Romania. This includes collaborating with local, national and European level authorities in the areas of defence, law enforcement, border police, coast guard, and critical infrastructure protection.

Channel/Actions:

- Integrate EURMARS capabilities into border surveillance infrastructure at high-risk border areas.
- Provide specialized training to border police personnel on utilizing integrated surveillance systems.
- Participate in joint exercises with other agencies to demonstrate EURMARS outcomes.

- Engage national and European policymakers on adopting advanced technologies for border security.
- Collaborate in future research projects to continue improving border management solutions.

Expected Sales: As a public agency, RBP's aim is improved border security rather than revenue generation. However, successful adoption of EURMARS outcomes could lead to budget allocations for procuring new systems.

Achieved exploitation goals: Can't be determined at this stage.

5.13 European Union Satellite Centre (SATCEN)

Results to exploit: SATCEN aims to exploit EURMARS based in two actions: Long-term sustainability and engagement activities from the foreseen living labs. The aim of this strategy will be the technologic transference and scientific advancements to increase internal capabilities as a benefit for the decision-making process. Moreover, the expected exploitation will be linked with the foreseen improved border authority surveillance capabilities, the security and risk assessment improvement and performance of the current existing surveillance capabilities. Among the expected capabilities to be developed, the automatic detection of dark vessels, pattern recognition algorithms and 24/7 vessel tracking will be a considerable potential added value to be exploited internally with the aim to improve internal capabilities. Those new capabilities will come hand-in-hand with gained know-how which could be the base for developing, improving and/or enlarging our existing portfolio.

Market Sectors: Currently, it is foreseen to be exploited internally by our imagery analyst, being their main tasks linked with the Security and Defence sector. Expected partners can benefit from the development and availability of EURMARS. Obtained scientific and technological development can improve skills and know-how, and will be not just shared within our Agency but externally to our user´s community whenever that possibility exists (i.e.: interagency cooperation, training activities,...).

Channel/Actions: Use of appropriate channels to efficiently communicate with the target groups and stakeholders (internal events, meetings and social media networks when feasible) to support relevant actions for project dissemination. Other relevant EU projects synergies can be identified and used as a multiplier for dissemination.

Expected Sales: Cannot be estimated at the current stage; however, this information will be updated once the first results of the pilot use case are released.

Achieved exploitation goals: Cannot be measured at this moment of the project.

5.14 Institut Po Otbrana (BDI)

Results to exploit: The Bulgarian Defence Institute "Prof. Tsvetan Lazarov" renowned for its expertise in defence and security, has consistently demonstrated its prowess as a scientific institution. One of its key endeavours includes providing training for the attainment of academic and scientific degrees, such as the "Doctor" and "Doctor of Science" degrees through accredited doctoral programs. Notably, the EURMARS system's outcomes are poised to significantly enhance and refine the training of PhD students. The methodically crafted and rigorously validated EURMARS system carries considerable potential as an invaluable asset for educational endeavours within the Bulgarian Defence Institute. Tapping into the capacities of the EURMARS system is anticipated to heighten the Institute's educational capabilities while also bolstering its research undertakings.

The Bulgarian Defence Institute believes that the technological advancements and knowledge garnered from the EURMARS project can play a pivotal role in aiding the initiatives of the Bulgarian Ministry of Interior and the Bulgarian Ministry of Defence. The goal is to bolster efforts in curbing cross-border crime and establishing capabilities to pre-empt illicit cross-border activities. In alignment with these ambitions, the BDI will execute essential training and educational initiatives for border enforcement agencies affiliated with the Ministry of Defence, Bulgarian Naval Academy, Ministry of Interior, and Bulgarian Ports Infrastructure Co (BPI Co.). These entities will be equipped to adeptly utilize the integrated EURMARS platform, with future potentiality for establishing a Distributed Command Centre.

The advanced technologies integrated into EURMARS, which encompass the collection and analysis of data from diverse sensors and information sources, confer a distinct informational edge. This confers enhanced situational awareness and the capacity to anticipate malicious actions by prospective migrants and traffickers. An envisioned implementation of the EURMARS platform is poised to significantly augment the capabilities of the Ministry of Interior and the Ministry of Defence in managing cross-border crime and pre-empting illegal activities within the economic and offshore zones along the Black Sea coastline.

With a steadfast commitment, the Bulgarian Defence Institute "Prof. Tsvetan Lazarov" remains resolute in its dedication to ensuring that the EURMARS platform significantly enhances border control capabilities, aligning harmoniously with the directives set forth by the European Commission. In this way, we will increase our expertise in the security engineering domain and the exploitation of the EURMARS asset will enhance the BDI’s capabilities for participating in proposals under the HORIZON Europe programme.

Market Sectors: National, EU-level and international public administrations or agencies working in the civil security and defence domains.

Channel/Actions: Participation in national and EU funding programmes serving similar aims as EURMARS.

Expected Sales: Cannot be estimated at the current stage.

Achieved exploitation goals: Cannot be determined at this stage.

5.15 The University Of Reading (UREAD)

Results to exploit: UREAD will develop advanced algorithms and methodologies for the research that needs to be conducted under the EURMARS project. The main contribution will be on findings related to the integration of AI and ML in maritime surveillance and various insights and knowledge from the collaborative academic/market explorations and joint studies undertaken with partners.

Market Sectors: The contribution of UREAD will be primarily on digital technology & computing as well as consulting in meteorology and environmental studies. However, university's law school and related research centres may, to the extent allowed by the circumstances, be engaged in consultancy or collaborative research, to provide legal and policy consultancy, leveraging its renowned capabilities in the respective field.

Channel/Actions:

- Collaborative projects with defence agencies and industry partners.
- Offering specialized courses or training programs based on the findings and methodologies derived from EURMARS.
- Licensing of developed technologies and related offerings to interested trusted stakeholders.

Expected Sales:

Although these would be quite speculative at this point, UREAD could anticipate:

- increased funding or research grants based on the successful outcomes and innovations achieved through EURMARS.
- Potential licensing deals with tech companies interested in utilizing the respective findings.

- Income from specialized training programs or courses tailored to professionals in the maritime and defence sectors.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.16 Home Office (UKH)

Results to exploit: UK security organisations already use a well-developed multi-source fusion system to collate, display and analyse maritime data. The results of the EURMARS project will be assessed to determine, if any of the capabilities can be ingested into that system to provide new or improved ways of working. The outputs of the AI/ML engines in particular could be of benefit as we seek even greater processing power for the vast amounts of data received. A second result would be to investigate the architecture that is developed and how multiple systems can be attached and operated through it. The project will allow UKH personnel to identify and engage with European providers on a range of ISR capabilities. The capabilities provided will also allow the UK to benchmark its systems against the latest EU technologies.

Market Sectors: The UK already collaborates broadly both nationally and internationally with government authorities, industry and academia working in the civil security and defence domains. EURMARS results will enable UKH as an end-user to identify technologies to chase for further development.

Post-Brexit, the UK's relationship with the EU is complicated. It is not known if further collaboration, planning and development may be possible out with the EURMARS project.

Channel/Actions: Post project analysis will enable UKH to identify the technology providers of interest and to follow up with additional trials and exploitation where funding and people resource allow. There may be unique services that can be incorporated into the UK national system.

Expected Sales: As an end user, UKH does not foresee being in a position to sell any part of the EURMARS system, nor what it would pay for any of the developed services. However, in terms of added value, there could be significant benefit in unique sources of data into the UK Common Operational Picture. The relationships developed through the project will also offer opportunities to enhance intelligence and analysis networks.

Achieved exploitation goals: Cannot be determined at this stage.

5.17 SKYLD Security And Defence Limited (SKYLD)

Results to exploit: SKYLD the previous years has invested in R&D in the topic of the project. This has resulted in participating in different collaboration projects with Cypriot and international stakeholders like the Cyprus Police (Community Police and Coast Guard), Ayia Napa Marina, etc.

SKYLD is interested in:

- keeping the ownership of any results generated exclusively from SKYLD IP and from work performed exclusively by SKYLD and have joint ownership regarding results which are generated by SKYLD in collaboration with one or more other partners. Moreover, SKYLD will improve the expertise in areas such as:
- create patents to protect the foreground IP of the consortium where possible.
- exploit (after project completion) the results and generate revenue by commercialising the project's solutions by having the option to deploy the full system without restrictions in cooperation with other partners, based on a previously-agreed contract and licensing agreement.

All the above, will increase the SKYLD's position in Cypriot market as well as will introduce SKYLD as an innovative company expert in her field that provides state of art solutions. This aspect will help in the better commercialization of all SKYLD product/services in Cypriot market as well as in other areas that SKYLD operates e.g., Balkans and Middle East. Moreover, an increase in the revenue from these product/services' commercialization is expected to help the company expand her scientific and business competences.

Market Sectors:

- National,
- EU-level,
- International.

Channel/Actions:

- Public tenders,
- Private (sub)contracting,
- Future Cypriot and EU funding programmes (Horizon Europe, EDF, etc).

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be evaluated at current stage.

5.18 Office National D'etudes Et De Recherches Aerospatiales (ONERA)

Results to exploit: ONERA plans to leverage the advancements fostered through the EURMARS project to enhance its technological offerings and establish itself as a vanguard in the field of aerospace and defence research. Key focus areas include:

- Research and Development: Harnessing the innovations in sensory technologies and AI algorithms developed in the EURMARS project to foster ground-breaking research initiatives and collaborations, thereby advancing ONERA's technological frontier.
- Consultancy and Expertise: Leveraging the knowledge and expertise acquired from the project to offer consultancy services to governmental and non-governmental organizations, aiding them in leveraging cutting-edge technologies for defence and security applications.
- Licensing and Products: Developing a portfolio of licensable technologies and products, including sophisticated sensing systems and AI algorithms, to offer to defence contractors and security agencies worldwide.

Market Sectors: ONERA aims to target the following sectors:

- Public Administrations and Agencies: Collaborating with national and EU-level public agencies involved in civil security and defence.
- Research Institutions and Academia: Establishing partnerships with research institutions and academic organizations for collaborative research and knowledge exchange.
- Industry: Collaborating with defence contractors and industry players to integrate ONERA's technologies into commercial products and solutions.

Channel/Actions: To exploit the results of EURMARS effectively, ONERA will undertake the following strategies:

- Knowledge Dissemination: Organizing webinars, seminars, and workshops to disseminate knowledge and foster collaborations with potential stakeholders.

- Collaborative Projects: Seeking collaborative projects at national and EU levels to apply the technologies developed in real-world scenarios.
- Licensing and Product Development: Developing a structured approach to licensing technologies and products to industry players, including offering comprehensive support for integration and deployment.
- Publications and White Papers: Publishing research findings in reputed journals and conferences.

Expected Sales: Cannot be estimated at current stage.

Achieved exploitation goals: Cannot be evaluated at current stage.

6 Intellectual Property Rights (IPR)

A comprehensive Intellectual Property Rights (IPR) strategy is crucial for the fruitful utilization, considerable influence, and safeguarding of key exploitable results generated during the EURMARS project. Consequently, it's imperative that all EURMARS consortium partners collectively design and consent to a strategy. This will delineate the cooperative framework and outline the commercial or industrial utilization aspects that will be safeguarded by Intellectual Property Rights. This mutual agreement will be codified in an IPR (Intellectual Property Rights) Agreement.

The IPR Agreement, which builds on the Consortium Agreement (CA) already endorsed by all partners, will dictate responsibilities and rights pertaining to EURMARS foreground Intellectual Property (IP) ownership and utilization. The agreement's primary functions are:

- Enhancing awareness about IP-related issues amongst participants.
- Helping resolve disputes between participants.
- Assisting in creating the plan for the application and spread of foreground.
- Identifying outcomes that require protection and advising partners on suitable protection methods.
- Supporting participants in gauging their input to the jointly owned foreground and deciding their corresponding shares
- Making decisions about third parties joining the consortium with the intention to gain ownership of a specific Party's Foreground.

EURMARS partners can choose from various methods to protect the Intellectual Property created during the project. These methods might include trademarks (exclusive rights over distinctive signs), patents (exclusive rights over an invention for a specified time), copyright (rights over literary, scientific, and artistic works, computer programs, databases), trade secrets (valuable technology or other types of information), etc.

Additionally, the potential outputs of the EURMARS project can be divided into three main categories:

- For additional research (for example, architecture module designs, algorithms, parts of software applications, etc.)

- For creating and commercializing marketable products (for example, application, tool, component, simulation hardware) or services (for example, border surveillance training, consultancy, EURMARS technical support, etc.)

- For creating and providing a service for others, either jointly exploiting the EURMARS solution developed under the project based on joint ownership terms and conditions, or individual exploitation of the individual contributions of the parties in the developed EURMARS solution.

This version of the deliverable D6.1 provides an initial identification of any new intellectual property created. Nonetheless, at this preliminary stage, partners have not yet decided on the most suitable strategy to protect this IP. In the upcoming months, during the project's second phase, an optimal path for protecting the foreground IP will be determined. These findings will be included in the next iteration of this deliverable.

As mentioned earlier, the foundation for the IPR was laid out in the EURMARS Consortium Agreement. It contains several sections relevant to IPR management, ownership, transfer of results, and exploitation rights:

- Ownership of Results (Section 8.1 of the CA): There are established guidelines for handling the ownership of results, stipulating that results are owned by the party that generates them.

- Joint Ownership of Results (Section 8.2 of the CA): Regulations are in place to handle the legal facets of the exploitation and protection of IPR in cases of joint ownership.

- Transfer of Results (Section 8.3 of the CA): Each party may transfer ownership of its own results, following GA Article 30 procedures.

- Access Rights to Results for Exploitation (Section 9.4 of the CA):

  - Access rights to results needed for exploitation of a party's own results will be provided on fair and reasonable terms.

  - Access rights to results for internal non-commercial research activities will be granted royalty-free.

6.1 Background technologies / Know-How

Background as defined on The European Participant Portal glossary:

"Any data, know-how and/or information, whatever its form or nature (tangible or intangible) including any rights such as intellectual property rights which are needed to carry out the project or exploit its results".

Table 3 shows all background technologies and know-how that the consortium partners have used for the implementation of the EURMARS project, with particular emphasis on the associated Intellectual Property Rights, as identified in the Consortium Agreement.

Table 3. IPR Ownership per Technology background and Know How

Background Technology / Know-How	IPR Ownership
Command and Control Platform (FOLDOUT C2 system along with upper modes)	ED
Methods, procedures and SW implementations for real-time thermal and visual data processing with NVidia platforms.	AIT
Methods, procedures and SW implementations for real-time capable thermal and visual detection and classification with artificial intelligence	AIT
Methods, procedures and SW implementations for real-time capable processing control and orchestration of multiple video or data processing modules (Connected Vision Framework / SDK).	AIT
Know-how and example setups of cross-platform, multi node real-time data communication.	AIT
Know-how and example setups of cross-platform, multi node software deployment and operation.	AIT
ROS interface between sensors and real-time fusion modules (software). ROS Nodes (software) for calibration and fusion.	AIT
Methods, procedures and SW implementations for real-time processing of location and orientation sensors.	AIT
Patent: Method for real-time fusion of sensor data and automatic alerting, EP 3 352 111 B1 "Critical event detection method".	AIT
Patent: Method for real-time fusion of sensor data and automatic alerting, EP 3 352 111 B1 "Critical event detection method".	AIT
GeoViewsion: Web-based GIS visualization for the display of georeferenced real-time sensor data and fusion results.	AIT

Clusterability tool: Clustering is used to gain an intuition of the structures in the data. It measures the prominence of clustering structure in the data to evaluate whether a cluster analysis could produce a meaningful insight to the relationships in the data.	VTT
Self-learning tool: In machine learning, Positive-unlabelled learning is a special case within semi-supervised learning. In positive-unlabelled learning, the training set contains some positive examples and a set of unlabelled examples from both the positive and negative classes. Self-learning is a semi-supervised method capable of PU learning in time-series data. In the self-learning approach, observations are individually added from the unlabelled data into the positive class until a stopping criterion is reached. The tool fundamentally is able to discriminate between classes automatically without parameterization and regardless of the balance of the classes (amongst different classes).	VTT
Hyperspectral image analysis algorithm: The Algorithm facilitates automatic identification of several materials or objects from a single pixel. In particular, this capability makes the algorithm suitable for detecting subpixel objects (objects smaller than a single pixel). The Algorithm is non-Bayesian, whereby it runs several times faster and is easier to interpret than its Bayesian counterparts. Furthermore, the algorithm appears to have substantially lower false positive rate than its Bayesian alternatives.	VTT
Software: ■ **DeeperVision**: a Thales Alenia Space internal project that consists in developing Artificial Intelligence image processing tools. During this project, different types of algorithms and architectures have been tested, the impact of the parameters and the quality of input data have been studied, and many tools have been developed to adapt the Deep Learning algorithms on EO satellite data. ■ **EarthLIVE**: Automated information extraction from Earth Observation Data from GEO Permanent Monitoring. Objects (position, speed, route), Meteo & Environment phenomena (cover, position, speed, route), Changes/ evolutions, etc. **Publications:** ■ M. Aubrun, A. Troya-Galvis, M. Albughdadi, R. Hugues, M. Spigai: Unsupervised learning of robust representations for change detection on Sentinel-2 Earth Observation images, ISESS, 2020	TASF

■ R. Hugues, A. Pailloux, M. Aubrun, M. Spigai, E. Barritault, A. Scotto di Perrotolo, A. Gaurier: Robust plane detector for multi-sensor satellite images, Big Data from Space, 2019	
SPACE-SI background know-how is related to the SPACE-SI Earth observation system that combines Nemo-HD microsatellite mission for acquisition of video and multispectral images, STREAM and AXYOM ground station systems and STORM satellite data processing chain.	SPACE-SI
Trilateral's Methods, Templates and Tools for impact assessments and related ethics/privacy work	TRI
SKYLD drones/ UAVs (including Small, Long Endurance Fixed Wing UAV, Helicopter UAV and Versatile Multi-Rotor Platforms) with different flying characteristics, payload configurations and operational costs and constitute the fleet ready to execute EURMARS requested missions	SKYLD
Methods and software module for object tracking	UREAD
Methods and software module for anomaly detection and alarming	UREAD
Methods and knowledge for data capture, annotation and generation of test data repository	UREAD
Methods and knowledge in benchmarking (performance evaluation)	UREAD
Methods and know-how for generation and execution of demonstration scenarios/use cases	UREAD

6.2 Foreground technologies / Know-How

Foreground as defined on The European Participant Portal glossary:

"*Any tangible or intangible output of the action (such as data, knowledge and information, whatever their form or nature, whether or not they can be protected), which are generated in the action, as well as any attached rights, including intellectual property rights*".

Table 4 shows preliminary information regarding IPR ownership of the EURMARS outcomes. This information should be considered as an initial identification since it will be updated and finalised towards the end of the project. IPR ownership is based on the development of relevant outcomes by specific partners, during the development of the project.

Table 4. IPR ownership of the EURMARS outcomes

PARTNER	No.	Project outcome
GSH	1	Maritime surveillance through satellite data
GSH	2	Monitor environmental indicators through satellite data
GSH	3	Vessel detection through satellite data
GSH	4	Oil spill detection through satellite data

7 Horizon Results Booster

In order to increase the impact of EU funded projects the EC has initiated the HORIZON Results Booster (HRB). In the oncoming months, EURMARS will take advantage of this initiative and explore the possibilities to boost its impact. As shown in Fig. 1, the main objective of the Horizon Results Booster is to assist the EU funded projects with broader dissemination and exploitation possibilities without additional costs for the consortia. It is supposed to shorten and enable a better transfer of results to policy makers, the market/industry and to society. The Booster itself consists of three different areas of support, which build upon each other. The overview of services is shown in Fig. 1.

Figure 1. Horizon Results Booster services

7.1 Portfolio Dissemination & Exploitation Strategy

This service consists of three separate modules which can be booked as single offers, in combinations of two of them or as the whole package:

- **Module A** is about identifying and creating the portfolio of R&I project results. Besides identifying the project results being suitable for dissemination, it also contains guidance for identifying similar ongoing publicly funded projects on regional, national or EU level and stakeholder and target audience mapping. This way synergies within common disseminating can be created.

- **Module B** represents the next step, where projects are supported in designing and executing a portfolio dissemination plan. For example, a short video describing the project results would also be a result of this part.

- **Module C** envisions the possibility of getting support in improving the already existing exploitation plan is offered: Key exploitable results of the project are identified, exploitation paths of results are being outlined and a risk analysis related to the exploitation is being performed.

7.2 Business Plan Development

As a next step and for taking the project results to the market a tailored training for setting up a business plan is being offered, including market analysis, a business strategy, an operation plan etc. A clear action plan to be implemented in a certain time frame is also being set up. Interesting in long-term for EURMARS is the assistance to identify solutions for implementation in terms of:

- Start-up operations (e.g., identification of incubators, third party support for management – legal, administrative)

- Investors (e.g., identification of venture capitalists in the market sector, identification of business angel networks)

- Funding (e.g., identification of financial instruments for start-ups or new businesses from banks, local governments, national funding, identification of crowdfunding platforms and schemes)

7.3 Go-to-Market Support

Last but not least, it is also possible to get assistance and mentoring as well as contacts with market stakeholders in regard of pitching the products, IPR, innovation management and other business services.

Service 1 – Portfolio Dissemination and Exploitation Strategy (PDES)		
Module A: Identification and creation of the	■ Identification of similar projects to form a project group.	Single projects &

portfolio of R&I project results	■ Identification of portfolio results. ■ Mapping of relevant Stakeholders.	project groups.
Module B: Portfolio Dissemination Plan (design and execution)	■ Design of a joint dissemination plan. ■ Creation of graphic material for joint activities. ■ Capacity building to improve your communication and dissemination skills. ■ Support on copywriting, social media activities, etc.	Project groups.
Module C: Assisting projects to improve their existing exploitation strategy	■ Review of key exploitable results. ■ Review of the exploitation plan and identification of the exploitation path. ■ Stakeholders' identification in the value chain. ■ Support for exploitation risk analysis.	Single projects.
Service 2 – Business Plan Development (BPD)		
Assist beneficiaries to bring their results closer to the market by developing an effective business plan.		Single projects.
Service 3 – Go-To-Market Support (G2M)		
Support to Pitching, IPR guidance, Innovation management, Business services, exploitation options, access to non-EU funding.		Single projects & project groups with high Technology Readiness Levels (>6) and mature projects.

8 Standardisation Activities

8.1 Introduction

The EURMARS project aims to constitute a robust solution for surveillance purposes incorporating state-of-the-art and novel technologies and workflows. The whole architecture includes hardware and software tools in a high TRL and tries to address major issues with the most efficient and reliable ways. Therefore, it is essential that the best practices and methodologies be monitored daily and standardized.

Task 6.3, more specifically, is responsible for the **Standardisation Activities.**

Task 6.3 - Standardisation Activities is twofold:

- it aims to continuously evaluate project developments towards compliance with the latest standards, regulations and methodologies. This point is essential for ensuring the smooth development of the project and to assure a minimum level of functional results.
- it aims to deliver any practical knowledge, practices, methodologies and procedures followed in every stage of the project's development to ongoing standardisation activities. Additionally, the project may contribute to more specialized agencies or unions that are engaged with awareness raising, consulting, promoting technological culture and supporting activities among all EU member states. These will be achieved by the participation of the consortium in standardization activities in relevant fields hosted by European and international organizations like CEN/CENELEC, ETSI, ISO and ENISA Ad Hoc Working Groups. Last but not least, this Task aims for openness that is to enable enterprises and communities to interface with EURMARS technology and concepts.

8.2 Standardisation landscape

8.2.1 An overview

Standards play a crucial role in facilitating smooth and efficient interactions between individuals, organizations, and industries. They provide a common language and framework that enables reliable communication, collaboration, and interoperability. Standards also establish a level of

quality, safety, and performance that fosters consumer confidence, protects public health and safety, and drives innovation. In many cases, standards are essential for regulatory compliance, market access, and international trade. By promoting consistency and predictability, standards can help reduce costs, improve productivity, and accelerate time-to-market. Moreover, standards can enable the integration of emerging technologies, such as Artificial Intelligence, into various applications and industries. Overall, standards are critical for achieving economic growth, sustainability and social progress in the globalized world.

There are numerous organizations involved in developing standards, ranging from companies, consortia, and industry in the private sector, to national, regional and international organizations. This deliverable has identified standards from the following organizations: ISO, CEN, CENELEC, ETSI and ENISA Ad Hoc Working Groups. Furthermore, the engagement and contribution of the program's delegates could pertain to collaborative Working Groups operating under the auspices of all the aforementioned entities.

8.2.2 Standardisation Documents

There is a series of standardisation documents that will be referred to in this sub-section followed by various details. The general definition of a standard is as follows, “document, established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context”. Specifically, standardisation documents can be divided into the following categories:

- **European standards:** European Standards are documents that have been ratified by one of the three European Standardization Organizations, CEN, CENELEC or ETSI. Their application is voluntary, but the adoption at national level as standard is mandatory. The process in theory, takes between 2 and 3 years.

- **ISO standards:** International Standards are documents that have been ratified by one of the two International Standardization Organizations, ISO or IEC. Their application is voluntary, and the adoption at national level is also voluntary. The process, in theory, takes 3 years.

- **National standards:** A national standard is a technical specification or document that is developed and maintained by a specific country's national standards organization or body. It outlines guidelines, requirements, and criteria for products, services, processes, or practices within that particular country. While compliance with national standards is typically voluntary, they can become essential for businesses to compete effectively in the domestic market.

Apart from European, international, and national standards, there are other types of documents, primarily Technical Specifications (TS) and Technical Reports (TR), which have a lower level of

consensus and a faster drafting timeframe. Additionally, there are Publicly Available Specifications (by ISO) and Guides.

- **Technical Specification (CEN/TS):** A Technical Specification (TS) is a normative document, the development of which can be envisaged when various alternatives that would not gather enough as to allow agreement on a European Standard (EN), need to coexist in anticipation of future harmonization, or for providing specifications in experimental circumstances and/or evolving technologies. The process usually takes between 15 and 21 months since activation. In addition, these documents require a high level of consensus in an established standardisation body. No time limit is specified for the lifetime of TSs, but the responsible Technical Body shall ensure that they are reviewed at intervals of not more than 3 years, starting from their date of publication by CCMC.

- **Technical Specification (ISO/TS):** A Technical Specification (TS) addresses work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard.

- **Technical Report (CEN/TR):** A Technical Report (TR) is an informative document that provides information on the technical content of standardization work. It may be prepared when it is considered urgent or advisable to provide additional information to the CEN and CENELEC national members, the European Commission, the EFTA Secretariat, other governmental agencies or outside bodies. A Technical Report is established by a CEN and/or CENELEC Technical Body and approved through a simple majority vote by the CEN and/or CENELEC national members. It involves no obligation at national level. No time limit is specified for the lifetime of TRs, but it is recommended that they are regularly reviewed by the responsible Technical Body to ensure that they remain valid.

- **Technical Report (ISO/TR):** A Technical Report (TR) contains information of a different kind from that of the previous two publications. It may include data obtained from a survey, for example, or from an informative report, or information of the perceived “state of the art”.

- **Publicly Available Specification (ISO/PAS):** A Publicly Available Specification is published to respond to an urgent market need, representing either the consensus of the experts within a working group, or a consensus in an organization external to ISO. As with Technical Specifications, Publicly Available Specifications are published for immediate use and also serve as a means to obtain feedback for an eventual transformation into an International Standard. Publicly Available Specifications have a maximum life of six years, after which they can be transformed into an International Standard or withdrawn.

- **Workshop Agreements (WA):** Thoroughly described in 8.6. (European case)

- **CEN/CENELEC Guides:** A Guide is a document that gives rules, orientation, advice or recommendations relating to European standardization. Guides are approved by a corporate body through a simple majority vote. Guides providing information or guidance on technical work shall be approved by the Technical Board, all others being approved by the General Assembly or Administrative Board.

- **ISO Guides:** Guides help readers understand more about the main areas where standards add value. Some Guides analyse how, and why, ISO standards can make it work better, safer, and more efficiently.

For the sake of completeness, the definitions of regulations and directives have also been included here.

- **Regulations:** A "regulation" is a binding legislative act. It must be applied in its entirety across the EU. For example, when the EU's regulation on ending roaming charges while traveling within the EU expired in 2022, the Parliament and the Council adopted a new regulation both to improve the clarity of the previous regulation and make sure a common approach on roaming charges is applied for another ten years.

- **Directives:** A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the EU single-use plastics directive, which reduces the impact of certain single-use plastics on the environment, for example by reducing or even banning the use of single-use plastics such as plates, straws and cups for beverages.

8.2.3 European and International Committees and Agencies

In this subsection, the main committees and unions that the project has participated or plans to participate in are described briefly. The main goal of the consortium remains the significant contribution to ongoing standardisation WGs or more general WGs that have multiple functions mainly in consulting and supporting EU member states or European organisations for specialized issues. More specifically, the aforementioned WGs can be summarized in the following bodies/agencies:

CEN: CEN is the European Committee for Standardization, an association that brings together the National Standardization Bodies of 34 European countries. It supports standardization activities in relation to a wide range of fields and sectors including air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

CENELEC: CENELEC is the European Committee for Electrotechnical Standardization, is an association that brings together the National Electrotechnical Committees of 34 European countries. It supports standardization activities in relation to a wide range of fields and sectors including: Electromagnetic compatibility, Accumulators, primary cells and primary batteries, Insulated wire and cable, Electrical equipment and apparatus, Electronic, electromechanical and electrotechnical supplies, Electric motors and transformers, Lighting equipment and electric lamps, Low Voltage electrical installations material, Electric vehicles railways, smart grid, smart metering, solar (photovoltaic) electricity systems, etc.

ETSI: ETSI is a European Standards Organization (ESO). It is the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. It has a special role in Europe. This includes supporting European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

ISO: ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 168 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant International Standards that support innovation and provide solutions to global challenges.

IEC: The IEC is a global, not-for-profit membership organization, whose work underpins quality infrastructure and international trade in electrical and electronic goods. Our work facilitates technical innovation, affordable infrastructure development, efficient and sustainable energy access, smart urbanization and transportation systems, climate change mitigation, and increases the safety of people and the environment. The IEC brings together more than 170 countries and provides a global, neutral and independent standardization platform to 20 000 experts globally. It administers 4 Conformity assessment systems whose members certify that devices, systems, installations, services and people work as required.

ENISA: The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

8.2.4 Standardisation ongoing efforts

In recent years, the European Union has shifted its focus to Defence and border Security. In pursuit of this objective, the Joint Communication to the European Parliament and the Council on the European Union Space Strategy for Security and Defence, published on 10th March 2023[1], identifies the critical technological domains. One of the key domains, as described in section 4, is the enhancement of the use of space for security and defence. Moreover, the EU Security Union Strategy[2] recognizes space infrastructure as an essential asset for anticipating threats and supporting resilience. Also, the EU and its Member States have developed a Strategic Compass[3] that provides the European Union with an ambitious plan of action for strengthening the EU's security and defence policy by 2030. All these initiatives will be substantially supported by the dedicated flagship programs Galileo, GOVSAT and Copernicus.

The space sector is currently experiencing a profound technological transformation characterized by the integration of onboard and on-site intelligence. Leveraging advanced AI techniques to process space-captured data holds the potential to enhance Earth Observation (EO) systems, rendering them more efficient, agile, autonomous, and adaptable. Achieving this goal necessitates a coordinated approach that addresses both software and hardware considerations, facilitating the development of a robust and efficient intelligence system tailored to Earth Observation applications. In addition, space capacities are an essential component for security-related policy objectives and can play a significant and pioneering role in defence by overcoming the limitations of traditional means. Therefore, the effort of standardization shall include several aspects, including the availability of different data sources, the need to ensure an adequate level of security of the infrastructure and services and the new technological developments as well as the long-term capacity of the private sector to continue delivering EUROMARS solutions.

In alignment with this strategic planning, the EURMARS project utilizes current assets and technology, identifies gaps and deficiencies and ultimately strives to establish crucial targets for this field within the EU.

More specifically, the EURMARS project constitutes a multidimensional and multifunctional border surveillance platform that integrates technologies and practices at various levels. As a result, the subjects of standardization that arise are numerous and pertain to different domains. These can be at a technological level, for instance, in the use of sensors that will be employed in the project, including coastal sensors, UAVs, high-altitude systems and satellite systems, navigation and AIS data, fast communication, at the level of systems architecture and assembly, and the functioning of different structural elements, at the level of information management and flow, as well as at the

[1] "European Union Space Strategy for Security and Defence", 10.3.2023 JOIN (2023) 9 final /JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL
[2] COM(2020) 605 final
[3] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

level of communication systems. Moreover, appropriate interfaces (APIs, graphical, or other user interfaces) will be developed for the purposes of the project, and this can act as a stepping stone to update an existing standard or create a new one. Another aspect that requires special attention and alignment with the needs of our era is the use of artificial intelligence, which plays a crucial role in several aspects of the project. For example, widespread utilization of artificial intelligence will occur in the sector of ship and oil spill detection through various sensors. This specific task falls within the general field of object recognition, and given the advancement of both artificial intelligence and sensor capabilities, it presents a fertile ground for standardization. Additionally, as stated previously, EUROMARS falls within the realm of security, defense, and protection of EU member states, and therefore, particular emphasis must be placed on how the project can substantially contribute to workgroups related to the safety and rescue of citizens living within the EU and those entering its borders. Last but not least, the information that will be stored and utilized on the platform will be sensitive and classified, underscoring the importance of cybersecurity as a top-priority issue to be ensured. The technological expertise employed in the project concerning cybersecurity matters can contribute to working groups focused on standardization or other entities with this subject matter.

Based on the above, Geosystems Hellas contacted the Greek NSB ELOT and requested the registration of the company's CEO as an expert in the field and also as a member of the EARSC[4] WG on Defence and Security and the ISO WG on the subject.

Downstream activities need to be addressed in a specific WG with clarified scope in order to:

- Federate experts, industries and operators in this domain
- Highlight and strengthen downstream activities in ISO/TC 20/SC 14
- Develop common international downstream standards to promote this market (which is also pulling the global Space market)
- Support large-scale deployment of space services and applications, including safety and critical ones (e.g., security and disaster management)

Lastly, it is worth mentioning that, according to the SIA State of Satellite Industry[5] report published in 2021, the market for downstream space services and space-based applications was approximately $240 billion in 2020, while the entire satellite industry was valued at $371 billion.

[4] https://earsc.org/
[5] https://brycetech.com/reports/report-documents/SIA_SSIR_2021.pdf

In conclusion, the consortium, through systematic efforts, should recognize the areas where it can make a greater and more substantial contribution, given the existing situation in the standards of the relevant fields with the project, and contribute maximally.

8.3 Regulations and Directives

Regulations and guidelines play an important role in the development and implementation of R&D projects, and should be an integral part of them to ensure their safety, quality, sustainability, and success. The issue of personal data is of high importance and is a priority for the European Union. Additionally, the EURMARS project is a comprehensive border monitoring system and therefore faces sensitive issues of immigration, search and rescue, and possibly managing human crises. Finally, cybersecurity is essential for the stable operation of any information system, especially when authorities and organizations of EU member states are involved.

To ensure that the project complies with the existing regulations and directives relevant to its characteristics and functions, and will continue to do so, we have included pertinent material in the same questionnaire that we used for standards and as we mentioned is part of Annex I.

8.4 Activity Plan

The activity plan adopted by the consortium aims to satisfy the two main requirements of Task 6.3 as described in the introductory section 2.1. Through discussions of the working package 6 meetings, as well as meetings dedicated to Task 6.3, with a primary focus on flexibility and effectiveness, the consortium decided to proceed based on the following steps.

In **the first step**, each contributor to Task 6.3 (ED, AIT, UREAD, VTT, BDI) was requested to designate a small number of eligible representatives for participation in standardization activities and processes. Below is a matrix illustrating the contributors' responses.

Table 5. Representatives of Task 6.3

Partner	Representative
GSH	Sofia Koukoura/ Vasiliki (Betty) Charalampopoulou

ED	Chris Antoniou/Alkiviadis Giannakoulias
AIT	Andreas Kriechbaum-Zabini
VTT	Laura Salmela
UREAD	Jonathan Boyle
BDI	Emil Ivanov

Table 5 contains the initial list of representatives and as the project develops more partners of the consortium may be engaged with standardisation activities.

The second step involved ensuring the project's compliance with existing standards, guidelines, and regulations at both international and European levels. For this purpose, all relevant standards from CEN/CENELEC and ISO were sought, as well as pertinent regulations and directives from the European Union that are applicable to the project. In summary, the tables containing the standards are included in Annex II and the related guidelines and regulations are included in Annex III. Significant effort was made to incorporate standards, regulations and guidelines that address all aspects of the project, with the aim of identifying potential gaps in standardization through this endeavour. The tables provided in the annexes will accompany the project throughout its duration and are subject to additions and modifications as per the project's needs and requirements.

The third step involved an exhaustive search of all active Working Groups within CEN, CENELEC and ISO**.** Subsequently, an investigation was conducted to determine whether the EURMARS project aligns with any ongoing standardization initiatives. This procedure adheres to established protocols and follows this sequence: Each designated representative identified in the first step (or an individual possessing specialized knowledge within their organization) is required to initiate contact with their respective National Standardization Body (NSB). For instance, Greece's Standardization Body is ELOT. Subsequently, they must adhere to the procedures prescribed by the relevant NSB. Typically, NSBs request a brief biography from the interested party. Upon approval by the NSB, the interested party gains access to the Working Group. The primary objective of participating in these groups is to contribute expertise that is currently in use or under development within the framework of the EURMARS project. The shortlist composed at the initial stage of this effort is below:

- CEN/CLC/JTC 5 - Space (especially WG3- Earth Observation)
- CEN/CLC/JTC 21 - Artificial Intelligence
- CEN/TC 287 - Geographic Information
- CEN/CLC/JTC 13 - Cybersecurity and Data Protection

- CEN/TC 391 - Societal and Citizen Security
- CEN/CLC/JTC 5/WG 2 - Space Situational Awareness Monitoring
- CLC/SR 80 - Maritime navigation and radiocommunication equipment and systems
- CEN/TC 239 - Rescue systems
- CEN/WS DIV - Requirements for acquiring digital information from victims during Search and Rescue operations.

The result of this effort is the participation of Geosystems Hellas in WG3 (Crisis management/civil protection) of the CEN Technical Committee 391 'Societal and Citizen Security' and in ISO/TC 20/SC 14 “Downstream space services and space-based applications”, following paragraph 1.7, ISO/IEC Directives Part 16.CEN Technical Committee 391 'Societal and Citizen Security': The initial communication with ELOT took place in March 2023 via email, including a general description of the EURMARS project, along with details about Task 6.3. Subsequent to this, several teleconferences were held with members of ELOT, including the director and employees of the Standardisation Department. These teleconferences aimed to clarify the entire procedure and organize the necessary steps. Furthermore, the scope of EURMARS was presented in detail, and all potential standardization opportunities were thoroughly discussed. The designated member to participate in this specific Working Group is Sofia Koukoura from GSH. In general, the main objective of CEN/TC 391 is to elaborate a family of European standards, standard-like documents (e.g., procedures, guidelines, best practices, minimal codes of practice and similar recommendations) in the Societal and Citizen Security sector including aspects of prevention, response, mitigation, continuity and recovery before, during and after a destabilising or disruptive event. Verification and training will also be considered.

The standardisation activities will consider the following main issues related to Societal and Citizen Security:

- Products and services (equipment, communication, information, goods, transport, energy, cultural inheritance and properties);
- Infrastructures (roads, ports, airports, rail stations, bridges, factories...);
- Stakeholder needs and requirements, potential conflicts;
- Relationship (cultural and geographical diversity);

[6] https://www.iso.org/directives-and-policies.html & https://www.iso.org/declaration-for-participants-in-iso-activities.html

- Citizen requirements and vulnerabilities, including privacy.

  More specifically, WG3 – Crisis Management/civil protection has the active project prEN ISO 22360 which examines the fact that crises conditions may manifest themselves throughout all elements of global society and significantly impact upon the goals and objectives of nations, regional and urban areas, communities, organizations (both public sector and private enterprise) and individual people. Crises may arise from failures to effectively manage security of assets, information, reputations or sovereign risks to governments or organizations or to provide safety and protection of members of society from personal injury, loss or harm.

  The issues of crisis management and civil protection are multi-layered, and their management requires the combination of knowledge, a plethora of solutions, and the collaboration of many parties. Therefore, EURMARS, through the multiple sensors it uses and the intelligent processing of these data through artificial intelligence, can significantly contribute to this field. Some examples are the timely detection and prediction of wildfires through satellite data. The identification of ships related to illegal migration has been a humanitarian crisis issue, especially in south-eastern Europe. The identification and prediction of the trajectory of oil spills to contain their impact and reduce environmental consequences.

- **ISO/TC 20/SC 14 "Downstream space services and space-based applications":** Since July 2023, the CEO of GEOSYSTEMS HELLAS has been actively engaged in exploring the scope of ISO/TC20/SC14/WG8. She has been in communication with Marie-Noëlle TOUZEAU, the Secretary, and Miguel Ortiz, the Convenor. Her efforts were supported ELOT's interest, leading to her appointment as the National expert. Also, a condition of the designation as an expert in the said working group is the creation or activation, at the national level, of a mirror standardization body / wider "circle" of interested parties related to the subject of the work of ISO/TC 20/SC 14. In this context, she registered as a Greek delegate and with her own contribution/cooperation, the actions for "investigation / mapping" of wider national/EU interest shall be launched. Currently, 27 members are registered on the ISO platform, 8 countries, and 1 liaison: France, Germany, India, Japan, Russia, United Kingdom, United States and Greece.

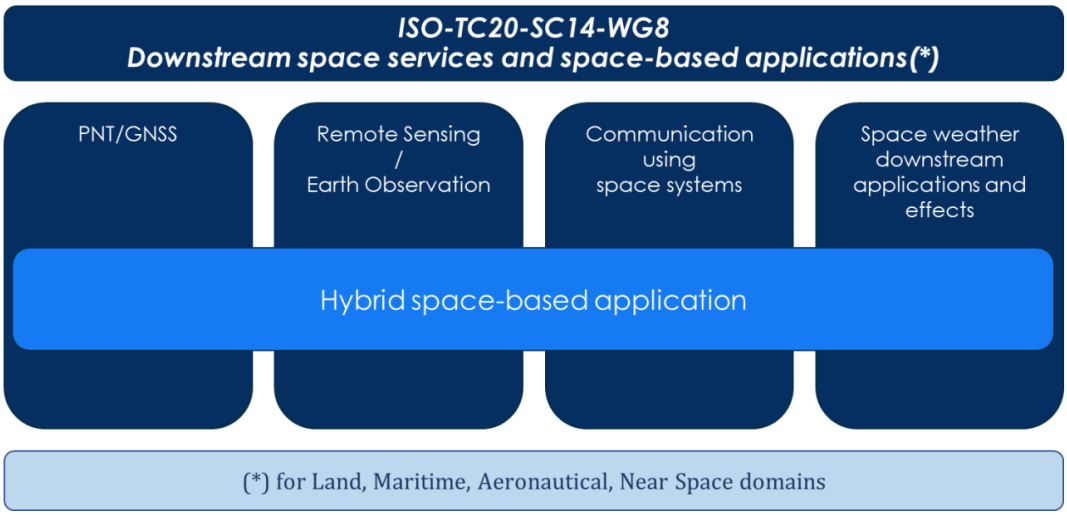

Figure 2. Overview of WG8 activities

Downstream space services consist of the following pillars:

- PNT/GNSS
- Remote Sensing / Earth Observation
- Communication using space systems
- Space weather downstream applications and effects

In the items mentioned above, communication using space systems encompasses a wide range of services, including mobile, fixed, internet access, digital broadcasting, IoT and more. Downstream space services and space-based applications need combination of expertise and therefore a need to develop “combinatorial standards” occurs. Effective collaboration with other entities is crucial, as it is essential for any standardization working group to be aware of other groups addressing similar topics. This awareness is vital to avoid redundant efforts and, even worse, the creation of conflicting standards. WG8 has taken the initiative to compile a list of potentially relevant working groups focusing on common areas. Among them, we have identified:

- ISO/TC 20/SC 13: Space data and information transfer systems
- ISO/TC 20/SC 16: Unmanned aircraft systems
- ISO/TC 204: Intelligent transport systems
- ISO/TC 211: Geographic information/Geomatics
- IEC/TC 80: Maritime navigation and radio communication equipment and systems

- ITU: Telecommunication

Considering that ISO's objective is the promotion of trade and the expansion of the world market, we align with this ISO objective in the field of standardization for downstream space services and space-based applications. The objective of standardization activity is to specify the definition of terminology, system performances, test procedures, characteristics of embedded equipment, products, data, signals, interfaces, securities, and safeties. From a high-level point of view, it is highly recommended that any WG8 standardization projects follow the following process before being sent to the SC14:

- Identification of a potential need. Any proposal for new work shall lie within the scope of WG8.
- Drafting and discussion of main ideas between WG8 experts and potential experts from other SDOs.
- Identification of a WG8 team that will carry the project; i.e. at least one project leader belonging to WG8.
- Once a first draft is ready for review: share this document with all WG8 experts.
- If no blocking point on the draft, then the project team can produce a reviewed and consolidated version for the official Form4 process.
- The project team has the responsibility to send Form 4 to SC14.
- This is highly recommended to share and agree on the resolutions of comments from ballots or consultations (NP, CD, DIS, FDIS), either during Spring/Fall meetings or by correspondence, before sending the update of the document to the Committee Manager.

Note: WG8 will use ISO Platform: ISO Documents, ISO Meetings, for global email distribution, management of meetings (calling notice, agenda, minutes), and management of Drafts and resolution of comments during Enquiry.

Moreover, ED participates in ENISA Ad Hoc Working Group on Security Operations Centres. The scope of this WG is to assist ENISA in capturing current practices across the EU regarding typical SOCs capabilities, i.e., capabilities to identify, protect against, detect, respond to and recover from cyber threats affecting a particular organisation. Our aim is to help the Agency capture current practices in CSIRTs and SOCs, Member States' cybersecurity policies and investment plans relevant to increasing the capacity of SOCs, identify gaps based on maturity models for SOCs that establish best practice (i.e., FIRST framework) and highlight pathways for research and innovation that will increase the maturity of current stakeholders in the field.

The fourth step is examining the potential to define a new Working Item (WI). According to the official definition of CEN\CENELEC, a new Working Item can be one of the following choices:

- A new project
- An amendment to the EN
- The revision of EN
- The conversion of TS into an EN
- The revision of TS
- The revision of TR

This is a more complex direction compared to the second one because a few parameters play an essential role. More specifically, the process of identification of a good methodology or practice that has the potential to be incorporated into a new Working Item depends strongly on the project's maturity level and the consensus among the partners.

8.5 Future steps

As the project reaches further maturity the strategy that has been adopted by the consortium is to establish a method to identify and record possible gaps towards the development of the different technologies or to pinpoint valuable methodologies and practices utilized during the project. After the first demonstration of the project, the Living Lab in Bulgaria, dedicated meetings will take place with high frequency in order for partners to conclude what has potential to constitute an interesting field of standardisation. The approach that very likely will be followed in order to address all the significant points/issues of the first demonstration-implementation of the system, includes the distribution of a questionnaire that will occur after the first discussions on the results of the Living Lab. Shortly after the end of the lab the consortium will try to identify and conclude to the most interesting and appropriate fields of technology-knowledge-science-etc. that have the potential to comprise the initial point of future standardization activities or contribute to similar groups of expertise like ENISA, as it was mentioned previously. Moreover, deficits observed by partners would be taken into consideration and analysed further in order to investigate if there is any potential for them to fulfil the Task 6.3 requirements. Once the consortium has reached a consensus on a specific item the process of submission for a new WI will begin. This process contains the completion of form 1 as it is attached in Annex IV.

For this purpose, GSH has contacted critical members of CEN in order to be prepared suitably for the submission of the form. More specifically, GSH has contacted the Greek Standardisation Body, the CCMC Programme Manager of the joint Technical Committee 5 (Space Technical Committee) and the secretariat of JTC 5. This TC covers all standardization activities in CEN and CENELEC related to space, including dual use aspects, systems of systems, as well as upstream and downstream applications, inasmuch as these topics are not covered by any other existing technical body in CEN or CENELEC or by the European Cooperation for Space Standardization (ECSS) or ETSI, therefore it is important and necessary that it coordinates its work with relevant technical bodies in ETSI. It develops European Standards that are needed to support the implementation of EU-level space projects. These communications led to the participation of GSH members (Vasiliki Charalampopoulou and Nikitas Georgakis) in their plenary meeting on 5th of July 2023, in which EURMARS project and possible standardisation items were presented. Through the discussion, it was concluded that the best options are the following:

- Joining the CEN/CLC/JTC 5/WG 6 – Upstream standards.
- Re-activate CEN/CLC/JTC 5/WG 3 – Earth Observation by defining a new WI. This group is devoted to analyse the “New Space” context with regard to standardization and propose, if necessary, evolutions in the actual set of ECSS requirements and associated Policies. The term “New Space” encompasses all the Space initiatives that revolutionize the commercial space field through the use of highly innovative solutions and processes, exotic business models, flat organisations, and low-cost space with another risks management approach.
- Defining a completely new WG in JTC 5.
- Active Participation at the 3rd SC14/WG8 Fall Meeting 2023 common place and week with WG1 BNAE, Issy-les-moulineau, France, 9th November 2023 & -4 th SC14/WG8 Spring Meeting 2024 Germany, date (TBD).

Furthermore, partners currently participating in WGs (TC391-WG3, WG8, and ENISA Ad Hoc Working Group on Security Operations Centres) will have a dual role. Firstly, they will contribute their knowledge and expertise from EURMARS to the WGs, and conversely, any valuable insights presented in these WGs will be attempted to be utilized by EURMARS through their advice and guidance. In this way, the dissemination and exchange of knowledge and experience to and from the project are achieved, thus ensuring the openness of the project, which is also a key requirement of Task 6.3.

8.6 CEN Workshop Agreement

Another option to be considered for future action is the pursuit of the CEN/CENELEC Workshop Agreement (CWA) which is the most widely used option for research and innovation projects. It is designed for them, due to the fast drafting and decision process. In theory, CWA can also be developed in a TC, but it is not usually the case. This entails establishing a novel working group, known as a Workshop, operating independently from the existing Technical Committees but maintaining coordination with them. The document undergoes approval directly from the Workshop members. Relevant Technical Committees are notified, and any organization is eligible to participate. The outcome of this process, known as Workshop Agreements, is published by the Standards Organizations and can be accessed freely by the public. However, it is essential that the content of these agreements does not contradict existing standards. If the scope of a Workshop Agreement falls under an existing Technical Committee, coordination with that committee is required. The process and criteria to develop a CEN/CENELEC Workshop Agreement (CWA) is summarised below.

1. A party interested in developing a CWA reaches out to a CEN Member or to CCMC. If CCMC is the first point of contact, it assists the Workshop Proposer in finding a CEN Member to take on the CEN Workshop Secretariat, following the process described in CEN-CENELEC Guide 29, clause 4.1.

2. With the assistance of the CEN Member, the Workshop Proposer of a CWA shall prepare the CEN Workshop Proposal Form. The form is then sent by the CEN Member to the CEN-CENELEC Director Standardization for allocation to a CCMC Project Manager (see CEN-CENELEC Guide 29, clause 4.2).

3. The Workshop Secretariat submits the CEN Workshop Proposal Form to relevant CEN and/or CENELEC Technical Committees (TCs), if any are identified in part A.2 of the form, for a 30-day consultation and to related CEN and/or CENELEC advisory and coordination groups, TC(s) use the same form to indicate if there is an active work item covering the scope of the proposed CWA and if there are any other arguments against the proposed CWA.

4.The CEN Workshop Proposal Form is submitted to the CEN Technical Board by the CCMC Project Manager for:

- Decision if the CWA:
  - addresses safety matters;
  - addresses management system aspects;
  - A TC identified as relevant in the proposal has voiced arguments against the proposed CWA (see 1.3 above).

- Information: In all other cases.

See also the summary of the consultation process of the launch of CWA.

5. The Workshop Secretariat and Workshop Proposer prepare the Workshop Draft Project Plan. If the consultation phase on the CEN Workshop Proposal Form is expected to take time (in particular if a CEN Technical Committee and/or CEN Technical Board consultation is needed), it is recommended to use this time to work on the Draft Project Plan. It is strongly recommended to define a dissemination strategy in the Draft Project Plan, to ensure the optimum impact for the future CWA.

6. CCMC announces the proposal for a new CEN Workshop (CEN/WS) on the CEN-CENELEC Website at least 30 days before the Kick-off Meeting. (See also guidance on WS announcement.)

The information posted on the website will include:

- the CEN/WS Draft Project Plan;
- initial information on the Kick-off Meeting (including Agenda and Venue);
- the WS Secretariat (and the proposed Workshop Chairperson - if known);
- how to submit comments to the Workshop Draft Project Plan.

Any comments submitted during this period shall be considered with the Workshop Secretariat and Workshop Proposer and in any case during the Kick-off Meeting at the latest.

7. During the Kick-off Meeting, the Workshop Secretary gives the participants information about the CEN/WS and the development process of the envisaged CWA, to help them understand how the CEN/WS will operate (see presentation template for generic information). The comments received on the Workshop Draft Project Plan are reviewed and the Final Workshop Project Plan is approved by those participants wishing to proceed. The formal launch of the CEN/WS happens at the Kick-off Meeting, provided there is sufficient support for the Workshop Project Plan. Participation to the Kick-off Meeting does not automatically ensure registration to the CEN/WS. After the Kick-off Meeting the participants wishing to continue contributing to the development of the draft CWAs will be requested to officially register to the CEN/WS by means of signing the registration form, therefore becoming CEN/WS participants.

8. The CEN/WS participants draft the CWA(s) according to the specifications laid down in the Final Workshop Project Plan. The draft CWA is made available for comments to the CEN/WS participants. To ensure transparency the documents of the CEN/WS should be uploaded on an electronic platform. If the CWA is in the same domain as an existing CEN/CENELEC Technical Committee, the Workshop Secretary is encouraged to follow the guidance on WS-TC communication, to ensure

proper exchange of information. In particular, whenever the draft CWA is sent to the CEN/WS participants for internal consultation, it shall be sent to that CEN/CENELEC Technical Committee for comments at the same time. In such cases, a commenting period of 30 days is recommended. Comments shall be sent to the Workshop Secretariat. These comments shall be considered by the CEN/WS participants. If foreseen in the Final Workshop Project Plan, and in any case if the draft CWA covers safety aspects, an open commenting phase (minimum 30 days and 60 days if it covers safety aspects) is launched. CCMC will make the draft CWA available for external comments on the CEN Website and the CEN-CENELEC Website. CCMC will also notify the CEN Members. In case of an open commenting phase, the Workshop Secretariat ensures the creation of a comments resolution report that compiles all the received comments. The comments are considered by the CEN/WS participants.

9. The WS Chairperson decides when agreement is reached amongst the WS participants on the final text of the CWA.

10. The Workshop secretariat submits the approved CWA to CCMC, with the cover page text and the European Forward (see Annex B of CEN-CENELEC Guide 29). CCMC ensures that:

the Cover Page and European Foreword are available and in line with Annex B of CEN-CENELEC Guide 29, a reference number is allocated to the CWA and added before circulating the published CWA to the CEN Members for announcement.

11. The Workshop secretariat shall inform any relevant TC of the publication of the CWA. At this stage, or at any later point in the CWA lifecycle, a TC can decide to take on the responsibility for the maintenance of the CWA. In this case, the TC Secretariat will conduct the consultation for the review of the CWA after 3 years.

12. A CWA is valid for 3 years, after which the former Workshop secretariat shall at least consult the former Workshop Chairperson and the relevant CEN/CENELEC Technical Committees, if any, and related CEN/CENELEC advisory and coordination groups, to determine whether the CWA shall be:

- confirmed for another 3 years,
- revised,
- withdrawn from the market.

The former Workshop Secretariat shall inform CCMC of the result of the query.

CWAs have a maximum lifetime of 6 years. After 6 years from initial publication, the CWA shall be submitted to the CEN (and CENELEC) BT(s) for decision regarding its transformation into another deliverable or its withdrawal, taking into consideration the recommendations from relevant CEN

(and CENELEC) Technical Body, if any, and related CEN/CENELEC Sector Fora, Focus Groups and Coordination Groups.

13. At any point in its lifecycle, a CWA can be transformed into another standardization deliverable (e.g., a TS or an EN), at the initiative of CEN Members or of a CEN and/or CENELEC Technical Body. This transformation shall be conducted according to the CEN-CENELEC Internal Regulations - Part 2.

14. Once the work described in its Project Plan is completed, the CEN/WS is disbanded (see also CEN-CENELEC Guide 29 Annex C: Overview of actions, responsibilities, and timeframes throughout the CEN/CENELEC Workshop Agreement process).

9 Dissemination and Communication Plan

The current section presents the Dissemination and Communication Plan (DCP) covering how the Dissemination and Communication Strategy (DCS) will be executed throughout the project's duration. A preliminary DCP version was developed and released at the early stage of the project M2 and the DCP for M12 is presented in the following sections. The current deliverable has 2 additional releases (M24, M36), with the production of the 3rd release of the deliverable, an updated and more robust DCP will be presented.

This DCP includes the following aspects:

- **What to disseminate/communicate and when**

  Sections 9.1 through 9.3 describe the executed and planned Dissemination and Communication (D&C) activities, including the channel(s) utilised, the estimated schedule and the responsible entities. The current DCP will act as the basis for evaluation of all D&C activities performed during the project's lifetime.

- **To whom to disseminate/communicate**

  Section 9.5 elaborates on the most significant stakeholder groups and target audiences.

- **How to disseminate/communicate**

  Section 9.4 presents an overview of the intended D&C channels to be used.

In this section, the preliminary DCP of activities is presented.

9.1 Dissemination Activities

Error! Reference source not found. shows a preliminary plan of the intended (preliminary) dissemination activities. This plan will be the guideline, and basis for evaluation, for all dissemination and communication activities during the project lifetime.

Table 6. Preliminary Dissemination Plan Details

Activity	Schedule	Responsibility
Exhibition stands in	**M1-M18:** Participate in at least 2 external industry events	Coordination: HSE, ED

Activity	Schedule	Responsibility
industry events/fairs	**M19-M36:** Participate in at least 3 external industry events	Contribution: All Partners
Scientific publications (in highly ranked international journals, and magazines and international peer-reviewed conferences, under open access principles)	**M1-M18:** 2 publications in international journals and magazines (possibly in the pre-publication pipeline, due to the short time available until M18), 2 publications in international conferences **M19-M36:** 13 publications in international journals and magazines, 6 publications in international conferences (in addition to the above)	Coordination: ED Publications by: ED, HSE Contribution: All Partners
Thematic Workshops	**M1-M18:** Organise at least 1 workshop to engage specific audiences and promote specific aspects of the project (preferably within the scope of larger international events to promote wider discussion with stakeholders) **M19-M36:** Organise at least 3 workshops to engage specific audiences and promote specific aspects of the project (preferably within the scope of larger international events to promote wider discussion with stakeholders)	Coordination: HSE, ED, Contribution: All Partners
Cluster with related European projects and other initiatives	**M1-M18:** Participate in at least 8 clustering events with related projects or initiatives **M19-M36:** Participate in at least 12 clustering events with related projects or initiatives	Coordination: ED Contribution: All Partners
Meetings with policymakers and regulators	**M1-M18:** Participate in at least 3 meetings with policymakers or regulators **M19-M36:** Participate in at least 3 meetings with policymakers or regulators	Coordination: ED Contribution: All Partners

Activity	Schedule	Responsibility
Industrial "Showcase" (for stakeholders' engagement and demonstration of the EURMARS Framework)	**M30-M36** Organise and implement a large-scale demonstration event of the integrated EURMARS Framework based specifically on stakeholders' engagement	Coordination: ED Contribution: All Partners

9.2 Dissemination Activities Details

This section elaborates on the core dissemination activities envisioned during the execution of EURMARS's DCP focusing on the first year of the project.

9.2.1 Dissemination and Communication Survey

Throughout this stage of DCP, we designed a ANNEX VI: Dissemination and Communication Survey and collected responses online. By carefully examining and consolidating the data, we drew meaningful conclusions and updated our initial plan accordingly. In this section, we present the results, offering a clear overview of the key insights and trends that emerged from the gathered responses.

9.2.1.1 Survey Results

- In general, the outcomes of the survey align with our expectations, as the established communication channels for the project (project website, Twitter, LinkedIn) have proven to be the most frequently utilized and preferred by all partners involved.
- Based on the survey results, a minimal number of partners (3 responses) utilize a digital newsletter as their regular communication channel, while none of the respondents reported using a printed newsletter. Consequently, these findings indicate that neither a digital nor a printed newsletter of the partners would be an effective communication tool for EURMARS-related activities.

- The only worrying discovery from the survey is the limited intention or experience by some partners to produce research publications. The partners that intent to publish academic journals should have in mind that there may be partners needing assistance in documenting and disseminating research results.

- Based on the votes received, here is a short summary of the target audience groups for the EURMARS project, arranged in descending order of importance:

    1. Border security/management and coast guard agencies,
    2. Member States/ministries/government departments,
    3. Law enforcement agencies/intelligence agencies,
    4. Technology/service providers, investors,
    5. Scientific R&D institutions,
    6. Regulators and policy-makers,
    7. Data providers/Data service providers,
    8. Media,
    9. Citizens,
    10. Standardization bodies.

  Please note that these rankings are based on the votes provided, and the importance of each audience group may vary depending on the specific objectives and context of the EURMARS project.

- The partners viewpoints regarding which communication channels/tools should receive the greatest attention in EURMARS are consistent with the existing communication channels of the EURMARS Project.

9.2.2 Scientific Publications

When project results and achievements are made, consortium members will be urged to publish findings in highly ranked international journals and magazines and international peer-reviewed conferences. The EURMARS consortium will abide by the publication guidelines outlined in the GA to enable open access to its scientific publications either by submitting them to Open Research

Europe or ensuring open access from an established document repository with scientific content (e.g., Zenodo - https://zenodo.org/).

The project's results (by WP) which are most suitable and promising to generate the various scientific publications envisioned in the project's DCP (minimum 15 journal and 8 conference publications) are the following:

- WP3: Coastal Ground and Low Altitude Sensing Systems, High Altitude Sensing Systems, Satellite Based Systems, Digital Interfaces and Integration of Existing Infrastructures, Multimodal Data Fusion
- WP4: Collaborative C2, Visualization & Alarming, Risk Assessment Framework, Decision Support System
- WP5: Evaluation, Benchmarking & Lessons Learned
- WP6: Standardisation Activities, Industrial Showcase

In the following the most relevant scientific journals and conferences, to be preferably addressed by publications in the context of EURMARS, are listed:

9.2.2.1 AI Related Scientific Journals

- Foundations and Trends in Machine Learning
- Journal of Artificial Intelligence Research
- IEEE Transactions on Pattern Analysis and Machine Learning
- IEEE Transactions on Neural Networks and Learning Systems
- International Journal of Information Management
- IEEE Transactions on Fuzzy Systems
- IEEE Computational Intelligence Magazine
- Synthesis Lectures on Artificial Intelligence and Machine Learning
- Journal of the ACM
- Neural Networks
- ACM Transactions on Intelligent Systems and Technology

- IEEE Transactions on Cognitive Communications and Networking

9.2.2.2 Security Related Scientific Journals

- Journal of Global Security Studies
- International Journal of Information Security
- EURASIP Journal on Information Security
- European Journal of Criminology
- European Journal on Criminal Policy and Research
- International Journal for Crime, Justice and Social Democracy

9.2.2.3 AI Related International Scientific Conferences

- AIAM - International Conference on Artificial Intelligence and Advanced Manufacturing
- International Conference on Machine Learning
- International Conference on Learning Representations
- AAAI Conference on Artificial Intelligence
- International Joint Conference on Artificial Intelligence (IJCAI)
- International Conference on Artificial Intelligence and Statistics

9.2.2.4 Security International Scientific Conferences

- Information Security Conference
- Infosecurity Europe Conference
- European Crime Prevention Conference
- ISS World MEA
- IEEE International Conferences on Intelligence and Security Informatics (ISI)

9.2.3 Cluster With Related European Projects and Other Initiatives

In respect to the coordination with similar projects and liaison with European initiatives, the following relevant dissemination actions are envisioned and planned within the EURMARS framework of actions.

9.2.3.1 Clustering With Other Research Projects in the Field

Clustering with relevant EU security projects and Intra-project dissemination is an essential and important tool for improving collaboration between researchers within Europe. The EURMARS project will establish connections not only with currently running EU research projects that focus on the same application area, but also with related EU research or scientific programs. It will create relationships and investigate potential common interests, along with similar and/or different approaches that could act in a complementary way.

These connections will facilitate the exchange of views and information with other EU researchers, focusing on common approaches or activities of interest and to jointly raising awareness concerning the related aspects. This interaction can help reduce replications of research in multiple projects while leveraging activities and joint forces in respect to effective knowledge dissemination and especially assisting exploitation of the project result by policy makers. The clustering activities with other related EU projects will enable the consortium partners to discuss and present the project-related matters, fostering cooperation with other researchers in the field, providing expert feedback, and enabling stakeholder interaction. A catalogue of research projects similar to EURMARS that could provide collaboration opportunities are listed in Table 7.

Table 7. Research Projects Similar to EURMARS

Acronym	Title	Start Date	End Date	Website
MEDEA	The Mediterranean & Black Sea Security Practitioners' Network	1/06/2018	31/05/2023	https://www.medea-project.eu/
CALLISTO	Copernicus Artificial Intelligence Services and data fusion with other distributed data sources and processing at the edge to support DIAS and HPC infrastructures	1/01/2021	31/12/2023	https://callisto-h2020.eu/project/
AI-ARC	Artificial Intelligence based Virtual Control Room for the Arctic	1/09/2021	29/02/2024	https://ai-arc.eu/
EFFECTOR	An End to end Interoperability Framework For MaritimE Situational Awareness at StrategiC and TacTical OpeRations	1/10/2020	30/09/2022	https://www.effector-project.eu/

Acronym	Title	Start Date	End Date	Website
NESTOR	aN Enhanced pre-frontier intelligence picture to Safeguard The EurOpean boRders	1/12/2021	30/04/2023	https://nestor-project.eu/

Since these projects are ongoing or running in their final stage, the EURMARS project will exploit their outcomes and current research to foster collaboration and leverage its own research results, exchanging methods and information. EURMARS will reach the projects mentioned above by establishing contacts through their coordinator, sending focused emails, and promoting the EURMARS website and social media. Joint Press releases and newsletters and co-organization of workshops will also be pursued.

9.2.3.2 Participation in Clustering Events organized by EC, Research Initiatives, or Security Organisations:

External clustering events are an ideal space to disseminate the activities of the EURMARS project. During these events, cooperation between related EU projects can be fostered, leading to synergies and collaboration. Besides bringing together coordinators and partners from similar projects, these events can also offer the following:

- To promote research carried out in the projects, forge new links and networks, and identify the appropriate partners for possible future research collaborations
- To meet and exchange information with the representatives of the related projects but also with the Clustering Events' Organizers
- To inform them about the tools that are being developed in the EURMARS project and policy issues that have been identified
- To engage the involved attendees in a dialogue about the utilization of the technologies being developed by EURMARS in terms of needed technology and legal framework improvements
- To encourage them to raise awareness concerning the EURMARS project and consider the adoption of the project system, methods, and technologies within new research frameworks
- To get feedback on needs, requirements, or possible offers by the involved attendees, along with contacting other participants representing other sectors (i.e., industrial / technology partners, other end users, etc.)

To this respect, the EURMARS project intends to actively participate in the relevant clustering events with research projects organized by the following:

- The Directorate-General of Migration and Home affairs (DG HOME)
- The Joint Research Center Initiative (DG-JRC) of the European Commission

Among others, the above Initiatives aim to manage EU external borders in a more efficient and modern way by using new and innovative technologies, exploring next-generation technologies, using new, more effective tools to improve personnel performance, and better use public authorities' resources.

9.2.4 Exhibition Stands in Industry Events/Fairs

The EURMARS consortium intends to participate in key national and international events and conferences relevant to the project's scope and domain and participation by the project and consortium partners will be highlighted through each entity's communication channels. The objectives of such activities include the presentation of the project in these fora and platforms with intention to raise awareness, disseminate project outcomes and liaise with other relevant organisations and stakeholders. Ideally, the connections and interactions with the entities reached at these industry events will continue engaging in a reciprocal update on the respective activities through the project's lifetime.

An indicative list of industry events suitable for disseminating EURMARS activities and results is presented below:

- Security Research Event (https://home-affairs.ec.europa.eu/policies/internal-security/innovation-and-security-research/security-research-event_en)
- eu-LISA Annual Conference (https://www.eulisaconference.eu/)
- Berlin Security Conference (https://www.euro-defence.eu/)
- International Conference on Border Security and Protection (https://waset.org/border-security-and-protection-conference)
- Global Aviation Security Symposium Events (https://www.icao.int/Meetings/AVSEC2022/Pages/default.aspx)
- World Border Security Congress (https://world-border-congress.com)
- FRONTEX Border Control Conferences and Events ((https://frontex.europa.eu/future-of-border-control/research-and-innovation/announcements)
- Border Security (https://www.smgconferences.com/defence/uk/border-security)

- The Official UK Government Global Security Event (https://www.securityandpolicing.co.uk/)
- European Police Congress (https://www.european-police.eu/)
- Maritime Reconnaissance and Surveillance Technology (https://www.smgconferences.com/defence/uk/conference/Maritime-Reconnaissance)

9.2.5 Meetings with Policymakers and Regulators

The consortium aims to perform dissemination efforts in close collaboration with various stakeholders and especially policymakers and regulators. A core objective is to involve policymakers through bilateral cooperation workflows into the shaping of EURMARS's secure multitasking surveillance platform to ensure that their impact on the development of the framework and tools is acknowledged. In addition, EURMARS has the ambition to improve applicable regulations by exposing policymakers and regulators to the EURMARS results constituting currently unidentified outlooks into European legislation for improved maritime surveillance and international public authority collaboration.

Indicative policymakers and regulators to potentially seek collaboration with include:

- European Commission
- European Parliament
- Council of the European Union
- European Court of Justice

9.2.6 Thematic Workshops

Thematic Workshop activities are significant activities aiming to engage specific audiences and promote specific aspects of the project. To organise and perform them, requires on behalf of the project to have made significant progress and obtain tangible outcomes to showcase. At this point, an entire national or international event can be built around the findings and results of the project and the experiences partners can share on the domain. This practically imposes the execution of even the first event of this kind between M12 and M18.

It should be noted that there are 2 different options/opportunities to consider. The first option entails the organisation of the workshops within the scope of larger international events to promote wider awareness and interaction with industry stakeholders, initiatives and policymakers. The other option is to incorporate workshops into living lab activities and the various specialised events like

exercises, pilots, etc. In this context, the workshop would not only present the technologies developed but also disseminate the full extent of the innovation achieved by EURMARS, while the drawback of this approach would be the more limited audience compared to the previous option.

9.3 Communication Activities

In Table 8 the preliminary plan of the intended communication channels and related activities is described.

Table 8. Preliminary Dissemination-Communication Plan (DCP) Details

Channel/Activity	Schedule	Responsibility
Project Website	**M1-M2:** Design, development, and deployment of the first version of the project's website	HSE
	M3-M6: Review and update website structure/static content. Establish newsletter subscription and visitor tracking mechanisms. Include appropriate public ethical compliance, privacy, and data protection policies disclaimers	Coordination: HSE Contribution: All Partners
	M3-M36: Regular update of the website content	
Social Media	**M1-M2:** Establish the project's presence on LinkedIn and Twitter	HSE
	M3-M6: Explore potential suitability of additional social media to extent online presence	Coordination: HSE Contribution: All Partners
	M3-M36: Post project updates and news to online communities (optionally engage in discussions and exchanges)	

Channel/Activity	Schedule	Responsibility
Brochure	**M1-M32:** Produce and distribute project brochures in both electronic and printed formats (at events, workshops, meetings etc) providing overview of the project, its challenges and expected impacts	Coordination: HSE Contribution: All Partners (Optionally, partners will adapt selected brochures to national context for each different country/language in the project)
Poster/ Banner	**M1-M32:** Design project banners providing overview of the project its challenges and expected impacts for use/exhibition at events, workshops, and meetings as well as at partners' premises	Coordination: HSE Contribution: All Partners (Optionally, partners will adapt selected poster/banner to national context for each different country/language in the project)
Project Presentation	**M1-M3:** Produce project presentation including basic information about the project (activities, objectives, partnerships, events) **M4-M32:** Update and/or create additional versions of the project presentation to meet project's communication needs	Coordination: HSE Contribution: All Partners (Optionally, partners will adapt the presentation to national context for each different country/language in the project)
Trial videos	**M1-M32:** Produce and distribute via all available communication channels a set of videos presenting the EURMARS platform scope, pilot use cases as well as the tested and evaluated technologies	Coordination: HSE Contribution: All Partners
Infographics	**M1-M32:** Design a series of infographics to depict the project details and results in a clear and simple manner	Coordination: HSE Contribution: All Partners
Final Publishable Report	**M31-M36:** Produce report with the tangible results of the project, lessons learnt, and impacts achieved	Coordination: ED Contribution: All Partners

Channel/Activity	Schedule	Responsibility
Articles	**M1-M18:** Compose, at least, 2 articles or conduct interviews for publication in electronic or printed media focused on EURMARS related AI topics, technology advancements, security practitioners' methods and demonstration results	Coordination: HSE Contribution: All Partners
	M19-M36: Compose, at least, 3 articles or conduct interviews for publication in electronic or printed media focused on EURMARS related AI topics, technology advancements, security practitioners' methods and demonstration results	
Newsletters	**M1-M6:** Produce and circulate the 1st EURMARS newsletter issue	Editor: HSE Contributors: All Partners (All partners will provide potential contacts to send it. Anyone interested can subscribe through website)
	M7-M12: Produce and circulate the 2nd EURMARS newsletter issue	
	M13-M18: Produce and circulate the 3rd EURMARS newsletter issue	
	M19-M24: Produce and circulate the 4th EURMARS newsletter issue	
	M25-M30: Produce and circulate the 5th EURMARS newsletter issue	
	M31-M36: Produce and circulate the 6th EURMARS newsletter issue	
Press releases	**M1-M18:** At least 1 International (European) press releases about the project	Editors: HSE, ED Design/Templating: HSE Contributors: All Partners (Moreover, partners may adapt the press releases to national context and transmit to local media for each different country in the project)
	M19-M36: At least 1 International (European) press releases about the project	

Channel/Activity	Schedule	Responsibility
Talks in workshops	**M1-M36:** Communicate the project activities and results in workshops and international events when invited	Coordination: ED
Market Uptake Launch-Event	**M31-M36:** Organise and hold at least one Market Uptake Launch-Event of selected project's result(s)	Coordination: ED Contributors: All Partners

9.4 Communication Channels Details

This section elaborates on the core communication channels to be exploited during the execution of EURMARS's DCP focusing on the first year of the project.

9.4.1 Website

The project's website was developed in 2 phases. During the first phase, from M1 to M2, the initial website design was developed, and the basic content was included in the first version of the website which was lunched at the end of M2.

The second phase of the project's website development which is also the current, was executed from M3 to M6. During the second phase, the following activities were performed:

- Reviewed and updated the website structure/static content with the collaboration and involvement of all partners.
- Established newsletter subscription.
- Established visitor tracking mechanisms.
- Included appropriate public ethical compliance, privacy, and data protection policy disclaimers.
- Established a blog/articles section to accommodate articles focusing on specific project topics and aspects curated by various consortium partners.

The structure of the website's current version is depicted in

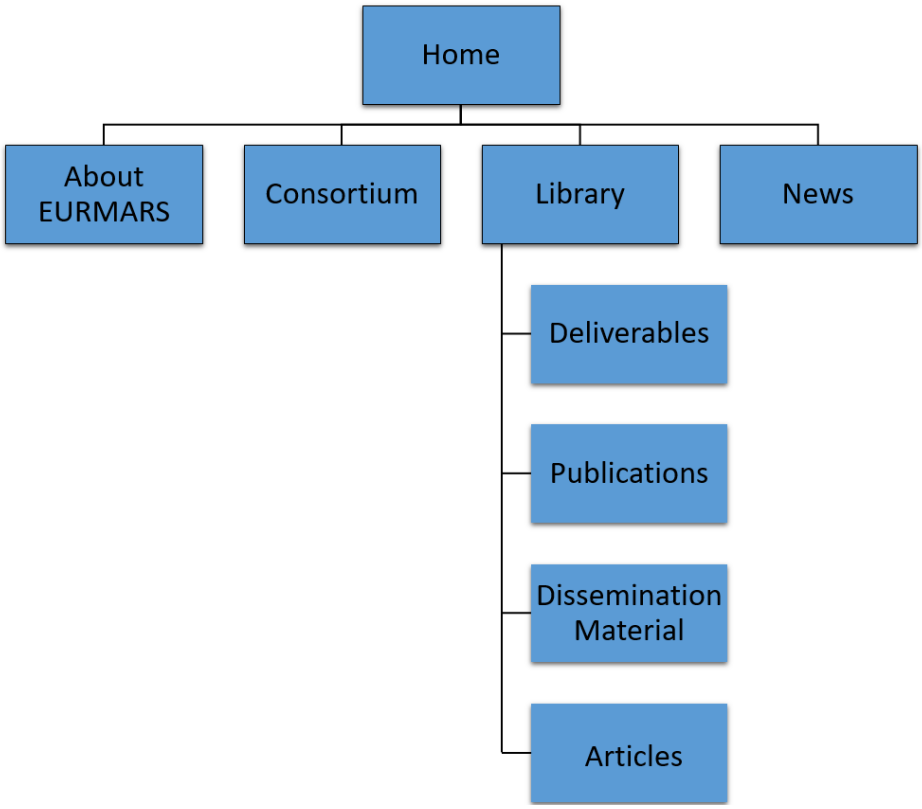

Figure 3. Sitemap of the Second phase of EURMARS Website

The website's homepage is presented in Fig. 4. The website is the main tool for dissemination and communication of the project activities continuously and publicly. This feature provides to all project participants, individuals or organisations, the option to redirect inquiries about the project to this information repository independently of their project-internal authorisation level and/or knowledge of the entire project's specificalities.

The website is registered and can be accessed under the following domain name:

eurmars-project.eu

The project website is expected to be live on the internet for at least three years after the end of the EURMARS project. It will constitute the project's main communication channel for online dissemination and communication while the additional channels presented in the next sections below will serve as amplifiers to the project's messages.

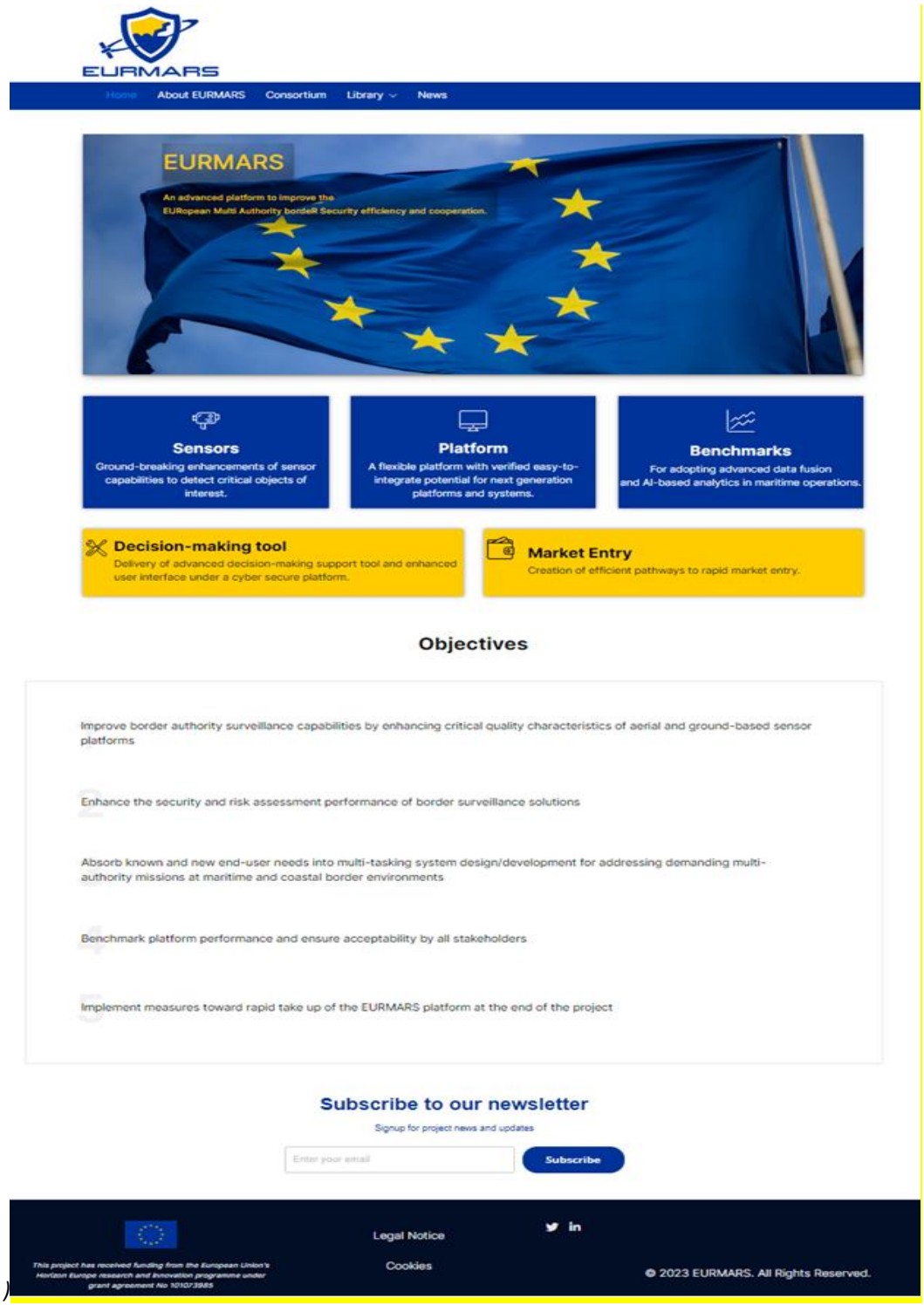

Figure 4. The Homepage of EURMARS Website (June 2023)

9.4.2 Social Media

The EURMARS social media presence is established to the most business-oriented social media channels, namely LinkedIn and Twitter. The intention is to have an open approach and share the project's achievements with the public through these channels, in order to inform, communicate and raise awareness around EURMARS activities.

In the first two months of the project (M2) the following social media channels have been launched:

LinkedIn	https://linkedin.com/company/eurmars-horizoneu
Twitter	https://twitter.com/EURMARS_Project

9.4.2.1 LinkedIn

With the EURMARS LinkedIn-page, the most professional and business-oriented target audiences will be covered and involved. The specific platform is ideal for disseminating, particularly at the later stages of the project, achievements and results of exploitational nature and enhance the objectives of the project's exploitation plan.

The project's LinkedIn homepage is depicted in Fig. 5.

9.4.2.2 Twitter

In addition to LinkedIn, a EURMARS Twitter account was also created. With Twitter, the motivation is the reach of all types of audiences but also at the same time focus in networking and exchange of points of view with industrial and European related initiatives, experts and professionals, public and business organisations and entities.

The project's Twitter homepage is depicted in Fig. 6.

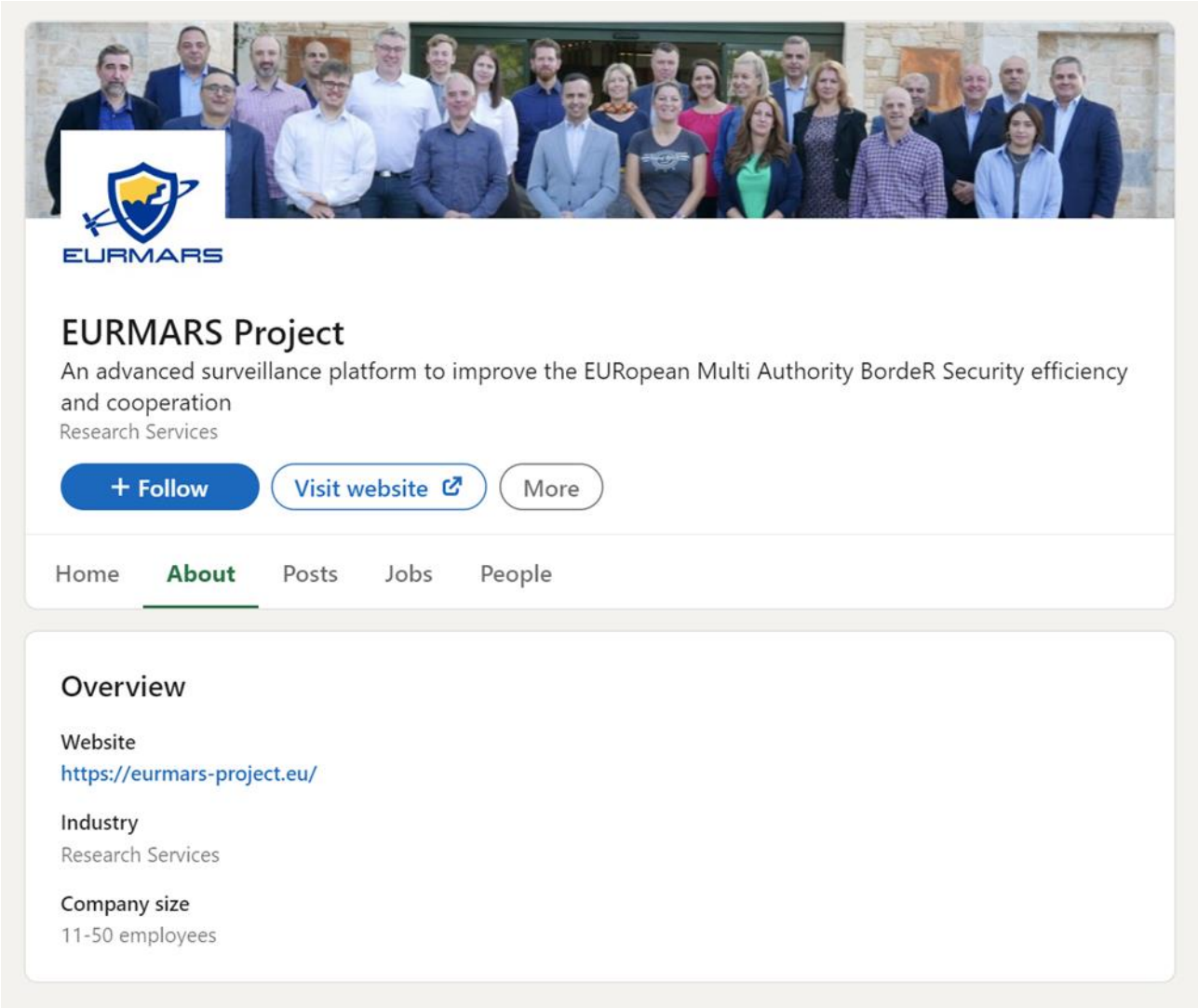

Figure 5. EURMARS LinkedIn Page (June 2023)

Figure 6. EURMARS Twitter Page (June 2023)

9.4.3 Press Releases

As already indicated in Table 8, HSE and ED are responsible for the coordination of communication via press channels and will prepare templates and the general press releases, which will be used by the other partners for the issuing of press releases on a national level.

Fig. 7 shows the workflow and the responsibilities for this process.

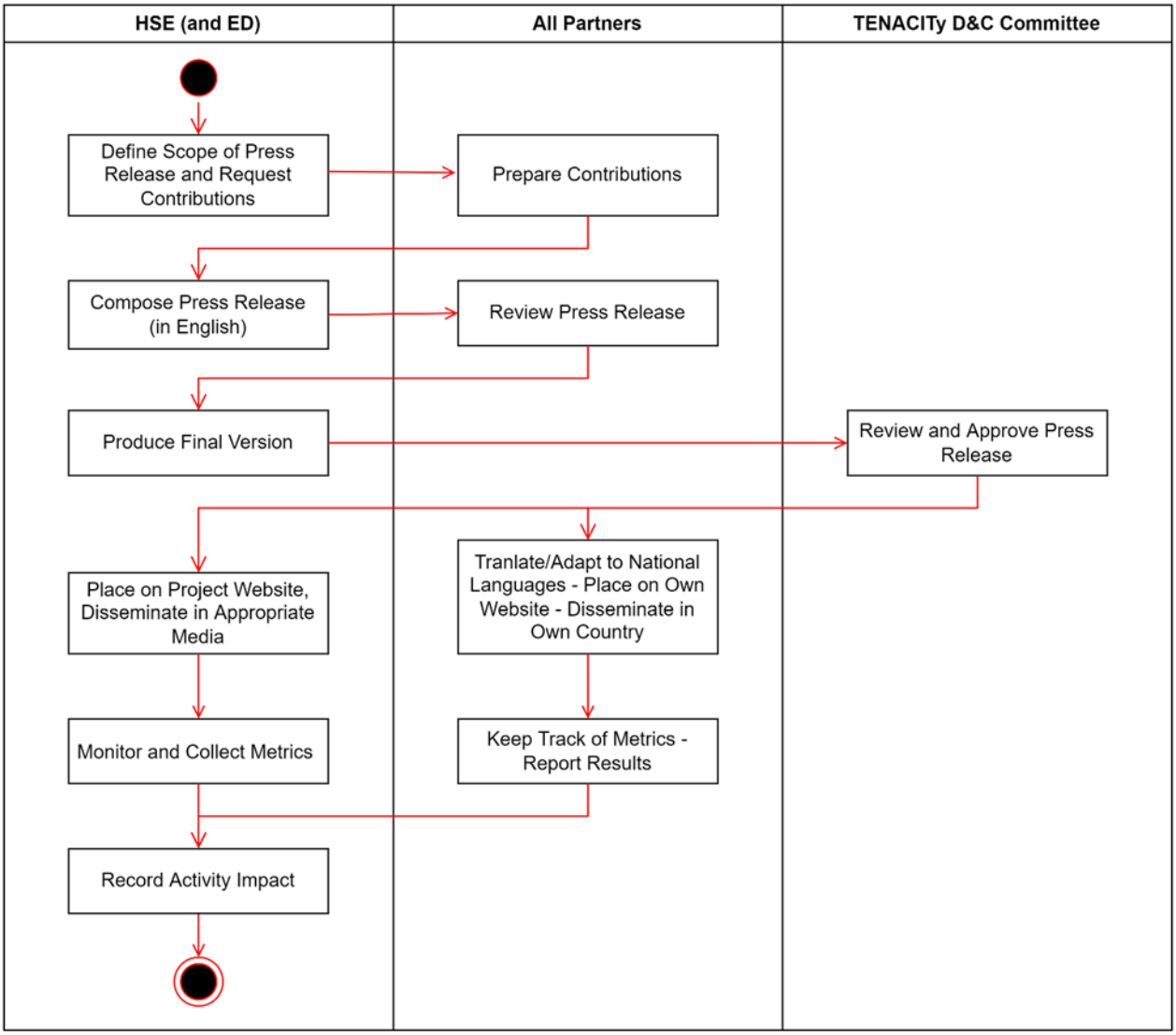

Figure 7. Workflow for Producing Press Releases

9.4.4 Newsletters

In EURMARS, as indicated in Table 8, a project newsletter will be generated twice a year to engage and update subscribers of important news and advances the project is making. The development of the newsletter will be based on the same workflow that is used for the creation of the press releases, as detailed in the previous section. The EURMARS newsletter will be sent to all recipients who opted-in via the dedicated form on the EURMARS website.

The intention is to utilise a dedicated commercial platform like MailerLite (https://www.mailerlite.com/) that can cover all the related requirements and at the same time makes the process of subscribing and unsubscribing to the newsletter very easy and automatic (without additional steps and/or monitoring on behalf of the consortium).

By creating interactive newsletters that are linked to posts and articles on the project's website and social media, the stakeholders' awareness of the project activities is increased, and the project's communication channels are enhancing their interactions and therefore the visibility of the project and its results.

9.4.5 Articles

EURMARS aims to share findings and achievements through articles and/or interviews in third party media, like websites, newspapers, magazines and external newsletters. This communication may comprise original content created for this use, or it may involve re-purposed materials from other EURMARS communication channels. It will focus on specific project topics and aspects of interest at the time period of publication (EURMARS related AI topics, technology advancements, security practitioners' methods and/or demonstration results). Contributions for the production of these articles are expected from all partners involved in work related to the main theme of the article and the overall process will be based on the workflow used for the creation of the press releases detailed in section 9.4.3. Publication in third party media promotes EURMARS and makes its standpoints accessible to a broader audience while promoting the consortium in the public sphere and the special audiences these media address.

9.4.6 Additional Communication Instruments

In addition to the communication channels analysed the previous sections, the following ones are envisioned to be part of the EURMARS DCP as specified in Table 8.

- Discussions in Workshops
- Market Uptake Launch-Event
- Final Publishable Report

Regarding discussions in non-EURMARS organised workshops, the objective is to communicate the project activities and results in workshops and international events when invited. These after-invitation discussions will depend on the project's awareness built in the sector by the overall DCP activities performed and their impact. All related events will be documented in the future releases of the deliverable.

The Market Uptake Launch-Event and the Final Publishable Report are communication instruments that, according to the current DCP, will be organised and developed at the last semester of the project, therefore details about them will be documented in the third release of this deliverable (M24).

9.5 Audiences

The dissemination activities are expected to ensure that the project's advancements are widely diffused to the intended targeted audiences with appropriate mechanisms in a timely manner, and that the key stakeholders for the project's exploitation and market uptake are early engaged and actively participating to the various project's implementation phases. The project's Consortium aims to implement an intensive, yet clear, strategy and conduct effective dissemination, communication, and exploitation activities from the very early stages of the project's implementation. An initial list of the target groups for EURMARS is depicted in Table 9.

Table 9. Initial List of EURMARS target groups.

Technology/ Service Providers, Investors	They are considered as a critical target group for the exploitation of the project results. Their continued interest and investment in order to deploy the EURMARS results will greatly boost the project's exploitation opportunities. EURMARS offers them increased business opportunities focused on developing safety and security services, related to the project's integration, analysis and collaboration technologies.
Member States/ Ministries/Government Departments	They are a key target group for EURMARS dissemination and exploitation, to encourage approval and take-up of EURMARS technological outputs, as the recipients of the policy and regulation recommendations EURMARS will produce, especially where identifying possible weaknesses and gaps in legislation, policy and operational cooperation, and, overall, for the adoption of the EURMARS secure multitasking surveillance platform.
Regulators And Policy-Makers	
Citizens	They need to be provided with evidence that their personal data are being handled in a secure way, in order to gain their trust and confidence, thereby promoting behaviours which contribute to European safety and security. An important focus will be on communicating about the use of novel technologies that respect fundamental rights, both in

	terms of the right to privacy, as well as with regard to potential consequences (right to non-discrimination, etc.).

9.6 Best Practices and Guidelines

The following is a preliminary set of best practices and guidelines for all partners to adhere to throughout the project's D&C activities:

- Acknowledge EU funding as specified by the European Commission[7] and in the project's grant agreement.
- Use the developed EURMARS file templates for all project-related documentation of activities.
- All partners should use the EURMARS mailing lists for general communication and specifically to inform other partners of the availability of new dissemination material and results.
- All partners should support the implementation of EURMARS's DCP as defined in this deliverable and its next releases.
- All D&C activities should be approved by the EURMARS's D&C Committee, so planning and execution of specific activities should take into consideration the time and effort required by the D&C Committee to process related requests.
- All partners should document and update D&C activities to the online file shared for tracking D&C activities as soon as the activity has been concluded. In addition, a reminder will be scheduled to be sent at the end of each month to all partners to fill in the list with their D&C activities.
- Each partner to create at least one entry in each individual communication channels (website, social media etc.) mentioning the participation in EURMARS, including the EURMARS logo and website domain name or link to it.
- All partners should participate in the consortium's communication efforts, by sending to the D&C leader any news that are pertinent to the project's scope and can be potentially transmitted through the project's communication channels. This includes news about

[7] Communicating about your EU-funded project, European Commission. Accessed October 21, 2022, URL: https://rea.ec.europa.eu/communicating-about-your-eu-funded-project_en .

partner's involvement in events and conferences, publications, news about other similar or relevant projects, or news stories that are relatable to the work performed in EURMARS.

- Posts referencing the project on Twitter, should include the @EURMARSProject mention and the hashtag #EURMARSProject.
- Posts referencing the project on LinkedIn, should include the @EURMARSProject mention and the hashtag #EURMARSProject.
- EURMARS-related communications to external entities should include the EURMARS's project website domain name and approved contact information.

This set of practices and guidelines is not static but may be updated if necessary. All the appropriate steps will be taken to ensure that these directives are relevant and respected during the project's lifetime.

9.7 Project Identity Material

This section presents the current status of development of the project's identity material. These identity elements will ensure a coherent and easily recognisable presence to all target audiences and stakeholders.

9.7.1 Colour Scheme

To develop a visual identity the first action entails the adoption of the colours, namely the colour scheme, to adopt in all key visual elements of communication. Once established, the actual identity material can be developed utilising the adopted colour scheme. For EURMARS's project identity the adopted colour scheme is depicted in Figure 8. EURMARS Colour

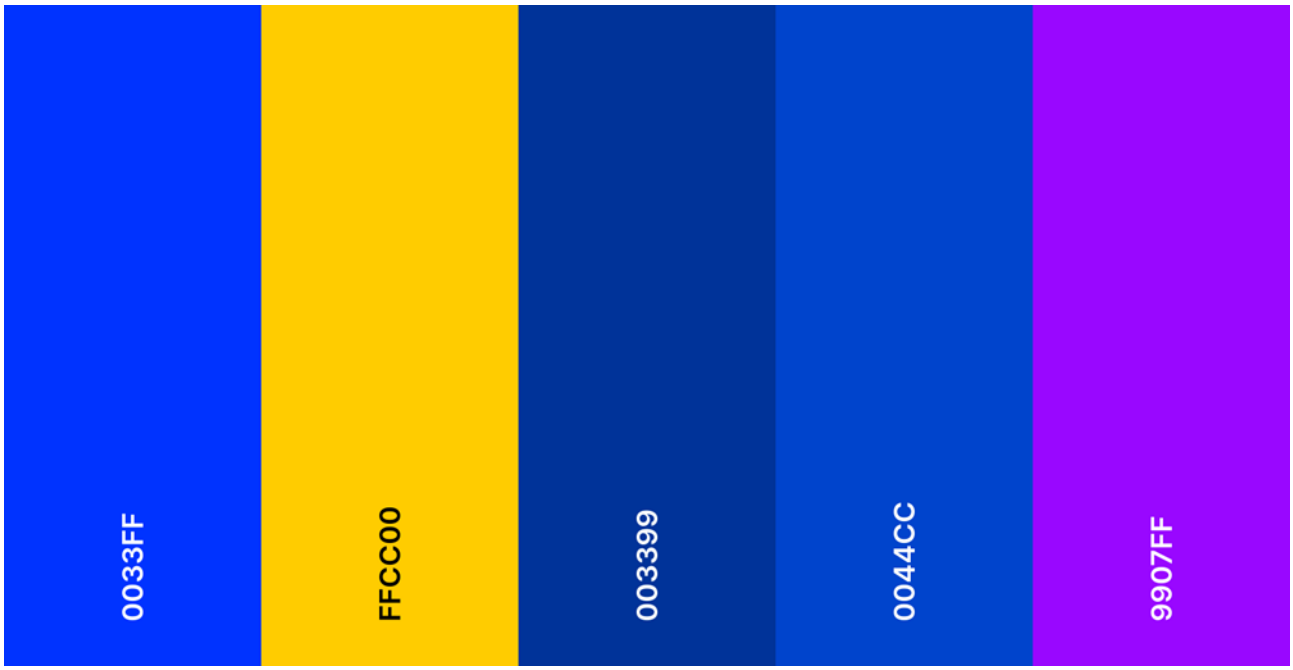

Figure 8. EURMARS Colour Palette

9.7.2 Project Logo

The consortium agreed to the logo through a process providing 4 different alternative ideas/creations and putting these alternatives for voting within the consortium in an online poll. The logo that has received more than 50% of the votes in the poll and selected to be EURMARS's logo is depicted in Fig. 9.

Figure 9. The EURMARS Logo

The logo design includes the project's acronym, is quite simple and subtle indicating, at the same time, key elements of the project's scope. Moreover, the graphic element at the left of the acronym can be used as an icon in specific environments/uses.

Figure 10. The EURMARS Icon

9.7.3 File Templates

The consortium has, both internally and externally, specific communication requirements through electronic documents that can be printed if necessitated. Currently, the following templates have been identified as required to incorporate the project's visual identity for supporting internal and external communications:

- Deliverable Template (in Microsoft Word format)
- Presentation Template (in Microsoft PowerPoint format)
- Meeting Agenda Template (in Microsoft Word format)
- Minutes of Meeting Template (in Microsoft Word format)

These templates integrate the project's logo, the colour scheme for the various elements in them and the EU flag alongside the funding disclaimer with the grant id. The objective is to succeed in establishing a consistent project identity as well as awareness and recognition among external stakeholders, EU bodies and the general public. Selected samples are depicted Fig. 11 and Fig. 12.

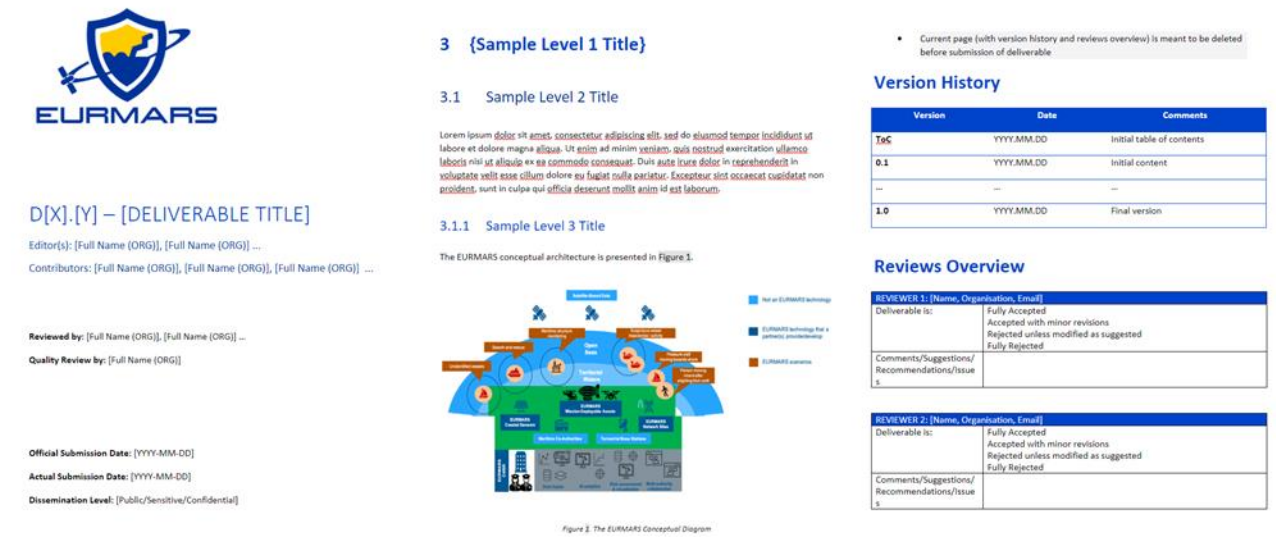

Figure 11. Sample Pages of the EURMARS Deliverable Template

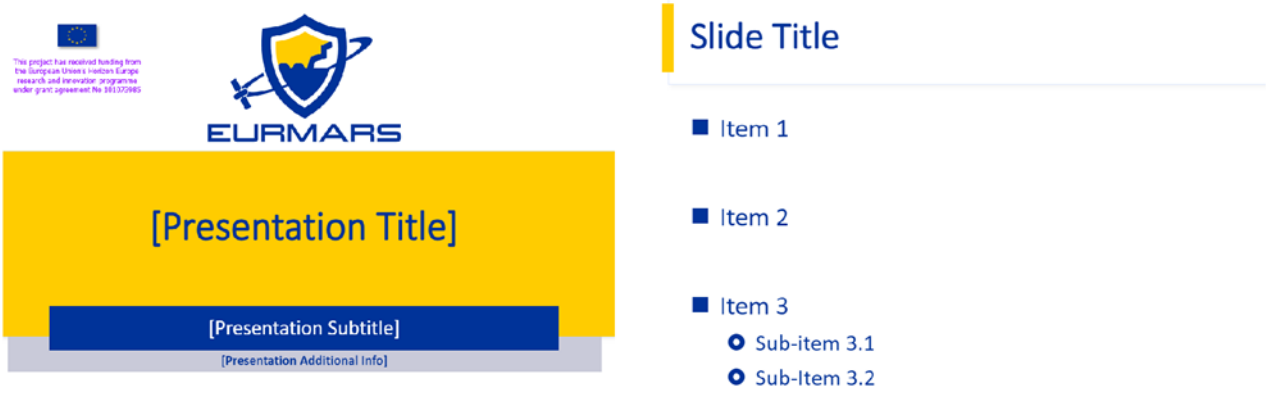

Figure 12. Sample Slides of the EURMARS Presentation Template

9.7.4 Project Presentation

The project's scope, aim and objectives, as well as an overview of what EURMARS plans to develop, demonstrate and evaluate will be included in the core EURMARS project presentation. According to the devised DCP detailed in Table 8, the project presentation should be available to all partners at the end of M3. It constitutes the basic tools for presenting and communicating the project scope in a uniform and coherent manner by any particular partner and any general-purpose situation.

As the project's activities progress, the core project presentation will be updated when necessary. This is foreseen at least towards the end of the project, where the results attained should be

incorporated into a format that can be used by the partners to narrate the project's success stories and outcomes.

Additionally, the EURMARS project presentation may be adapted and/or translated by partners to meet their individual demands for different situations and contexts (e.g. national vs European events, meetings etc).

9.7.5 Additional Material

Besides the aforementioned D&C material in the previous sections, additional material will be created as foreseen in the DoA:

- Brochure(s)
- Poster(s)/ Banner(s)
- Trial videos
- Infographics

This material will be created at specific points in the project's lifetime either when certain project milestones have been reached or when partners or the whole consortium participate in particular events (workshops, industry events, presentations of publications etc.). At this stage of the project the dissemination material that has been designed and developed to align with the specific requirements of the events in which the project actively participated are presented in the following figures.

Figure 13. EURMARS Brochure

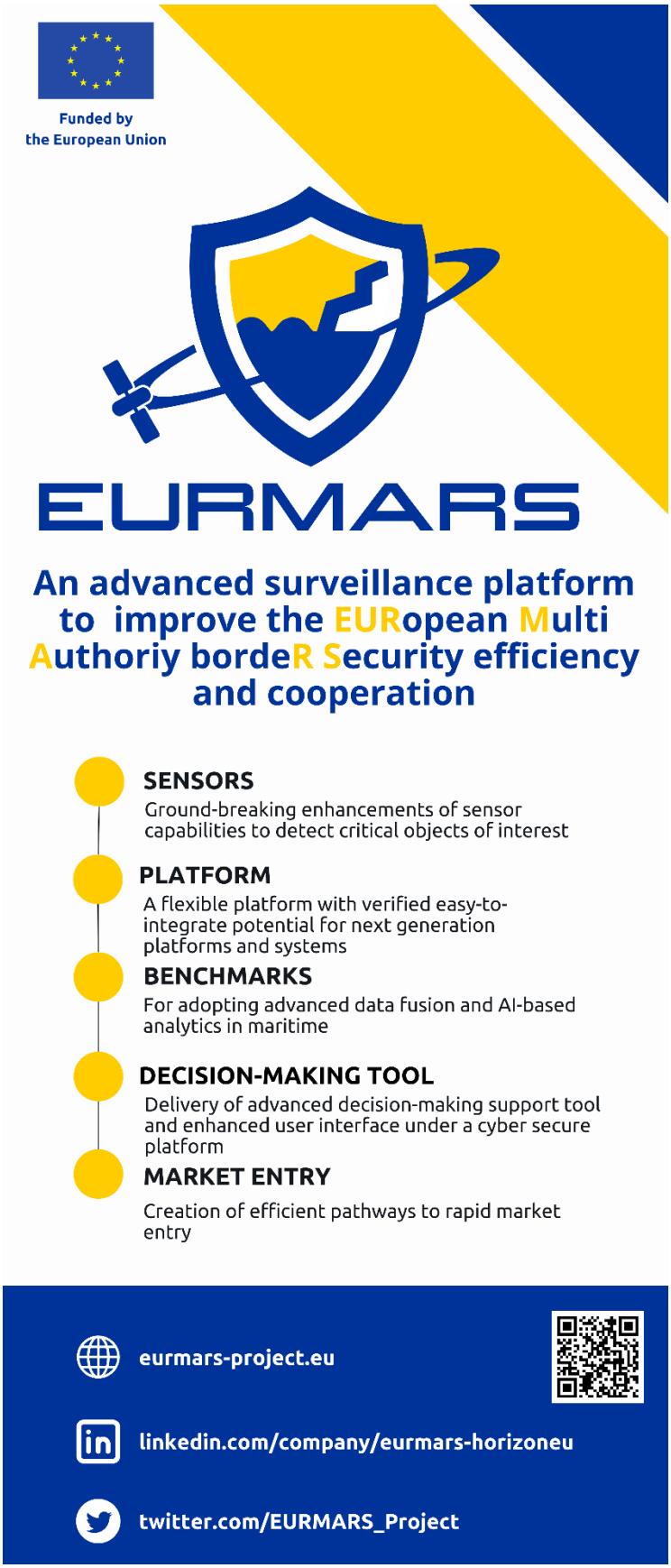

Figure 14. EUMARS Banner

9.8 Monitoring and Performance Evaluation

In order to assess the consortium's D&C performance and to take corrective actions if/when necessary, all D&C efforts will be continuously monitored and evaluated during the project's lifespan. The foundation for the evaluation is provided by the definition of KPIs related to the D&C activities.

There will be 4 versions of the deliverable and probably 3 different versions of the DCP (M2, M12 and M24 if required) thus a qualitative and quantitative evaluation using these indicators will be performed at the next 3 releases of the deliverable. Depending on the performance of EURMARS's DCP the KPIs may be updated and/or adjusted in the next versions.

9.8.1 Objectives

Table 10 presents the quantified targets of the EURMARS project's main dissemination activities as outlined in the DoA. The current schedule for achieving these targets is presented in the current (preliminary) DCP and specifically in **Error! Reference source not found.** 8.

Table 10. KPI target values of the dissemination activities within the project lifespan

Dissemination Activity	KPIs Target
Exhibition Stands in The Industry Innovation Events/Fairs	**> 5**
Publication In Highly Ranked International Journals and Magazines	**> 15**
Contributions In International Peer-Reviewed Conferences	**> 8**
Organisation Of Thematic Workshops	**>= 4**
Cluster With European Projects and Other Initiatives	**> 20**
Targeted Meetings with Policy Makers	**> 6**
Industrial "Showcase" for stakeholders' engagement and demonstration of the EURMARS Framework	**= 1**

Error! Reference source not found. presents the quantified targets of EURMARS main communication channels and related activities as outlined in the DoA. The current schedule for achieving these targets is presented in the current (preliminary) DCP and specifically in Table 8.

Table 11. KPI target values of the communication channels and related activities within the project lifespan

Communication Channel/Activity	KPIs Target
Project website	**1 (Frequently updated)**
Social media	**> 50**
Brochures	**8**
Posters/Banners	**> 4**
Institutional Presentation	**1**
Trial videos	**>= 4**
Infographics	**6**
Final Publishable Report	**1**
Articles	**>= 5**
Newsletters	**> 4, periodical**
Press releases	**>= 2**
Talks in workshops	**On invite**
Market Uptake Launch-Event	**>= 1**

The KPIs for the main communication channels (website, social media) are quite general at this stage. For the next version of the deliverable and consequently the DCP, the related KPIs may be redesigned and adjusted based also on the performance observed of these communication channels in the time between M2 and M12.

9.8.2 Monitoring

All D&C actions and efforts accomplished within the project's context are recorded in a dedicated online form, where partners can document their D&C activities as soon as they are concluded. This form serves not only for activity tracking and reporting but also enables the real-time performance evaluation of the DCP.

Acronym	Title	Relevance to TENACITy	Project Reference (Grant id)	Topic	Start Date [YYYY-MM-DD]	End Date [YYYY-MM-DD]	Website

Figure 15. Form for recording/monitoring/evaluation EURMARS's dissemination and communication activities

For each activity the following information is recorded:

- Partner (Acronym),
- Type of Activity
- Date of activity (in the form: [YYYY.MM.DD])
- Description of Activity (location, title of event, the main content of the message, etc.)
- Country/Region
- Language
- Evidence Kept/URL (if applicable)
- Audience Type
- Estimated Persons Reached (after 1 month – if available)
- Additional information

9.8.3 Evaluation

The achievement of quantified targets stated in 9.8.1 can guarantee the effectiveness of our dissemination and communication strategies and plans. Moreover, other factors can be considered during assessment, as indicated below:

- **Website**
  The evaluation of the website will be carried out using a cookie-less analytics plugin which will provide us mainly information about the total number of visitors, average visitors, number of unique visitors thought the lifetime of the project website.

- **Social Media**
  Social Media channels performance can be measured quantitatively by the numbers of:

  - Followers

- Clicks
- Interactions
- Retweets
- Comments etc.

At this stage of the project all the partners have been followed on the social media profiles they provided in the ANNEX VI: Dissemination and Communication Survey and the dissemination and communication activities are recorded to the Figure 15. Form for recording/monitoring/evaluation EURMARS's dissemination and communication activities that has been shared throughout the partners.

- **Newsletter**
  The newsletter evaluation will be monitored through the MailerLite dashboard which provides additional information about the newsletter such as number of subscribers, newsletter opens and clicks.

- **General guideline of Dissemination and Communication evaluation**
  During our project meetings, we engage in a comprehensive evaluation of our dissemination and communication performance as a consortium. We reflect upon our past activities and strategize for future endeavors. The following questions guide our discussions:

  - Has our overall dissemination and communication strategy been faithfully implemented?
  - What tasks and activities are still outstanding?
  - What are the next steps we need to take?
  - Who bears the responsibility for upcoming project components?
  - Have we met our previous deadlines?
  - Are our activities progressing as planned to meet upcoming deadlines?
  - Have our dissemination efforts aligned with the vision and objectives of EURMARS, as outlined in our dissemination and communication strategy?

Table 12 presents the targets of the dissemination and communication activities of the project and their current status:

Table 12. Current Status of DCP

Dissemination and Communication Activities	KPI	Target	Progress
Project Website	Increase Total Visitors	1000/ year	1060 Visitors / 1st year
Twitter	Increasing Followers Numbers	30%/ year	18 Followers / 1st year
	Number of Posts	>50	7 Posts
LinkedIn	Increasing Followers Numbers	30%/year	48 Followers / 1st year
	Number of Posts	>50	7 Posts
Poster/Banner	Number of Posters/Banners	>4	Figure 14. EUMARS Banner
Brochure	Number of Brochures	8	Figure 13. EURMARS Brochure
Project Presentation	1 Project Presentation/ Updated when necessary	1	Produced project presentation including basic information about the project
Press release	Issues a press release	>=2	
Talks in workshops		On Invite	
Trial Videos	Number of Trial Videos	>=4	No Trial Videos published yet
Infographics	Number of Infographics	6	No infographics published yet
Articles	Number of Articles	>=5	Articles are currently under development, with partners actively contributing based on their assigned tasks and deliverables.
Newsletter	Issue newsletter about progress of the project	>4,periodical	Sent the 1st issue of the EURMARS Newsletter
	Subscribers	200	20 subscribers

Dissemination and Communication Activities	KPI	Target	Progress
Exhibition stands in industry events/fairs	Number of exhibition stands in industry events/fairs	>5	n/a
Scientific publications (in highly ranked international journals, and magazines and international peer-reviewed conferences, under open access principles)	Number of Publications	>15	n/a
Thematic Workshops	Number of Workshops	>=4	n/a
Cluster with related European projects and other initiatives	Number of clusters with related European projects and other initiatives	>20	n/a
Meetings with policymakers and regulators	Number of meetings with Policy Makers	>6	

In evaluating the performance of EURMARS, it has come to our attention that certain Key Performance Indicators (KPIs) have not been met, specifically concerning the number of followers on our Social Media Channels, namely Twitter and LinkedIn, and the frequency of published posts on these platforms.

To address this situation and align with the required KPIs, we have devised a comprehensive plan. Firstly, we intend to enhance our social media presence by increasing the frequency of posts to a

weekly or biweekly schedule on our established channels. This measure aims to engage our audience more consistently and stimulate higher levels of interaction and interest.

Furthermore, we are committed to boosting our outreach efforts through collaboration with the responsible teams for dissemination and communication within each partner organization. Our overarching objective is to fortify the online visibility and engagement of EURMARS, thereby cultivating a larger and more active community. This undertaking will not only enhance our KPI performance but also enable us to foster stronger connections with our stakeholders and disseminate our mission more effectively.

10 Conclusions

This deliverable intends to serve as a foundational element for the next two out of its three releases. Simultaneously, its purpose is to spread the accomplishments within the project while outlining future planning and actions. More specifically, its objective is to establish clear exploitation plans, not only for the project as a whole architecture but also for its individual sub-components, thereby leading to the formulation of distinct exploitation strategies.

Furthermore, with regard to the project's standardization aspect, special attention was dedicated during the first year to ensure the project's alignment with pertinent standards, regulations, and directives. This effort was undertaken to enhance efficiency, reliability, consistency and sustainability.

Furthermore, there was active participation in standardization groups, with the goal of contributing EURMARS solutions, workflows, practices, and procedures to relevant standardization projects. Additionally, this involvement aimed to maintain project’s receptivity to scientific or practical knowledge associated with these groups, which could be valuable for integration into EURMARS.

Lastly, the Dissemination and Communication plan provides the EURMARS project with a robust framework, roadmap, and toolkit essential for effectively disseminating project results and activities.

11 References

[1] CEN-CENELEC Guide 29
https://boss.cen.eu/media/Guides/CEN-CLC/cenclcguide29.pdf

[2] ISO 3166-1:2020 Codes for the representation of names of countries and their subdivisions — Part 1: Country code

[3] ISO 8601-1:2019 Date and time — Representations for information interchange — Part 1: Basic rules

[4] ISO 13537:2010 Space data and information transfer systems — Reference architecture for space data systems

[5] ISO 19161-1:2020 Geographic information — Geodetic references — Part 1: international terrestrial reference systems (ITRS)

[6] CCSDS 311.0-M-1 Reference Architecture for Space Data Systems, https://public.ccsds.org/Pubs/311x0m1.pdf, Retrieved on 2023-01-04

[7] CCSDS 312.0-G-1 Reference Architecture for Space Information Management, https://public.ccsds.org/Pubs/312x0g1.pdf, Retrieved on 2023-01-04

[8] CCSDS 351.0-M-1 Security Architecture for Space Data System, https://public.ccsds.org/Pubs/351x0m1.pdf, Retrieved on 2023-01-04

[9] CCSDS 371.0-G-1 Application and Support Layer Architecture, https://cwe.ccsds.org/sea/docs/SEA-SA/Draft%20Documents/App%20-%20Support%20Layer%20Green%20Book/ASL%20ADD%20Review%20inputs%20-%20resolutions/371x0g0_CESG_Approval.pdf, Retrieved on 2023-01-04

[10] ISO/IEC 80000-1:2022 Quantities and units — General

ANNEX I: Structure of Technical Committees

In this section, a brief overview of the structure of the organisations and agencies mentioned in 8.2.3 is given. The role of this section is to give a clear image of the organization chart and to clarify the roles of every member.

CEN/CENELEC:

- Technical Board (BT)
  - Composition
    - Chairperson: CEN Vice-President Technical
    - Chairperson of the BT Technical Committee Management Group (TCMG)
    - Secretariat: CCMC
    - Membership: one representative per country
    - Observers: ANEC, ECOS, SBS, ETUC, European Commission…
  - Working
    - By correspondence (4 weeks)
    - Meetings/year: 2 CEN/BT meetings + 3 TCMG meetings
  - Responsibilities
    - Advises and decides on technical matters (organization, procedures coordination, overlaps and planning)
    - Examines and decides on new projects (New Work Items (NWIs))
    - Imposing and releasing the standstill obligations
    - Undertakes any task with regard to technical work as may be requested by the General Assembly or the Administrative Board
    - 'Management by exception' principle
- Technical Committee
  - Responsibilities

- Established by CEN/BT
- Precise title and scope
- Responsible for drafting deliverables
- Support CCMC during the negotiations on standardization request
- Timely execution of standardization request deliverables

- Composition
  - Chairperson and Secretary
  - National Delegations (national position, voting right)
  - European Partners (observers, no voting right)
- Chairperson
  - Neutral
  - Appointed by CEN/BT (delegated decision)
  - Presides meetings and manages consensus
  - Interface with CCMC (strategic directions, specific issues, external relationships, …)
  - Ensures coordination and info exchange with other committees
- Secretary
  - Appointed by CEN member holding the secretariat of TC
  - Ensures that TC works efficiently and agreed timetables are kept
  - Prepares and distributes documents (agenda, reports, decisions, etc.)
  - Manages documents distribution via Livelinkplatform
  - Is aware of CEN/BT decisions related to technical work and reacts on any question raised by the Technical Board or other competent CEN body in relation to his/her assigned CEN/TC
  - Ensures coordination and info exchange with other committees

- Liaises with CEN-CENELEC Management Centre
- In case of Standardization Requests, he/she is responsible for preparing reports

- Working Groups (WGs)
  - Working Group(s)
    - Established by the Technical Committee
    - Short term task (prepare first drafts of EN/TS/TR)
    - Individual experts
  - Working Group Convenor
    - Seeks support from the parent body (if needed)
    - Ensures that WG experts know rules and procedures
    - Responsible for sending drafts to TC
    - Actively progresses work and reports regularly to TC

Below there are two figures related to the structure of the TCs of CEN/CENELC. Fig. 16 depicts the decision layers in the Technical Committees and the second depicts the composition of a TC. All collaborations with organizations, teams, individual experts or any other entities are governed by Regulation 25, as shown in Fig. 17.

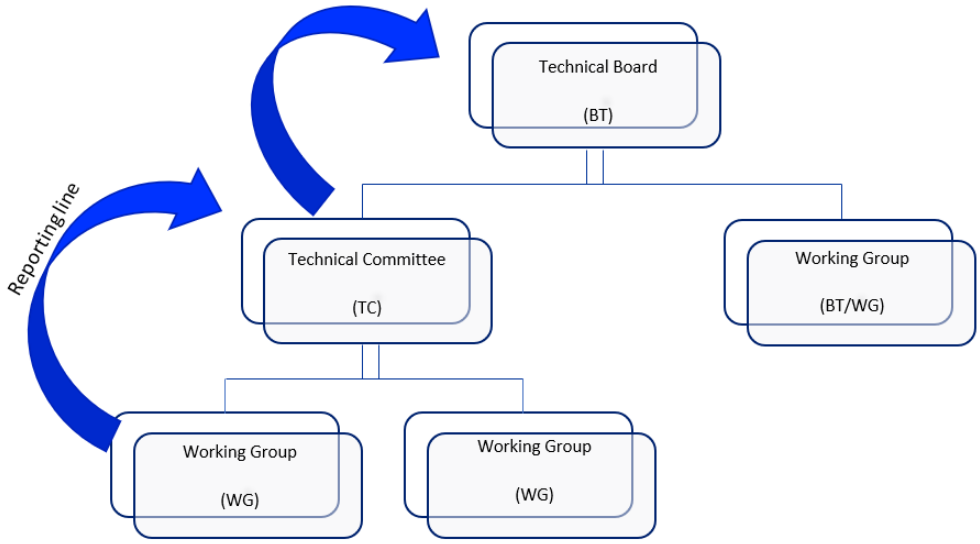

Figure 16. The three-decision layers at technical level

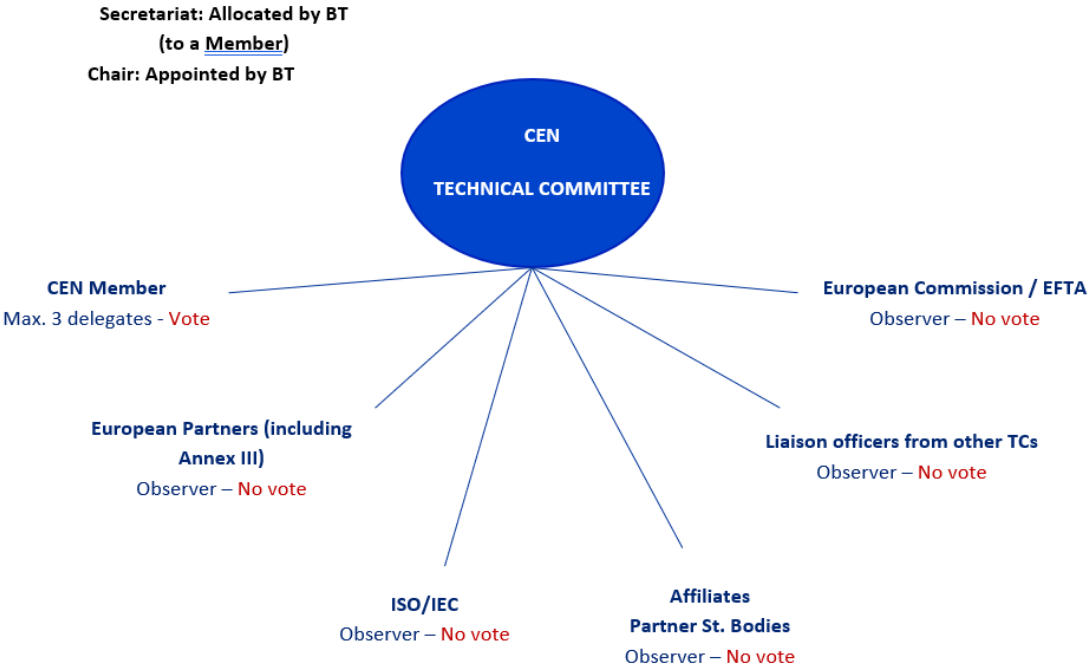

Figure 17. Technical Committee - Composition

ISO:

- The General Assembly: The General Assembly is the overarching organ and ultimate authority of the organization. It is an annual meeting attended by our members and our Principal Officers.

- The ISO Council: The ISO Council is the core governance body of the organization and reports to the General Assembly. It meets three times a year and is made up of 20 member bodies, the ISO Officers and the Chairs of the Policy Development Committees CASCO, COPOLCO and DEVCO. The Council has direct responsibility over a number of bodies reporting to Council:

  - The President's Committee advises Council on matters decided by Council.

  - Council Standing Committees address matters related to finance (CSC/FIN), strategy and policy (CSC/SP), nominations for governance positions (CSC/NOM), and have oversight over the organization's governance practices (CSC/OVE).

  - Advisory groups provide advice on matters related to ISO's commercial policy (CPAG) and information technology (ITSAG).

  - CASCO provides guidance on conformity assessment.

  - COPOLCO provides guidance on consumer issues.

  - DEVCO provides guidance on matters related to developing countries.

Membership to the Council is open to all member bodies and rotates to make sure it is representative of the members community.

- Technical Management Board (TMB): The management of the technical work is taken care of by the Technical Management Board, which reports to Council. This body is also responsible for the technical committees that lead standards development and any strategic advisory boards created on technical matters.

Fig. 18 is the composition of the Technical Committee of ISO.

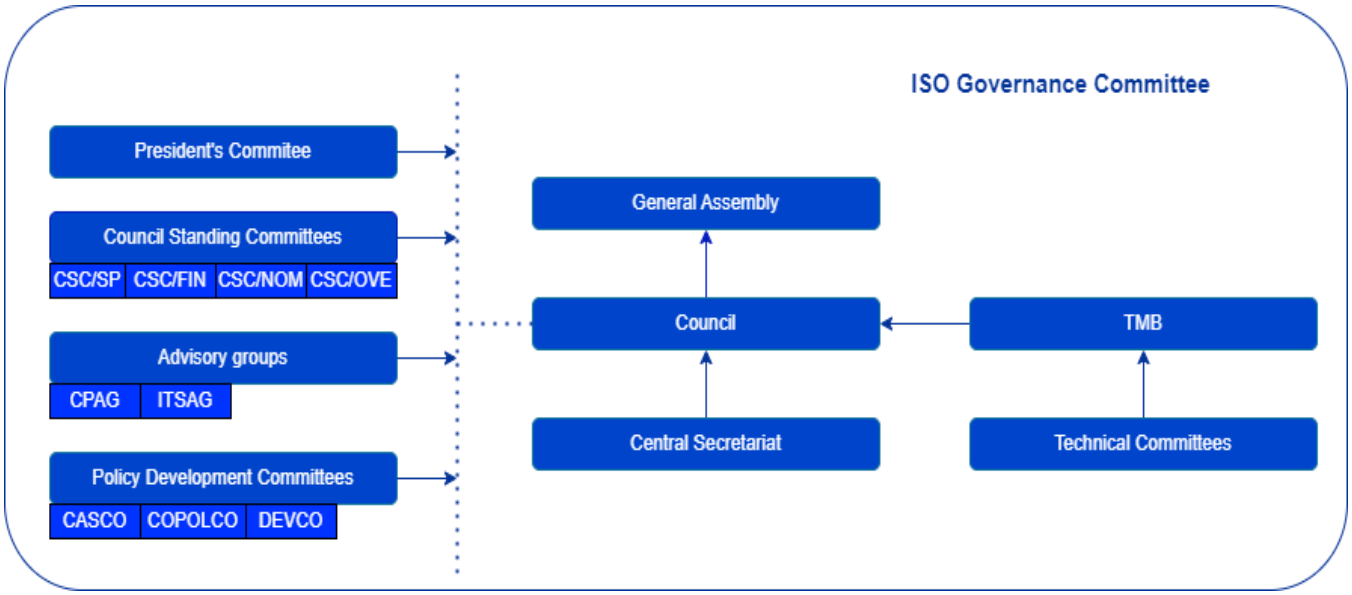

Figure 18. Technical Committee - Composition

ENISA:

As provided in the Regulation (EU) 2019/881, the bodies of the Agency comprise:

- A Management Board: The Management Board is ensuring that the Agency carries out its tasks under conditions which enables it to serve in accordance with the founding Regulation.
- An Executive Board: The Executive Board is preparing decisions to be adopted by the Management Board.
- An Executive Director: The Executive Director is responsible for managing the Agency and performs his/her duties independently.
- A National Liaison Officers Network: The NLOs facilitate the exchange of information between ENISA and the EU Member States.
- An Advisory Group: The Advisory Group assists ENISA in drawing up its work programme, achieving its strategic objectives and communicating with key stakeholders.
- The Regulation 2019/881 also foresees that ENISA shall assist the Commission in providing the secretariat of the European Cybersecurity Certification Group (ECCG) and ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group (SCCG).
- Ad hoc Working Groups: The Executive Director establishes ad hoc Working Groups composed of experts. The ad hoc Working Groups are addressing specific technical and scientific matters.

Fig. 19 depicts the composition of the Technical Committee of ENISA.

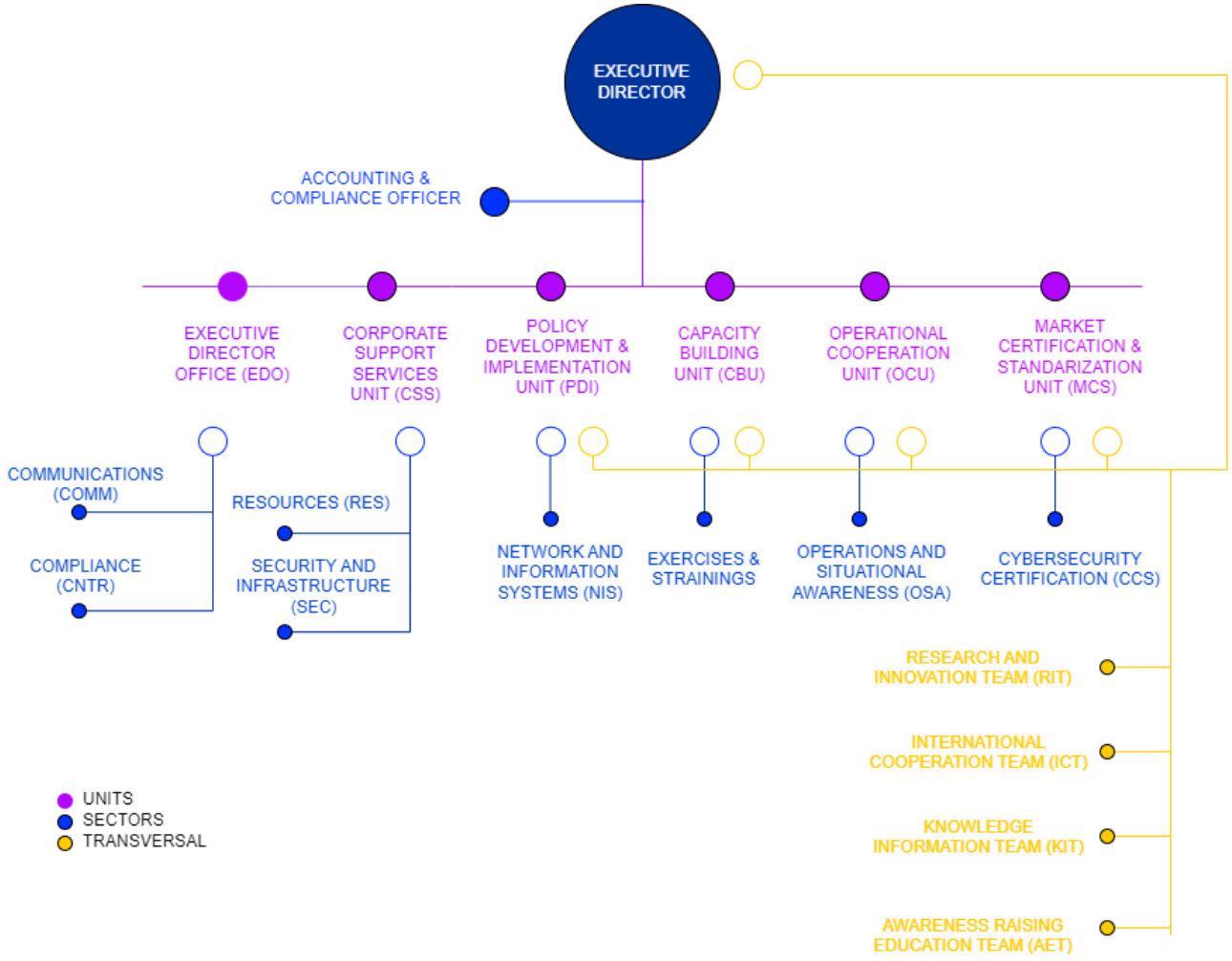

Figure 19. Technical Committee - Composition

ANNEX II: List of identified Standards

In this Annex we present three tables that were part of the questionnaire distributed to partners. The questionnaire includes relevant standards, regulations and directives that are relevant to the EURMARS project.

Also, partners were advised to follow the next steps for the completion of the questionnaire. The original passage is the following:

Every partner is to fill the table accordingly:

1. Complete the Tasks that are related to the specific Standards.
2. Verify whether the following Standards have been followed, used, or are intended to be used in the project.
3. Add any Standards that may fit in the EURMARS project.
4. Provide any general comments or questions.

Table 13 and Table 14 present European and ISO standards respectively.

Table 13. EN standards

No	Code/Name	Task	Yes/No	Description/Scope
1	EN 50136-1:2012 - Alarm Systems-Alarm transmission systems and equipment-Part 1: General requirements			This European Standard specifies the requirements for the performance, reliability and security characteristics of alarm transmission systems. It specifies the requirements for alarm transmission systems providing alarm transmission between an alarm system at a supervised premises and annunciation equipment at an alarm receiving centre. This European Standard applies to transmission systems for all types of alarm messages such as fire, intrusion, access control, social alarm, etc. Different types of alarm systems may in addition to alarm messages also send other types of messages, e.g. fault messages and status messages. These messages are also considered to be alarm messages in the context of this standard. The term alarm is used in this broad sense throughout the document. Additional alarm transmission requirements

				of specific types of alarm systems are given in the relevant European Standards.
2	EN 62676 - Video surveillance systems for use in security applications			IEC 62676-5:2018 defines recommendations and requirements for representation and measuring methods of performance values to be described in materials such as instruction manuals, brochures and specifications of video surveillance camera equipment. The first part of this document defines requirements for description of video surveillance camera specification items. The second part defines requirements for measurement methods of video surveillance camera specification items.
3	EN 50132 - Alarm systems - CCTV surveillance systems for use in security applications			This European Standard gives recommendations for the selection, planning, installation, commissioning, maintaining and testing of CCTV systems comprising of image capture device(s), interconnection(s) and image handling device(s), for use in security applications. The objectives of this standard are to a) provide a framework to assist customers, installers and users in establishing their requirements, b) assist specifiers and users in determining the appropriate equipment required for a given application, c) provide means of evaluating objectively the performance of the CCTV system.
4	EN 60825-1:2014 - Safety of laser products - Part 1: Equipment classification, requirements and user's guide			IEC 60825-1:2014 is applicable to safety of laser products emitting laser radiation in the wavelength range 180 nm to 1 mm. A laser product may consist of a single laser with or without a separate power supply or may incorporate one or more lasers in a complex optical, electrical, or mechanical system. Typically, laser products are used for demonstration of physical and optical phenomena, materials processing, data reading and storage, transmission and display of information, etc. Such systems have found use in industry, business, entertainment, research, education, medicine and consumer products. Laser products that are sold to other manufacturers for use as components of any system for subsequent sale are not subject to IEC 60825-1, since the final product will itself be subject to this standard. Laser products that are sold

				by or for manufacturers of end products for use as repair parts for the end products are also not subject to IEC 60825-1. However, if the laser system within the laser product is operable when removed from the end product, the requirements of this Part 1 apply to the removable laser system. The objectives of this part of IEC 60825 are: - to introduce a system of classification of lasers and laser products emitting radiation in the wavelength range 180 nm to 1 mm according to their degree of optical radiation hazard in order to aid hazard evaluation and to aid the determination of user control measures; - to establish requirements for the manufacturer to supply information so that proper precautions can be adopted; - to ensure, through labels and instructions, adequate warning to individuals of hazards associated with accessible radiation from laser products; and - to reduce the possibility of injury by minimizing unnecessary accessible radiation and to give improved control of the laser radiation hazards through protective features. This edition includes the following significant technical changes with respect to the previous edition: - a new class, Class 1C, was introduced; - the measurement condition 2 ("eye loupe" condition) was removed; - a classification of the emission of laser products below a certain radiance level that are intended to be used as replacement for conventional light sources can, as an option, be based on the IEC 62471 series; - and the accessible emission limits (AELs) for Class 1, 1M, 2, 2M and 3R of pulsed sources, particularly of pulsed extended sources, were updated to reflect the latest revision of the ICNIRP guidelines on exposure limits (accepted for publication in Health Physics Journal 2013, see also www.icnirp.org).
5	EN 50518-1:2013 - Monitoring and alarm receiving centre - Part 1:			This part of EN 50518 specifies the minimum requirements for the design, construction, and functioning equipment for premises where the monitoring, receiving and processing of (alarm) signals generated by one or more intruder and hold-up alarm systems takes place as an integrated part of the total

	General requirements			safety and security process. The requirements apply for applications in a remote configuration where multiple systems report to a single or multiple Alarm Receiving Centre(s) (ARC) as well as to a single site facility aimed for the monitoring and processing of alarms generated by one or more alarm systems installed within the perimeter of that particular site. This part of EN 50518 is to be read in conjunction with Part 2 and Part 3, and cannot be used separately.
6	EN 50133 - Alarm systems - Access control systems			This standard specifies requirements for automated access control systems and components in and around buildings. It includes: system architecture and general requirements of an access control system for security applications, requirements for functions, definition of the environmental and electromagnetic compatibility conditions, requirements for communication of an access control with others, such as access point actuators and sensors, alarm system, etc... The standard does not apply to access point actuators and sensors
7	EN 50136-2:2013 - Alarm systems - Alarm transmission systems and equipment - Part 2: Requirements for signalling equipment			This European Standard specifies the general equipment requirements for the performance, reliability, resilience, security and safety characteristics of supervised premises transceiver (SPT) installed in supervised premises and used in alarm transmission systems (ATS). A supervised premises transceiver can be a stand-alone device or an integrated part of an alarm system. These requirements also apply to SPT's sharing means of interconnection, control, communication and power supplies with other applications. The alarm transmission system requirements and classifications are defined within EN 50136-1. Different types of alarm systems may in addition to alarm messages also send other types of messages, e.g. fault messages and status messages. The term alarm is used in this broad sense throughout the document. Additional requirements for the connection of specific types of alarm systems are given in the relevant European Standards. Because the SPT can be applied in different applications (e.g. I&HAS, fire

				and social alarm systems), requirements for the SPT, additional to those of this European Standard, may be specified in separate application specific documents. This European Standard specifies the requirements specific to alarm transmission. Application specific requirements for the connection of the SPT to specific types of alarm systems are given in the EN 50131 (all parts) for I&HAS, and EN 54 (all parts) for fire. For other SPT applications, see the relevant National or European standards.
8	EN 50600 - Information technology - Data centre facilities and infrastructures			This document: a) specifies the Energy Reuse Factor (ERF) as a KPI to quantify the reuse of the energy consumed in the data centre; b) defines the measurement, the calculation and the reporting of ERF; c) describes the application of ERF and its discrimination from Power Usage Effectiveness (PUE). The ERF does reflect the efficiency of the reuse process, which is not part of the data centre.
9	EN 301 549 - Accessibility requirements for ICT products and services			The standard contains, among other contents: • A description of the needs of persons with disabilities, written as functional performance statements, explaining the functionality that is needed to enable users with different abilities to locate, identify and operate functions in technology (chapter 4). • The accessibility requirements, organised by functions or product features, rather than by commercial product or service categories (chapters 5 to 13). • The description of which requirements of the Standard presume conformance with European Directive 2016/2012 (the Web Accessibility Directive) (annex A). • A description of the relationship between requirements and functional performance statements (annex B).
10	EN 62676-4:2015 - Video surveillance systems for use in security			IEC 62676-4:2014 gives recommendations and requirements for the selection, planning, installation, commissioning, maintaining and testing video surveillance systems (VSS) comprising of image capture device(s), interconnection(s) and image handling

	applications - Part 4: Application guidelines			device(s), for use in security applications. The objectives of this part of IEC 62676 are to: - provide a framework to assist customers, installers and users in establishing their requirements; - assist specifiers and users in determining the appropriate equipment required for a given application; - provide means of evaluating objectively the performance of the VSS.

Table 14. ISO standards

No	Code/Name	Task	Yes/No	Description/Scope
1	ISO/IEC 27001:2013 - Information security management systems – Requirements			ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
2	ISO/IEC 27002:2013 - Code of practice for information security controls			ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: 1. select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; 2. implement commonly accepted information security controls; 3. develop their own information security management guidelines.

3	ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation			ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given. It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations. The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.
4	ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC			ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

	27002 for cloud services			- additional implementation guidance for relevant controls specified in ISO/IEC 27002; - additional controls with implementation guidance that specifically relate to cloud services. This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.
5	ISO/IEC 29100:2011 - Information technology - Privacy framework			ISO/IEC 29100:2011 provides a privacy framework which • specifies a common privacy terminology; • defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for information technology. ISO/IEC 29100:2011 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.
6	ISO/IEC 29151:2017 - Information technology - Security techniques - Code of practice for personally identifiable information protection			ISO/IEC 29151:2017 establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII). In particular, this Recommendation | International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the requirements for processing PII that may be applicable within the

				context of an organization's information security risk environment(s). ISO/IEC 29151:2017 is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII.
7	ISO 9001:2015 - Quality management systems - Requirements			ISO 9001:2015 specifies requirements for a quality management system when an organization: a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements. All the requirements of ISO 9001:2015 are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.
8	ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories			ISO/IEC 17025:2017 specifies the general requirements for the competence, impartiality and consistent operation of laboratories. ISO/IEC 17025:2017 is applicable to all organizations performing laboratory activities, regardless of the number of personnel. Laboratory customers, regulatory authorities, organizations and schemes using peer-assessment, accreditation bodies, and others use ISO/IEC 17025:2017 in confirming or recognizing the competence of laboratories.
9	ISO/IEC 20000-1:2018 - Information			This document specifies requirements for an organization to establish, implement, maintain and

	technology - Service management - Part 1: Service management system requirements			continually improve a service management system (SMS). The requirements specified in this document include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value. This document can be used by: a) a customer seeking services and requiring assurance regarding the quality of those services; b) a customer requiring a consistent approach to the service lifecycle by all its service providers, including those in a supply chain; c) an organization to demonstrate its capability for the planning, design, transition, delivery and improvement of services; d) an organization to monitor, measure and review its SMS and the services; e) an organization to improve the planning, design, transition, delivery and improvement of services through effective implementation and operation of an SMS; f) an organization or other party performing conformity assessments against the requirements specified in this document; g) a provider of training or advice in service management. The term "service" as used in this document refers to the service or services in the scope of the SMS. The term "organization" as used in this document refers to the organization in the scope of the SMS that manages and delivers services to customers. The organization in the scope of the SMS can be part of a larger organization, for example, a department of a large corporation. An organization or part of an organization that manages and delivers a service or services to

				internal or external customers can also be known as a service provider. Any use of the terms "service" or "organization" with a different intent is distinguished clearly in this document.
10	ISO/IEC 25010:2011 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models			ISO/IEC 25010:2011 defines: 1. A quality in use model composed of five characteristics (some of which are further subdivided into subcharacteristics) that relate to the outcome of interaction when a product is used in a particular context of use. This system model is applicable to the complete human-computer system, including both computer systems in use and software products in use. 2. A product quality model composed of eight characteristics (which are further subdivided into subcharacteristics) that relate to static properties of software and dynamic properties of the computer system. The model is applicable to both computer systems and software products. The characteristics defined by both models are relevant to all software products and computer systems. The characteristics and subcharacteristics provide consistent terminology for specifying, measuring and evaluating system and software product quality. They also provide a set of quality characteristics against which stated quality requirements can be compared for completeness. Although the scope of the product quality model is intended to be software and computer systems, many of the characteristics are also relevant to wider systems and services. ISO/IEC 25012 contains a model for data quality that is complementary to this model.

				The scope of the models excludes purely functional properties, but it does include functional suitability. The scope of application of the quality models includes supporting specification and evaluation of software and software-intensive computer systems from different perspectives by those associated with their acquisition, requirements, development, use, evaluation, support, maintenance, quality assurance and control, and audit. The models can, for example, be used by developers, acquirers, quality assurance and control staff and independent evaluators, particularly those responsible for specifying and evaluating software product quality. Activities during product development that can benefit from the use of the quality models include: • identifying software and system requirements; • validating the comprehensiveness of a requirements definition; • identifying software and system design objectives; • identifying software and system testing objectives; • identifying quality control criteria as part of quality assurance; • identifying acceptance criteria for a software product and/or software-intensive computer system; • establishing measures of quality characteristics in support of these activities.
11	ISO/IEC 24762:2008 Information technology — Security techniques			ISO/IEC 24762:2008 provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management, applicable to both

	— Guidelines for information and communications technology disaster recovery services			"in-house" and "outsourced" ICT DR service providers of physical facilities and services. ISO/IEC 24762:2008 specifies: • the requirements for implementing, operating, monitoring and maintaining ICT DR services and facilities; • the capabilities which outsourced ICT DR service providers should possess and the practices they should follow, so as to provide basic secure operating environments and facilitate organizations' recovery efforts; • the guidance for selection of recovery site; and • the guidance for ICT DR service providers to continuously improve their ICT DR services.
12	ISO 22301:2019 - Security and resilience - Business continuity management systems - Requirements			This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity. This document is applicable to all types and sizes of organizations that: a) implement, maintain and improve a BCMS; b) seek to ensure conformity with stated business continuity policy;

				c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption; d) seek to enhance their resilience through the effective application of the BCMS. This document can be used to assess an organization's ability to meet its own business continuity needs and obligations.
13	ISO 31000:2018 - Risk management – Guidelines			ISO 31000:2018 : -provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context. -provides a common approach to managing any type of risk and is not industry or sector specific. -can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

ANNEX III: List of relevant Regulations and Directives

In this Annex we present Table 15 that contains relevant Regulations and Directives that were distributed as the other part of the questionnaire.

Also, partners were advised to follow the next steps for the completion of the questionnaire. The original passage is the following:

Every partner is to fill the table accordingly:

1. Complete the Tasks that are related to the specific Regulations and Directives.
2. Verify whether the following Regulations and Directives have been followed, used, or are intended to be used in the project.
3. Add any Regulations and Directives that may fit in the EURMARS project.
4. Provide any general comments or questions.

Table 15. Regulations and Directives

No	Code/Name	Task	Yes/No	Description/Scope
1	General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679			This regulation sets out rules for the collection, use, and storage of personal data within the EU, and applies to any organization that processes personal data of EU residents. It provides individuals with greater control over their personal data, and requires organizations to implement appropriate technical and organizational measures to protect personal data.
2	Network and Information Security Directive (NIS) – Directive (EU) 2016/1148			This directive aims to enhance cybersecurity across the EU by setting minimum standards for the security of network and information systems in critical sectors such as energy, transportation, banking, and healthcare. It requires organizations to take appropriate security measures and report significant security incidents to relevant authorities.
3	Regulation on the European Border and Coast Guard –			This regulation establishes the European Border and Coast Guard Agency (Frontex), which is responsible for coordinating and carrying out operations to manage the EU's external borders. It provides for increased

	Regulation (EU) 2019/1896			surveillance of the EU's external borders and allows for the deployment of tech'Ical equipment to support border management.
4	Directive on Police and Judicial Cooperation in Criminal Matters (Prüm)–- Council Decision 2008/615/JHA			This directive aims to facilitate cross-border cooperation between law enforcement authorities in the EU by allowing for the exchange of DNA profiles, fingerprints, and vehicle registration data. It sets out rules for the use and protection of this data, and includes safeguards to protect the privacy of individuals.
5	Directive on Security of Network and Information Systems (NIS 2)–- Directive (EU) 2019/881			This directive updates and strengthens the original NIS directive by expanding its scope to cover new sectors, such as online marketplaces and search engines. It also requires organizations to take additional security measures and report security incidents to a dedicated Computer Security Incident Response Team (CSIRT).
6	Regulation on Privacy and Electronic Communications (ePrivacy)–- Proposal for a Regulation (COM(2017) 10 final)			This regulation aims to update and strengthen the rules on privacy and electronic communications in the EU. It sets out rules for the use of cookies, direct marketing, and unsolicited communications, and includes provisions to protect the privacy of individuals in electronic communications.
7	Regulation on Search and Rescue–- Regulation (EU) 2019/1238			This regulation sets out the rules and procedures for search and rescue operations at sea within the EU. It establishes the legal framework for coordinating and carrying out these operations, and provides for the exchange of information and cooperation between relevant authorities.
8	Regulation on the Cybersecurity Act–- Regulation (EU) 2019/881			This regulation establishes a cybersecurity certification framework for information and communication technology (ICT) products, services, and processes in the EU. It aims to improve the security and trustworthiness of ICT products and services, and provide a common certification framework that is recognized across the EU.

9	Regulation (EU) No 656/2014			This regulation establishes rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
10	Regulation (EU) 2018/1725			Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
11	Regulation (EU) No 2019/947			This Regulation lays down detailed provisions for the operation of unmanned aircraft systems as well as for personnel, including remote pilots and organisations involved in those operations.
12	Directive (EU) 2018/1972			This directive establishes the European Electronic Communications Code.

ANNEX IV: Form of new Working Item

Below is the official form of the new Working Item that has to be completed in order to be submitted for a ballot to the CEN/CENELEC committee.

New Work Item Proposal	
* to be attached to the CIB	
TC name – *TC title*	
Secretariat:	Proposal documented in N xx
Date of circulation:	Closing date for voting:
Decision reference:	Decision date:

Proposal

0. This proposal relates to

☐ the adoption of a New Work Item in the committe''s work programme (stage 10.99)

☐ the adoption of a Preliminary Work Item in the committe''s work programme (stage 00.60)

☐ the activation of a Preliminary Work Item in the committe''s work programme (stage 10.99): PWI *XXXXX*

1. Deliverable

☐ European Standard (EN)

☐ Technical Specification (TS)

☐ Technical Report (TR)

2. This item corresponds to

☐ A new project

☐ An amendment to the EN *XXX*

☐ The revision of EN *XXX*

☐ The conversion of TS *XXX* into an EN *XXX*

☐ The revision of TS *XXX*

☐ The revision of TR *XXX*

2.1–- Only for wls of CEN/TCs (not applicable to CEN-CLC/JTCs wls): if this item corresponds to an amendment/revision of an EN indicate if:

☐ the scope will change (weighted vote required–- select the right option in the CIB)

☐ the scope will not change (simple majority vote required–- select the right option in the CIB)

3. Explain the purpose and give a justification for this proposal (max 4000 characters). This text should provide information on technical topics to be discussed.

Note: in case the WI is based on documents from other organizations than ISO/IEC, please specify it here

4. Titles

English title:

French title:
(*Optional*)

German title:
(*Optional*)

5. Scope of the proposed work item (max 4000 characters)

6. Digital aspects

☐ The deliverable is intended to be developed using the Online Collaborative Authoring platform

☐ The deliverable is intended to include non-Word/PDF content, e.g. audio files, XML schemas, machine-readable formats or software.
Please provide details of the non-Word/PDF content:

☐ None of the above.

If yes to either of these questions, CCMC will contact you for feasibility and organizational aspects.

7. Stakeholder categories immediately affected by the proposal

☐ Industry and commerce	☐ Societal consumer groups	☐ Standards application
☐ SMEs	☐ Labour	☐ Non-governmental organization (NGO)
☐ Government	☐ Academic and research bodies	☐ Environmental stakeholders
☐ Consumers		
☐ None of the above categories		

8. How will these Stakeholders benefit from or be impacted by the proposed deliverable?

9. Document developed in drafting body

☐ Existing drafting body *(please give name and title)*:

☐ New drafting body *(please give name and title)*:

10. Proposed Project Leader (including contact details)–- *Optional*

11. United Nations Sustainable Development Goals (SDGs)

Please select any United Nations Sustainable Development Goals (SDGs) that this document will support. For more information, please visit the SDG section of the CEN website (currently under development).

☐ **GOAL 1:** No Poverty
☐ **GOAL 2:** Zero Hunger
☐ **GOAL 3:** Good Health and Well-being
☐ **GOAL 4:** Quality Education
☐ **GOAL 5:** Gender Equality
☐ **GOAL 6:** Clean Water and Sanitation
☐ **GOAL 7:** Affordable and Clean Energy
☐ **GOAL 8:** Decent Work and Economic Growth
☐ **GOAL 9:** Industry, Innovation and Infrastructure
☐ **GOAL 10:** Reduced Inequality
☐ **GOAL 11:** Sustainable Cities and Communities
☐ **GOAL 12:** Responsible Consumption and Production
☐ **GOAL 13:** Climate Action
☐ **GOAL 14:** Life Below Water
☐ **GOAL 15:** Life on Land
☐ **GOAL 16:** Peace and Justice Strong Institutions
(N/A **GOAL 17:** Partnerships to achieve the Goal)
☐ None of the above

Proposed rationale for the selected SDG(s)- (optional):

12. Accessibility aspects

See CEN-CENELEC Guide 6:2014 'Guide for addressing accessibility in standard'

☐ Accessibility aspects are relevant for this NWI *(please indicate which ones):*

See the 'protocol' to help you decide when accessibility following a Design for All approach is relevant: https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/accessibility/design-for-all/

☐ Accessibility aspects are not relevant for this NWI

Please provide a written explanation detailing why accessibility aspects do not apply to the current proposed WI:

13. Environmental aspects

☐ Discharges to soil	☐ Discharges to water	☐ Emission to air
☐ Heat	☐ Noise/Vibration	☐ Use of land
☐ Radiation	☐ Use of energy	☐ Other effects on biodiversity
☐ Use of material	☐ Use of water	☐ Waste
☐ Risk to the environment from accidents/misuse		☐ Chemicals

☐ Other:

☐ None of the above.

Please provide a written explanation detailing why these environmental aspects do not apply to the current proposed WI:

14. How do you plan to address these environmental aspects?

☐ Bring in environmental expertise to the WG

☐ Contact EHD for help/support (cen.ehd@cencenelec.eu) and/or use examples from Environmental Framework https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/environment-and-sustainability/environmental-helpdesk-and-trainings/

☐ Use of environmental checklist and guides (please visit the dedicated section in the CEN website https://boss.cen.eu/reference-material/guidancedoc/pages/environment/

☐ Other:

15. Vienna Agreement (parallel procedure)

☐ No or Vienna Agreement with CEN lead proposed

☐ Yes – Vienna Agreement Parallel with ISO Lead

ISO project reference:
ISO project ID:
ISO/TC:

16. The project is based on

☐ No document from another organization

☐ An ISO or ISO/IEC document (not covered by a parallel procedure)

☐ Identical

☐ Non-identical

ISO/IEC project reference:
ISO/IEC project ID:
Publication date:

☐ A document from another organization than ISO or ISO /IEC:

Note: Please explain the purpose and give a justification for this proposal in Section 3.

☒

17. Please indicate whether the proposed project is linked to a specific European Research and Innovation Project

☐ **No**

☐ **Yes**

Research and/or Innovation project code:
Research and/or Innovation project acronym:
Research and/or Innovation project title:

18. Track

☐ Enquiry + Formal Vote (for EN)

☐ Vote on TS or TR by correspondence

19. Please provide the target dates for the below key stages.

19.1 – For eNs

This section applies only to wIs for homegrown CEN standards (excluding ISO adoptions), wIs under VA with CEN lead only and homegrown standards developed by a CEN-CLC/JTC (with CEN lead). This section does not apply to the adoption of PWIs. For JTCs also add the durations in week.

Project start date (10.99)	**Dispatch of 1st WD (20.60)**	**Dispatch of ENQ (30.99)**	**Dispatch of FV draft** (45.99)
yyyy-mm-dd	It is half the number of weeks planned for ENQ (30.99) For CEN/TC: automatically calculated via Working Area For JTC: date will be added by CCMC	yyyy-mm-dd For JTC only: to indicate the duration in weeks from 10.99 10.99 + X weeks	yyyy/mm/dd For JTC only: to indicate the duration in weeks from 40.60 40.60 + X weeks

19.2 – For TSs and TRs

Project start date (10.99)	**Dispatch of 1st WD (20.60)**	**Dispatch of draft for Vote (30.99)**
yyyy-mm-dd	yyyy-mm-dd	yyyy/mm/dd

20. Related standardization request(s) (formerly mandate):

☐ No

☐ Yes *(please specify)*:

21. Related directive(s)/regulation(s)

☐ No

☐ Yes

Directive/ Regulation reference

Candidate for citation in Official Journal?

☐ No ☐ Yes

☐ No ☐ Yes

22. Relation to other legislation or established public policy.

☐ No

☐ Yes

Please specify which legislation or established public policy is/are in relation with the proposed project:

23. Is the proposed project covered by Intellectual Property Rights (IPR)?

Please indicate whether there is any knowledge of items covered by IPR(s), for instance patents, copyright, trademark, etc.

☐ No

☐ Yes

Please provide full information about these items and the identified IPR(s):

24. Commitment This section applies only to *CEN-CLC/JTC* To *be completed for NWI request to be approved by CEN and CENELEC BTs.*

The following members (at least five) are committed to participate in the development of the project:

ANNEX V: Monitoring

Table 16. List of Similar Projects

Acronym	Title	Website
I-SEAMORE	INTEGRATED SURVEILLANCE ECOSYSTEM FOR EUROPEAN AUTHORITIES RESPONSIBLE FOR MARITIME OPERATIONS LEVERAGED BY RELIABLE AND ENHANCED AERIAL SUPPORT.	https://iseamore-project.eu/
BLENDED	Synergetic use of Blockchain and Deep Learning for Space Data.	
MAGINet	GEOSPATIAL INFORMATION NETWORKING TECHNIQUES FOR MARITIME AWARENESS SERVICES.	
NESTOR	An enhanced pre-frontier intelligence picture to safeguard the European border.	https://nestor-project.eu/
BorderUAS	Semi-autonomous border surveillance platform combining nest generation unmanned aerial vehicles.	https://borderuas.eu/
FOLDOUT	Foliage detection, in the inner and outermost regions of the EU.	https://foldout.eu/
MEDEA	"Mediterranean practitioners' network capacity building for effective response to emerging security challenges".	https://www.medea-project.eu/
ARESIBO	Augmented Reality Enriched Situation awareness for Border security.	https://aresibo.eu/
SUNRISE	"Strategies and Technologies for United and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe".	https://sunrise-europe.eu/
AI-ARC	Artificial Intelligence based Virtual Control Room for the Arctic (AI-ARC).	https://ai-arc.eu/
PERIVALLON	Protecting the EuRopean terrItory from organised enVironmentAl crime through inteLLigent threat detectiON tools.	https://perivallon-he.eu/

Table 17. List of Related Industry Events

Title	Topic	
European Association for Biometrics Research Projects Conference 2023	The 10th edition of the EAB Research Projects Conference is organised by the European Association on Biometrics (EAB) with the contribution of eu-LISA through its Governance and Capabilities Unit, the support of DG HOME of the European Commission, Fraunhofer IGD and Halmstad University. The conference is currently the largest event on research funded by the European Union in the area of Biometrics and Identity Management. Over the previous successful editions, EAB-RPC has become the main forum in Europe where attendees can simultaneously: promote research carried out in biometrics, forge new links and networks, and identify the appropriate partners for possible future project applications. Last year's edition welcomed over 70 participants from academia, industry and public institutions.	https://eab.org/events/program/300
Research and Innovation Symposium for European SECURITY and Defense 2023	The goal of the Symposium is to provide a unique forum for disseminating scientific results, support knowledge exchange, and create networking and clustering opportunities for security stakeholders of EU-funded projects in security and defense.	https://rise-sd.net/
Berlin Security Conference		https://www.euro-defence.eu/
International Conference on Border Security and Protection	Border Security and Protection Conference aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Border Security and Protection Conference. It also provides a premier interdisciplinary platform for researchers, practitioners, and educators to present and discuss the most recent	https://waset.org/border-security-and-protection-conference

	innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Border Security and Protection Conference.	
World Border Security Congress	The World Border Security Congress is the premier multi-jurisdictional global platform where the border protection policy-makers, management and practitioners together with security industry professionals, convene annually to discuss the international challenges faced in protecting borders.	https://world-border-congress.com/
The Official UK Government Global Security Event	Security & Policing offers a world-class opportunity to meet and discuss the latest advances in delivering national security and resilience with leading UK suppliers, UK and overseas Government officials and senior decision makers across the law enforcement and security sectors.	https://www.securityandpolicing.co.uk/
European Police Congress	The European Police Congress is an international congress for decision makers from police forces and security authorities and industries. Its intention is to strengthen the dialogue between the authorities and enable the participants to establish new contacts to colleagues from all over Europe. Every year critical discussions on upto-date issues are held and the latest developments in technologies for the professional use in the security sector are presented by the exhibitors. The European Police Congress is the largest conference for internal security in the European Union.	https://www.european-police.eu/
2nd European Conference on Border Management		https://migration.gov.gr/en/announcement-2nd-european-conference-on-border-management/
Security Research Event		https://home-affairs.ec.europa.eu/policies/internal-security/innovation-and-security-research/security-research-event_en
eu-LISA Annual Conference		https://www.eulisaconference.eu/

Global Aviation Security Symposium Events		https://www.icao.int/Meetings/AVSEC2022/Pages/default.aspx
FRONTEX Border Control Conferences and Events		https://frontex.europa.eu/future-of-border-control/research-and-innovation/announcements/
Maritime Reconnaissance and Surveillance Technology		https://www.smgconferences.com/defence/uk/conference/Maritime-Reconnaissance
DEFEA	The largest and most prominent land, sea, air and national security defence industries around the world participate as exhibitors showcasing their latest technologies and the defence systems that will prevail in the future.	https://defea.gr
NICOSIA RISK FORUM	Nicosia Risk Forum, since 2018, is a merging point for Civil Protection the area of South-Eastern Europe, which brings together academic, industrial, governmental, policy and other societal stakeholders with a significant interest in societal safety.	https://cerides.euc.ac.cy/nicosia-risk-forum/nicosia-risk-forum-2022/
ESREL -European Conference on Safety and Reliability	ESRA aims at the promotion and application of safety and reliability techniques and risk management in all branches of technology.	https://www.esrel2022.com/
NCT Europe 2023	NCT Europe 2023 taking place in the Onderzeebootloods, Rotterdam, The Netherlands, will welcome the highest decision makers from the European CBRNe, C-IED, EOD Community, again providing a networking and knowledge exchange platform for local & federal first responders, as well as industry leaders in the fields of CBRNe, C-IED and EOD. Over the duration of three days, NCT Europe will feature a Conference, an Exhibition, the NCT PRO eXperience, and multiple Networking Opportunities.	https://nct-events.com/event/nct-europe
IGARSS 202X	The International Geoscience and Remote Sensing Symposium (IGARSS) is the flagship conference of the IEEE Geoscience and Remote Sensing Society (GRSS). It is aimed at providing a platform for sharing knowledge and experience on recent developments and advancements in geoscience and remote sensing technologies, particularly in the context	https://www.igarss2022.org/

of earth observation, disaster monitoring and risk assessment.

Table 18 List of Dissemination and Communication Activities

Partner	Type of Activity	Description (location, title of event, the main content of the message, etc.)	Evidence Kept/URL (if applicable)	Date [YYYY.MM.DD]
ALL	Article/Post on EURMARS Website	Project Start post on EURMARS Website	https://eurmars-project.eu/project-start/	2022.10.01
HSE	Article/Post on Own Web Site	Website post on HSE participating in EURMARS	https://hse.gr/hse-participates-in-the-eurmars-project/	2022.10.12
ALL	Article/Post on EURMARS Website	Kick Off Meeting post on EURMARS Website	https://eurmars-project.eu/kick-off-meeting/	2022.10.13
GMD	Post on Facebook Site	Facebook post on GMD participating in Kick off meeting in EURMARS project	https://www.facebook.com/photo/?fbid=485666723603987&set=pcb.485668063603853	2022.11.11
GMD	Article/Post on Own Web Site	Website post on GMD participating in EURMARS	https://dpdetare.gov.al/projekt-eurmars/	2023.01.09
ALL	Article/Post on EURMARS	EURMARS Project live on Twitter	https://twitter.com/EURMARS_Project/status/1612408687640940544	2023.01.09

	Social Media (Twitter)			
ALL	Article/Post on EURMARS Social Media (Linkedin)	EURMARS Project live on Linkedin	https://www.linkedin.com/posts/eurmars-horizoneu_twitter-horizoneu-bordersecurity-activity-7018175136184840192-iSbw?	2023.01.09
ALL	Article/Post on EURMARS Website	Post on Sofia End User Workshop	https://eurmars-project.eu/sofia-end-user-workshop/	2023.02.03
ALL	Article/Post on EURMARS Social Media (Twitter)	Twitter post on Sofia end User Workshop	https://twitter.com/EURMARS_Project/status/1625791022541447169?ref_src=twsrc%5Etfw	2023.02.15
ALL	Article/Post on EURMARS Social Media (Linkedin)	Linkedin post on Sofia end User Workshop	https://www.linkedin.com/feed/update/urn:li:activity:7031577056807129088	2023.02.15
GSH	Article/Post on Social Media(Twitter)	Twitter post on Sofia end User Workshop	https://twitter.com/GeosystemsGr/status/1625864805172015105	2023.02.15
GSH	Article/Post on Social Media(Linkedin)	Linkedin post on Sofia end User Workshop	https://www.linkedin.com/feed/update/urn:li:activity:7031630325587820544	2023.02.16
BDI	Article/Post on Social Media(Linkedin)	Linkedin post on Sofia end User Workshop	https://www.linkedin.com/feed/update/urn:li:activity:7039901573044416514	2023.03.10
ALL	Article/Post on EURMARS Website	Post on EURMARS Website Sofia 1st Plenary Meeting	https://eurmars-project.eu/1st-plenary-meeting-sofia/	2023.04.03
ALL	Article/Post on EURMARS Social Media (Twitter)	Twitter post on Sofia 1st Plenary Meeting	https://twitter.com/EURMARS_Project/status/1642874596780064774?s=20	2023.04.03

ALL	Article/Post on EURMARS Social Media (Linkedin)	Linkedin post on Sofia 1st Plenary Meeting	https://www.linkedin.com/feed/update/urn:li:activity:7048643637403918336	2023.04.03
ALL	Article/Post on EURMARS Website	EURMARS CYPSEC2023 Website Post	https://eurmars-project.eu/eurmars-project-presentation-at-cyprusdefence-security-conference-cypsec2023/	2023.05.23
ALL	Article/Post on EURMARS Social Media (Twitter)	Twitter post EURMARS CYPSEC2023	https://twitter.com/EURMARS_Project/status/1660978750077513728?s=20	2023.05.23
ALL	Article/Post on EURMARS Social Media (Linkedin)	Linkedin post EURMARS CYPSEC2023	https://www.linkedin.com/feed/update/urn:li:activity:7066755526293958659	2023.05.23
ALL	Article/Post on EURMARS Website	EURMARS RISE-SD Website Post	https://eurmars-project.eu/eurmars-presented-in-rise-sd-2023/	2023.06.07
ALL	Article/Post on EURMARS Social Media (Twitter)	Twitter post EURMARS RISE-SD	https://twitter.com/EURMARS_Project/status/1666414922664689665?s=20	2023.06.07
ALL	Article/Post on EURMARS Social Media (Linkedin)	LinkedIn post EURMARS RISE-SD	https://www.linkedin.com/feed/update/urn:li:activity:7072192562794500096	2023.06.07
ALL	Article/Post on EURMARS Website	Post - The Ethics of Border management Surveilance Technology Workshop	https://eurmars-project.eu/the-ethics-of-border-management-surveillance-technology-workshop/	2023.06.16
ALL	Article/Post on EURMARS Social Media (Twitter)	Post - The Ethics of Border management Surveilance	https://twitter.com/EURMARS_Project/status/1669700037620760577?s=20	2023.06.16

		Technology Workshop		
ALL	Article/Post on EURMARS Social Media (Linkedin)	Post - The Ethics of Border management Surveilance Technology Workshop	https://www.linkedin.com/feed/update/urn:li:activity:7075466548231946240	2023.06.16
ALL	Article/Post on EURMARS Website	EURMARS to Project to Policy Seminar	https://eurmars-project.eu/eurmars-participated-to-projects-to-policy-seminar/	2023.06.19
ALL	Article/Post on EURMARS Social Media (Twitter)	EURMARS to Project to Policy Seminar	https://twitter.com/EURMARS_Project/status/1672201238706831361?s=20	2023.06.19
ALL	Article/Post on EURMARS Social Media (Linkedin)	EURMARS to Project to Policy Seminar	https://www.linkedin.com/feed/update/urn:li:activity:7076900449429127170	2023.06.19
ALL	Article/Post on EURMARS Website	EURMARS project presentation at iProcureNet Workshop	https://eurmars-project.eu/eurmars-project-presentation-at-iprocurenet-workshop/	2023.09.19
ALL	Article/Repost on EURMARS Social Media (Linkedin)	EURMARS project presentation at iProcureNet Workshop	https://www.linkedin.com/feed/update/urn:li:activity:7107685666108379136	2023.09.19
ALL	Article/Repost on EURMARS Social Media (Twitter)	EURMARS project presentation at iProcureNet Workshop	https://x.com/skyld_ltd/status/1701890378897440808?s=20	2023.09.19

ANNEX VI: Dissemination and Communication Survey

EURMARS

EURMARS Dissemination And Communication Survey

Dear EURMARS partners, this survey aims to better understand each partner's dissemination and communication channels, activities and capabilities. This knowledge about the experience, resources and communication channels and tools you can provide should help us to have a more efficient coordination of our dissemination and communication activities within EURMARS. The survey should take approximately 15-20 minutes to fill out. Thank you in advance for your support!

One (1) submission per partner!

1. Please select for which EURMARS partner organisation you provide information. *

Choose

2. Which communication channels/tools do your organisation use on a regular basis? *

- [ ] Own Website
- [ ] Facebook
- [ ] Twitter
- [ ] LinkedIn
- [ ] Youtube
- [ ] Newsletter and/or website of a parent organization/network
- [ ] Digital newsletter
- [ ] Printed newsletter
- [ ] Press release
- [ ] Policy brief
- [ ] Articles in magazines (to general audience)
- [ ] Academic journals
- [ ] Other:

3. If you use the newsletter/website of a parent organisation/network - please specify which organisation/network

Your answer

Own Website

4. Are you planning to use your website for the communication of EURMARS activities and dissemination of results? *

- ◯ Yes
- ◯ No

5. If no, please provide a short explanation why not

Your answer

6. What is the average visits per month on your Website?

Your answer

7. If you are representing a university, which parts of the website you have access to for publishing EURMARS related news?

- ◯ General university's website
- ◯ Website of our department
- ◯ Other:

8. Please select the relevant target audiences of your website

- [ ] General public
- [ ] Media
- [ ] Students
- [ ] Experts / scientific community
- [ ] Political stakeholders / NGOs
- [ ] Clients
- [ ] Other:

9. In which language(s) are contents published on your website?

Your answer

10. How complicated is it for you to update content on your website?

very easy

1 ◯
2 ◯
3 ◯
4 ◯
5 ◯

very complicated

11. Please share with us any other relevant information regarding your website that might be interesting for the dissemination and communication activities in the EURMARS project

Your answer

Facebook

12. Does your organisation have a Facebook account? *

- ◯ Yes
- ◯ No

13. If yes, what is your organisation's Facebook account URL?

Your answer

14. If yes, how many followers does your Facebook account have?

Your answer

15. If yes, do you plan to use this account for the communication of EURMARS related activities?

- ◯ Yes
- ◯ No

16. If you don't plan to use the account for EURMARS, please provide a short explanation why not

Your answer

17. In which language(s) are your Facebook posts published in?

Your answer

18. Please share with us any other information regarding your Facebook presence that might
be relevant for the dissemination and communication activities in EURMARS

Your answer

Twitter

19. Does your organization have a Twitter account?

- ◯ Yes
- ◯ No

20. If yes, what is your organisation's Twitter account URL?

Your answer

21. If yes, do you plan to use this account for the communication of EURMARS related activities?

- ◯ Yes
- ◯ No

22. If you don't plan to use the account for EURMARS, please explain why not

Your answer

23. In which language(s) are your Twitter posts published in?

Your answer

24. How many followers does your Twitter account have?

Your answer

25. Please share with us any other information regarding your Twitter presence that might be
relevant for the dissemination and communication activities in EURMARS

Your answer

LinkedIn

26. Does your organization have a LinkedIn account?

- ◯ Yes
- ◯ No

27. If yes, what is your organisation's LinkedIn account URL?

Your answer

28. If yes, do you plan to use this account for the communication of EURMARS related activities?

- ◯ Yes
- ◯ No

29. If you don't plan to use the account for EURMARS, please explain why not

Your answer

30. In which language(s) are your LinkedIn posts published in?

Your answer

31. How many followers does your LinkedIn account have?

Your answer

32. Please share with us any other information regarding your LinkedIn presence that might be
relevant for the dissemination and communication activities in EURMARS

Your answer

Youtube

33. Does your organization have a Youtube account?

- ○ Yes
- ○ No

34. If yes, what is your organisation's Youtube account URL?

Your answer

35. If yes, do you plan to use this account for the communication of EURMARS related activities?

- ○ Yes
- ○ No

36. If you don't plan to use the account for EURMARS, please provide a short explanation why not

Your answer

37. In which language(s) are your contents on Youtube published in?

Your answer

38. How many followers does your Youtube account have?

Your answer

39. Please share with us any other information regarding your Youtube presence that might be
relevant for the dissemination and communication activities in EURMARS

Your answer

Digital Newsletter
Please fill out this section only, if your organization has an digital newsletter. If that's not the case,
you can skip this part.

40. How often is the newsletter published
monthly, quarterly, twice a year, etc.)?

Your answer

41. How many subscriptions does your Newsletter have?

Your answer

42. Do you plan to use this newsletter for the communication of EURMARS related activities?

- ○ Yes
- ○ No

43. If no, please provide a short explanation why not

Your answer

44. Please select the relevant target audiences of your newsletter

- ☐ General public
- ☐ Media
- ☐ Students
- ☐ Experts / scientific community
- ☐ Political stakeholders / NGOs
- ☐ Clients
- ☐ Other:

45. In which language(s) are contents published
in your newsletter?

Your answer

46. Please share with us any other information regarding your electronic newsletter that might
be relevant for the dissemination and communication activities in EURMARS

Your answer

Printed Newsletter
Please fill out this section only, if your organization has a printed newsletter. If that's not the case, you
can skip this part.

47. How often is the newsletter published
(monthly, quarterly, twice a year, etc.)?

Your answer

48. What is the amount of copies you plant to print for the newsletter?

Your answer

49. Do you plan to use this newsletter for the communication of EURMARS related activities?

- ○ Yes
- ○ No

50. Space to explain (it necessary)

Your answer

51. Which is the geographical distribution of your newsletters?

- ○ European level
- ○ National level
- ○ Local level
- ○ Other:

52. At your organization, do you keep track of your press appearances or press related activities?

- ○ Yes
- ○ No

Academic Journals

53. Does anyone of the EURMARS related department/staff of your organization publish in academic journals?

- ○ Yes
- ○ No

54. Are you planning to do it related to the EURMARS project activities and results?

- ○ Yes
- ○ No
- ○ We are not sure yet

55. Which academic journals do you publish in, that are relevant for the scope of EURMARS?

Your answer

In the following, several possible target audience groups for the EURMARS project are listed. Please state how important you think these target audiences are for the work we do in EURMARS

56. Law enforcement agencies/ Intelligence agencies

very important

1 ○
2 ○
3 ○
4 ○
5 ○

not important at all

57. Border security/management and coast guard agencies

very important

1 ○
2 ○
3 ○
4 ○
5 ○

very important

58. Data providers/Data service providers

very important

1 ○
2 ○
3 ○
4 ○
5 ○

not important at all

59. Technology/ service providers, investors

very important

1 ○
2 ○
3 ○
4 ○
5 ○

not important at all

60. Member States/ ministries/ government departments

very important

1 ○
2 ○
3 ○
4 ○
5 ○

not important at all

61. Regulators and policy-makers

very important
1 ○
2 ○
3 ○
4 ○
5 ○
not important at all

63. Standardization bodies

very important
1 ○
2 ○
3 ○
4 ○
5 ○
not important at all

62. Citizens

very important
1 ○
2 ○
3 ○
4 ○
5 ○
not important at all

64. Media

very important
1 ○
2 ○
3 ○
4 ○
5 ○
not important at all

65. Scientific R&D institutions

very important
1 ○
2 ○
3 ○
4 ○
5 ○
not important at all

66. In your opinion, which communication channels/tools should receive the greatest attention
in EURMARS? Please choose up to 5 from the list below

- ☐ EURMARS website
- ☐ Websites of EURMARS partner organisations
- ☐ Facebook
- ☐ Twitter
- ☐ LinkedIn
- ☐ Youtube
- ☐ Press releases
- ☐ Newsletters
- ☐ Policy briefs / expert reports for political stakeholders
- ☐ Papers in academic journals
- ☐ Articles in magazines to general audience
- ☐ EURMARS brochures. flyers, folders, etc.
- ☐ EURMARS workshops
- ☐ Presentations at expert/academic conferences

EURMARS

An advanced surveillance platform to improve the EURopean Multi Authority BordeR Security efficiency and cooperation