ETSI GR CDM 001 V1.1.1 (2021-01)

Common Information Sharing Environment Service and Data Model (CDM); Use Cases definition

Disclaimer

The present document has been produced and approved by the european Common information sharing environment service and Data Model ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/CDM-001

Keywords
data sharing, maritime, safety, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2021.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

List of figures

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) european Common information sharing environment service and Data Model (CDM).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

On October 2009, the European Commission adopted a communication "Towards the integration of maritime surveillance in the EU: A common information sharing environment for the EU maritime domain (CISE)", promoting to integrate maritime surveillance activities of all public maritime sectors across Europe (Figure 1).

Figure 1: Schematic diagram of the CISE vision

The aim of the integrated maritime surveillance is to generate a situational awareness of activities at sea, impacting on the denominated seven maritime sectors Maritime Safety and Security, Border Control, Maritime Pollution and Marine Environment Protection, Fisheries Control, Customs, General Law Enforcement, Defence, as well as the economic interests of the EU, so as to facilitate sound decision making.

The added value of integrating maritime surveillance is to enhance the present sectoral maritime awareness pictures of the sectoral user communities, with additional relevant cross- sectoral and cross-border surveillance data on a responsibility to share basis. Such enhanced pictures increase Member States authorities' efficiency and improve cost effectiveness.

Thus, the decentralized information exchange system is directed to interlink all relevant User Communities, taking into account existing sectoral information exchange networks and planned system, and allowing for the improvement and development of both the existing sectoral systems, and the overarching CISE network architecture.

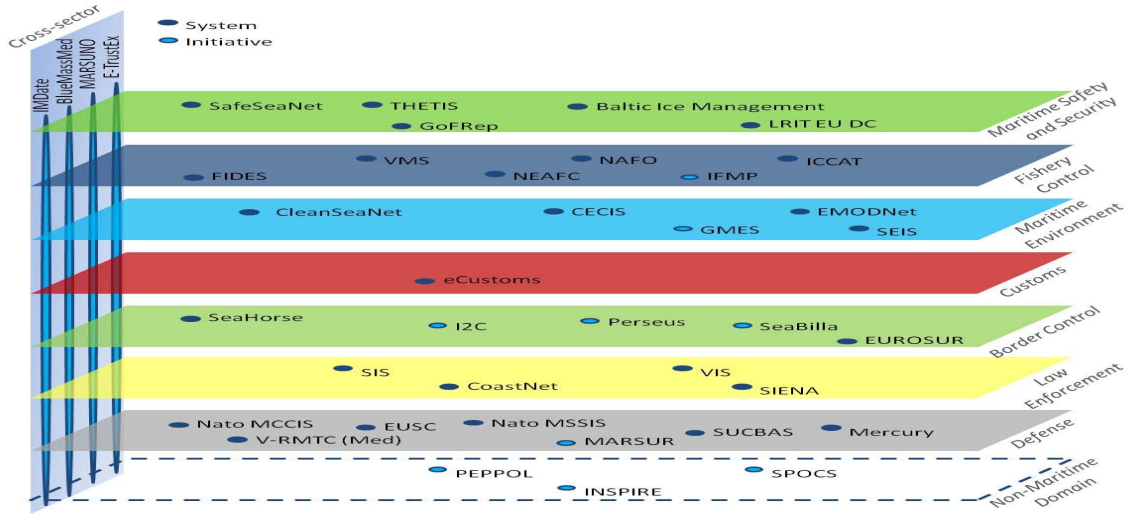

Figure 2: Existing sectoral information systems

To achieve the goals of the CISE vision, a series of EU sponsored projects, building up one on another, further investigated and developed the CISE vision, starting with the elaboration of the so-called CISE principles, which were defined as follows [i.1]:

- *"CISE must allow the interlinking of any public authority in the European Union (EU) or European Economic Area (EEA) involved in maritime surveillance".*
- *"CISE must increase maritime awareness based on the "responsibility-to-share" principle".*
- *"CISE must support a decentralized approach at EU-level".*
- *"CISE must provide interoperability between civilian and military information systems".*
- *"CISE must be compatible and provide interoperability between information systems at the European, national, sectoral and regional levels."*
- *"CISE must support the reuse of existing tools, technologies and systems."*
- *"CISE must provide for seamless and secure exchange of any type of information relevant to maritime surveillance."*
- *"CISE must support the change of services by information provider (orchestration)."*
- *"CISE subscribers and stakeholders should be entitled to obtain information only if they also contribute in a way commensurate with their capabilities."*

The CISE roadmap process that started with the definition of the CISE principles is shown in Figure 3.

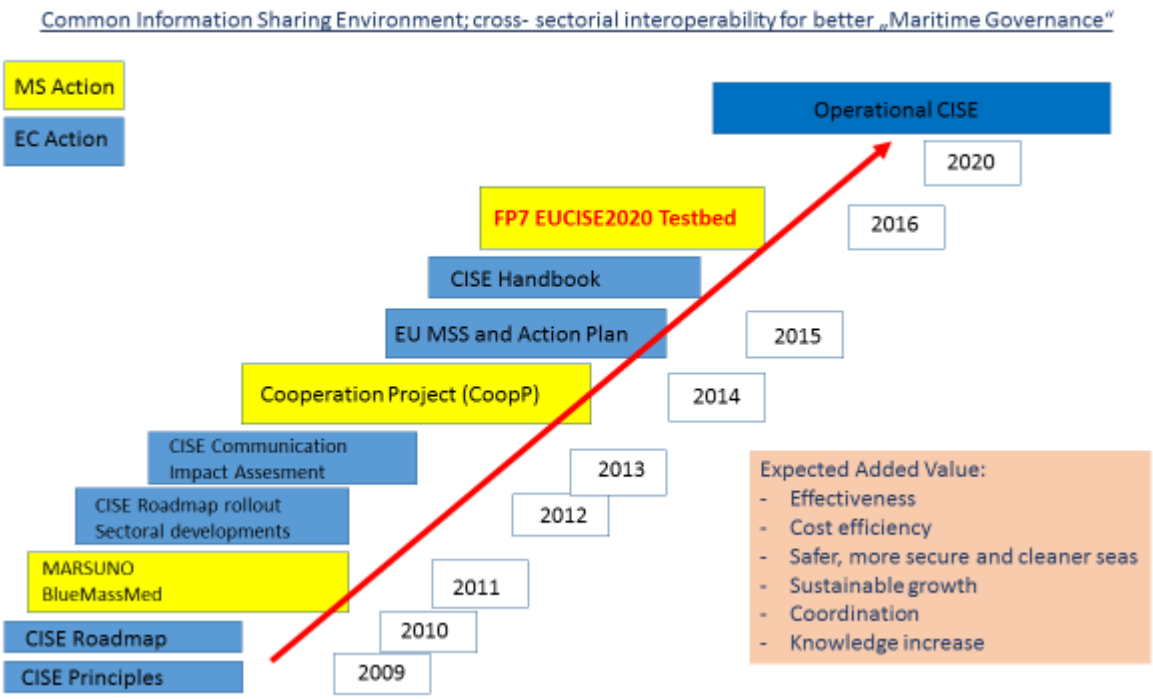

Figure 3: CISE Roadmap

During the roadmap process, a range of 82 use cases was defined representing the entire range of activities of the 7 maritime sectors and their related Coast Guard activity. Out of this range of 82 use cases, 9 use cases were identified as most characteristic and comprehensive, covering the most relevant activities of all sectors. These use cases were to form the operational basis for the further and more detailed investigation of CISE cross- sectoral and cross border information exchange.

The pre- operational validation project **"European test bed for the maritime Common Information Sharing Environment in the 2020 perspective", in short "EUCISE2020"**, based on the 9 use cases selected, defined the requirements and developed the common architecture of the CISE information exchange network. Consequently, a total of 12 so-called "CISE Nodes" were built, integrated and successfully tested in 9 European countries, connecting a total of 20 sectoral legacy systems of various nature (Figure 4).

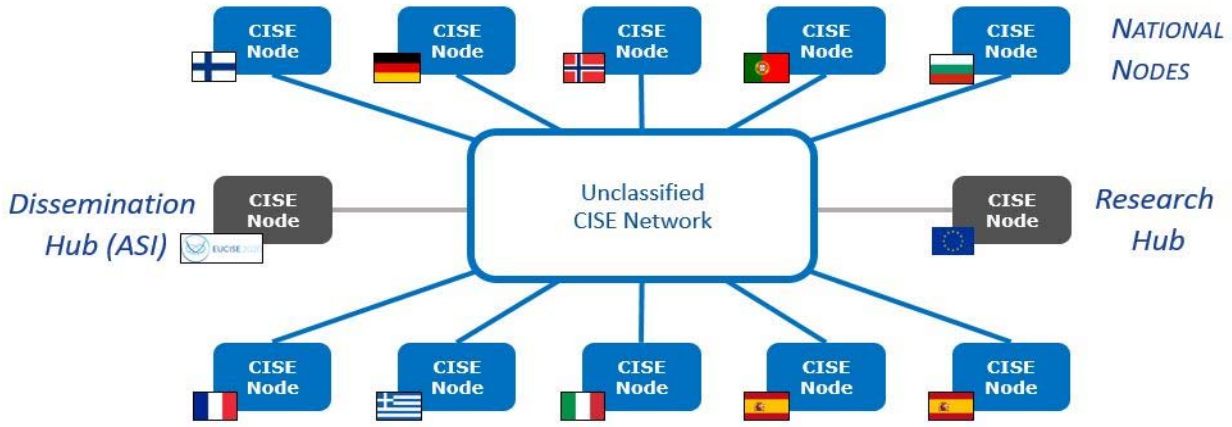

Figure 4: Diagram of the EUCISE2020 testbed set- up

Hybrid and complementary cross- sectoral and cross- border information exchange requires a common "data language" within the common network architecture as well as a common set of IT- services to handle the data transfer. The **technical standardization** proposal for CISE implementation was therefore directed towards a standardization process within the framework of a professional European standardization environment in order to elaborate universal and sustainable technical specifications for the implementation and development of CISE, as well as offering a technical solution for other, similar information exchange regimes.

The present document has been elaborated with the support of the Joint Research Centre (JRC) of the European Commission.

1 Scope

The present document describes the use cases of interest for the Common Information Sharing Environment for Maritime Surveillance (CISE). These use cases are based on the results of the pre-operational validation FP7 EUCISE2020 project.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] CISE Architecture Visions Document V3.0 06/11/2013.

NOTE: Available at https://webgate.ec.europa.eu/maritimeforum/en/node/4039.

[i.2] IMO MSC1/circ 1333.

NOTE: Available at https://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Pages/MSC.aspx.

[i.3] IMO MSC1/ circ 1334.

NOTE: Available at https://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Pages/MSC.aspx.

[i.4] Consolidated version of the Treaty on European Union (TEU).

NOTE: Available at http://data.europa.eu/eli/treaty/teu_2012/oj.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

activity: activity performed by a sector

agent: person or organization

CoopP: project financed by the European Commission in 2013 defining the CISE use cases and the first version of the CISE data and service model

NOTE: See https://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance_en for more information.

cross-border: exchange of information between EU or EFTA countries

cross-sector: exchange of information between two or more sectors

EUCISE2020: FP7 pre-operation validation project on CISE

NOTE 1: The project defined and developed the existing CISE Network and software (2014 - 2019).

NOTE 2: More information on the project can be found at http://www.eucise2020.eu/.

legacy system: existing software designed to perform specific tasks and that exposes certain functionalities through interfaces in the domain of the Maritime Surveillance

NOTE: In the present document, Legacy Systems are maintained by Public Authorities. Legacy Systems are the originator and final destinations of messages exchange in CISE.

localized object: object or event related with a geographic position

maritime object: tangible object relevant to maritime surveillance activities as vessel or cargo

public authority: any organization or legal entity that has an interest in maritime surveillance information

NOTE 1: An authority can be local, regional, national or European.

NOTE 2: This organization may have responsibilities linked to one of the seven sectors of maritime surveillance.

sector: one of the seven sector involved in maritime surveillance

NOTE: The seven sectors are the following:

- Maritime Safety, Security and Prevention of Pollution by Ships.
- Fisheries Control.
- Marine Pollution Preparedness and Response, Marine Environment.
- Customs.
- Border Control.
- General Law Enforcement.
- Defence.

user: person appointed by the Public Authorities, interacting directly with CISE or with a Legacy System connected to CISE

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
AIS	Automatic Identification System
C2	Common and Control system
CISE	Common Information Sharing Environment
CSDP	Common Security and Defence Policy
EEA	European Economic Area
EEZ	Exclusive Economic Zone
EMSA	European Maritime Safety Agency
EOS	Electro-Optical System
EU	European Union

EUROSUR	European border Surveillance System
HQ	High Quality
ICES	International Council for the Exploration of the Sea
IMO	International Maritime Organization
ISPS	International Ship and Port Security
ISSC	International Ship Security Certificate
IT	Information Technology
IUU	Illegal, Unreported and Unregulated fishing
JDP	Joint Deploy Plan (European Fisheries Control Agency)
MARSUR	Maritime Surveillance networking
MS	Member State
NAFO	North Atlantic Fisheries Organization
PCS	Port Community System
RFMO	Regional Fisheries Management Organization
RMP	Recognized Maritime Picture
RTC	Real Time Closure
SAR	Search And Rescue
SOP	Standard Operating Procedures
SRR	Search and Rescue Region
TEU	Treaty of the European Union
TW	Territorial Waters
UAV	Unmanned Arial Vehicles
VHF	Very High Frequency
VMS	Vessel Monitoring System
VTMIS	Vessel Traffic Management Information System
VTS	Vessel Traffic Services

4 Overview

The present document defines the scope of CISE by providing a high level description of the activities and situations related to Maritime Surveillance where the exchange of information could be beneficial. The present document provides the identified use cases to illustrate these exchanges as well as the nature of the information exchanged.

5 Activities and situations covered by Maritime Surveillance

5.1 Motivation

The main purpose of the use cases described in clause 5 is to allow the exchange of maritime information between Legacy Systems of different Public Authorities, cross sectors and cross borders, for surveillance purpose.

The main activities related to Maritime Surveillance have been divided in three main categories:

- baseline operations;
- targeted operations; and
- response operations.

Clause 5.2 describes the purposes of each of these activities, the main challenges and the potential improvements identified to increase the efficiency and effectiveness of the activity.

The situations monitored have been further divided in five main classes, designated as "events":

- Situational awareness.
- Anomalies.

- Operational availability.
- Extra-ordinary.
- Virtual interaction.

5.2 Maritime Surveillance sectors

The seven sectors of activities involved in Maritime Surveillance are identified as follow:

- Maritime Safety, Security and Prevention of Pollution by Ships.
- Fisheries Control.
- Marine Pollution Preparedness and Response, Marine Environment.
- Customs.
- Border Control.
- General Law Enforcement.
- Defence.

Within each sector, several activities are performed. The following list is not exhaustive and is illustrative:

- For the Maritime Safety, Security and prevention of pollution sector:
  - Vessel traffic management.
  - Vessel Traffic Safety.
  - Monitoring of security of ships.
  - Search and Rescue.
  - Support of response and enforcement operations (anti-piracy, SAR, salvage).
- For the Fisheries Control sector:
  - Early warning of illegal fisheries or fish landings.
  - Monitoring of compliance with regulations on fisheries.
  - Support of response and enforcement operations.
- For the Marine pollution preparedness and response sector:
  - Monitoring of compliance with regulations.
  - Early warning of environmental accidents and incidents.
  - Support of pollution response operations.
- For the Customs sector:
  - Monitoring of compliance with customs regulation on import, export and movement of goods.
  - Support of enforcement operations.
- For the Border Control sector:
  - Monitoring of compliance with regulations on immigration and border control crossings.
  - Support of enforcement operations.

- For the General Law Enforcement sector:
  - Monitoring of compliance with applicable legislation in sea areas where police competence is required.
  - Support to enforcement and response operations.
- For the Defence sector:
  - Monitoring in support of defence tasks such as national sovereignty at sea.
  - Combatting terrorism and other hostile activities outside the EU.
  - Other CSDP tasks as defined in Articles 42 and 43 of TEU [i.4].

5.3 Maritime Surveillance activities categories

The activities categories are described using the following fields:

- Purpose: identifies the purpose of the activity.
- Challenges: defines the type of activities covered by this category.
- Activity frequency: identifies how frequently the activity is carried out.
- Potential Improvements: identifies potential improvements to this category of activities to improve their efficiency.

5.4 Baseline Operations

Table 1

Details	Process Description
"Baseline" Everyday surveillance and information sharing	Everyday monitoring of events in the maritime domain or "Behaviour monitoring".
Purpose	This endeavour ensures the lawful, safe and secure performance of maritime activities. Furthermore, the activity covers the detection of anomalies (detection of possible non-compliance) and the gathering of triggers/intelligence to improve decision making for the use of response capabilities (e.g. targeting of inspections).
Challenges	In baseline operations, each sector or actor monitors its own responsibilities. Information is shared in accordance with the agreements in place, covering cross-sector and/or cross-border exchanges. The activity maximizes information sharing to increase awareness and to promote decision making. It uses pre-emptive actions and decision making to minimize the need for "response operations". Baseline operations includes also action against single events or minor actions, such as: - response to SAR situations; - action against a detected oil spill from a single ship; - detection and seizure of non-declared cargo; - routine fishery inspection; - work with detection of infringement and seizure; - boarding and inspections for different reasons, and so on. Baseline operations use national and cross-sector information tools and sensors. The activity includes sector-specific data exchange requirements, procedures and systems defined in specific EU or international regulatory frameworks. Baseline operations use: - national surveillance sensors shared with others as required; - common available data sets/services region-, EU- or worldwide such as e.g. AIS information; - agreed incident reporting systems; - sector-specific communication procedures and networks; - sector-specific data exchange systems and services.
Activity frequency	Ongoing (always).

Details	Process Description
Potential Improvements	This high-level activity describes basically "Everyday Operations". Improvements in this area will affect all other activities. It will enable better indication of unlawful, unsafe and unsecure activities, better planning, better use of operational assets and quicker response times. The following additional improvements are expected: - Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). - Common standard operating procedures across sectors and borders. - Common format for information and/or data from sensors. - Common entity services (as many as possible) across sectors and borders. - Sharing of best practises and results in anomaly detection and risk analysis. Applies across sectors and borders. - Common rules for history input to, e.g. databases.

5.5 Targeted Operations

Table 2

Details	Process Description
"Targeted" surveillance and information sharing for targeted operations	Targeted operations towards a specific activity.
Purpose	This activity consists in reacting to or confronting specific threats to sectorial responsibilities as discovered in risk analysis/intelligence gathering processes. This activity will give support to operational decision-making when employing operational assets.
Challenges	Targeted operations cover typically sector-driven operational activity planned in advance, often with the deployment of operational assets to detect and prevent violations of the safe, secure and lawful performance of maritime activities within own sector. Target Operations may be limited in time, space and geography. The scope of these targeted operations may be limited to a sector cooperation, cross-border, regional or EU wide. Target Operations may be triggered by sectorial risk, threat analysis or may be used as a "deterrence". Even though operations are sector driven, information sharing across sectors occurs. Examples may include and be exemplified by: - JDPs (e.g. NAFO) in international and EU waters. - Operation ATALANTA - Operation MINERVA, INDALO
Activity Frequency	As required - triggered by intelligence and/or risk analysis.
Potential Improvements	The key factor for success is a cooperation and interaction crow-border within a specific sector, as well as information sharing with all sector and Member States. Common tools for interactive communication and collaboration are of great value in planning operations and making best use of operational assets. The following improvements are expected: - Common collaborative tools (voice, HQ video). - Improvement of availability of information. - Clearer rules for inter- and intra-sector sharing mechanisms (access rights and security levels). - Common standard for operating procedures across sectors and borders. - Common format for information and/or data from sensors. - Common entity services (as many as possible) across sectors and borders. - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. - Common rules for history access to history of Targeted Operation.

5.6 Response Operations

Table 3

Details	Process Description
"Response" Operations	Response to major incidents, events or accidents.
Purpose	This activity ensures the appropriate response to events affecting many sectors and with a potentially major impact on, e.g. the environment and economy.
Challenges	Typically, a response to complex events involves several actors from different sectors and across borders. Events occur suddenly, without warning. Decisions are made under time pressure, implying complicated cross-border and cross-sector considerations. Potentially huge values are at stake - environmental, financial and human lives. Response Operations require a critical operational coordination across sectors and borders. Most of the time, a large amount of operational assets are involved. Examples of Response Operations: - "Estonia" or "Costa Concordia" -type ferry disaster. - Tanker collision with large passenger carrier. - Sudden massive migration flow due to specific events, e.g. natural disaster or war. - Terrorist attack or threat of attack with weapons of mass destruction. - Cross-border efforts to stop large amounts of drugs with unclear destination from reaching the EU. - Fishing gear conflicts and conflicts between groups of fishing vessels (which could lead to the need for immediate intervention (possibility of vessels attacking each other). (See note).
Activity Frequency	Irregular. Frequency based on a "case-by-case" basis. Predictions are not possible, and the event may be totally unforeseen. Response Operations may be required over long or short periods of time.
Potential Improvements	The following improvements are expected: - Establishment of common collaboration tools. - Knowledge of availability of operational assets across sectors and borders. - Established, frequently trained routines across sectors and borders for all sorts of intervention. - Common Standard Operating Procedures (SOPs). - Common or shared support services to detect anomalies and risks. - Immediate access to an extended array of data that is normally not included in the maritime field. - Cross-border or cross-sector agreements covering extensions of "normal" latitude.
NOTE: "Normal" incidents, such as a single SAR case, a single fishing violation or a case of smuggling are included under "Baseline Operations" above.	

5.7 Maritime Surveillance Events

5.7.1 General

Events are developments of the activities categories described in clause 5.3. They describe what overarching services may be used for each event.

The events are described using the following fields:

- Process Name: identifies the processes involved in the event.
- Event Name: provides a name to the event.
- Description: describes the event, including the type of information exchange involved.
- Event Frequency: describes how often the event is expected, it could be permanent (continuous activity) or punctual.
- Potential Improvements: identifies improvements that could increase the efficiency of the response to the event.

5.7.2 Situational awareness

Table 4

Details	Event Description
Process Name	Collecting, processing and sharing basic maritime data.
Event Name	Sector Recognized Maritime Picture (RMP) or situation.
Description	National, regional or EU-wide services are used to provide a recognized maritime picture for a specific sector. National or regional maritime situational awareness may be tailored for sectorial or cross-sectorial purposes depending on national legislation, bilateral or multilateral agreements. Information exchange and sharing are in line with this principle. Basic data sources or services contain open information. It is important that the amount of services used provides as much open information as possible. Map services, weather services, tools for visualization and compilation are examples of means to improve quality of information. Typically, basic and additional information is shared on a regular basis. This event can be divided into two levels: - Acquisition of a Common Basic Maritime Situation (level 1). - Elaboration of a Consolidated Common Maritime Situation (level 2). In the 1st level, actors are existing institutional communities acting in the acquisition domain (e.g. EMSA and Members States' communities). At this level, there is no sensitive information and there is no limitation on sharing information within the CISE environment. The 2nd level requires additional information, such as: - Information on the travel, cargo, etc. - Worldwide information history (ships, routes). - Additional data from non-permanent data sensors (naval, aerial, space sensors). - Information from maritime databases (ship characteristics for classification/recognition/identification). This additional information is collected in order to complete the picture, to avoid duplication of ships and routes, to detect falsification of ship's identity, and to perform the other necessary correlations for integrity control and for the validation of all information of the Consolidated Common Maritime Situation. This function cannot be merged with the acquisition function since it needs to correlate basic data with additional data (for example fishing vessel location). The function is activated in routine mode and represents the Level 2 of the operations flow. It can be activated in prevention mode; in this case, the procedure applied for the surveillance of the zone can be classified as sensitive information by the Member States.
Event Frequency	Permanent (H24).
Potential Improvements	The Situational awareness is linked to the high-level activity "Baseline", and the detailed use case No. 4.

5.7.3 Anomalies

Table 5

Details	Event Description
Process Name	Detect anomalies, incidents and conduct risk assessment and analysis in the maritime domain.
Event Name	Anomaly event triggering operational action.
Description	Manual and automated detection of incidents that falls outside the frame of "normal operations". The incidents are typically detected within its own sector or responsibility. They may require an action from other sectors. The services used may include sector or domain-wide anomaly detection tools, risk analysis and planning tools. Typically, basic and additional information is shared on a regular basis.
Event Frequency	Permanent (H24).
Potential Improvements	The following improvements are expected: - Sharing of anomalies and detected risks throughout sectors and borders. - Common or "best practices tools" would be of great importance for discovering threats to the lawful, secure and safe conduct of maritime and marine activities. This would improve the performance of authorities in different sectors. - Proper sharing mechanisms are essential (technical, SOPs and legal conditions).

5.7.4 Operational availability

Table 6

Details	Event Description
Process Name	Availability of assets.
Event Name	Knowledge of availability of operational assets.
Description	This event covers the cross-border and cross-sector knowledge of assets available for operations. It also covers the sharing of planned operations in the maritime domain. Common standards (SOPs) and communication tools are needed. A service for sharing this information (including contact information) is essential. During these events, basic and additional information is shared on a regular basis.
Event Frequency	Punctual (As required).
Potential Improvements	The following improvements are expected: - The knowledge of available assets which, in return, will reduce patrol cost, overlapping surveillance costs and readiness cost. - Great potential for savings in terms of lives, environmental and marine values, etc.

5.7.5 Extra ordinary

Table 7

Details	Event Description
Process Name	Extended information sharing.
Event Name	Extra-ordinary events requiring an increase of information availability.
Description	When major incidents or accidents occur there is a need to coordinate assets from several sectors and nations. These events require decision making across sectors and borders and information sharing outside normal patterns. The services of exchange should be designed to share information accordingly. Basic and additional information needs to be shared as well as restricted as required.
Event Frequency	Punctual (As required).
Potential Improvements	The following improvements are expected: - Quicker and more accurate decision making under time constraints, which will save time and costs during operations. - More accurate perception of the situation before decision making.

5.7.6 Virtual interaction

Table 8

Details	Event Description
Process Name	Virtual Interaction.
Event Name	Virtual User Groups.
Description	There is a need for virtual (online voice and video) interaction between decision makers, operators and on-scene commanders/coordinators when responding to events, coordinating resources and planning activities, both cross-border and cross-sector. The aim is to share information from person to person or between groups in order to attain a real-time recognizable picture of the event, whether for planning purposes, or during execution of a response operation. Services to facilitate this would include high quality video and audio streaming, video sensor information and document presentation. Services would enable pre-defined tailored user groups for specific purposes.
Event Frequency	Punctual (As required). The more frequent the use, the better the environment for information sharing, planning and decision making.
Potential Improvements	The following improvements are expected: - Better trust and confidence between authorities. - Easier to connect operational networks in case of accidents. - Better operational planning, saving time and money. - Potentially less risk of error when interacting person to person. - More robust decision-making.

6 Use Cases related to information

6.1 Motivation

Nine use cases focused on the type of information exchanged have been selected for their representativeness. The list of use cases is not exhaustive, and more use cases can be inferred from the list of potential cross sector information exchanged provided below.

The use cases are described using the following fields:

- Goal: defines the main goal of the use case.
- Operational situation/Trigger: identifies what triggers the use case.
- Lead Actor: identifies the user communities involved.
- Supporting Actor(s): identifies user communities that can contribute to the use case (as secondary actor).
- Activity category: identifies the Maritime Surveillance categories for the use case (among Baseline, Targeted and Response).
- Post-conditions: identifies the main output of the use case.
- Failure/Outcome: identifies the main potential failures, their outcomes and their causes.
- Flow of Events: describes the main flow of event for the use case.
- Alternative Scenarios: describes variations from the main flow of events.
- Procedures: identifies specific points to be added to the Standard Operational Procedures (SOP).
- Traceability: identifies how the traceability should be improved.
- Inputs Summary: summaries the main data type to be exchanged during the use case.
- Output Summary: summaries the main data type that can be exchanged at the end of the use case.
- Potential improvements: identifies the main improvements required to improve the efficiency of the use case.

NOTE: In EUCISE2020 and CoopP projects, different use case identifiers were used. A relationship of the use case ID is shown in annex A.

6.2 Use Case ID 1

Table 9

Use Case ID 1	Description
Goal	Inquiry on a specific suspicious vessel (cargo related).
Operational situation/ Trigger	Intelligence or other information systems reveal that a ship's cargo is illegal, dangerous or in other ways in breach of rules and regulations.
Lead Actor	Border Control, Customs, General Law Enforcement, Defence.
Supporting Actor(s)	Defence, General Law Enforcement, Marine Pollution Preparedness and Response/Marine Environment.
Activity category	Baseline, Targeted, Response.
Post-conditions	Sector decision makers made decision to act or not (and with what resources).

Use Case ID 1	Description		
Failure/Outcome	**Failure**	**Outcome**	**Condition leading to outcome**
	1) Failure to receive the requested information, information not precise, not relevant or not provided in a timely manner.	Uncertainty if cargo is illegal or not: 1) Illegal cargo will reach its destination. 2) Operational resources not deployed to verify cargo. 3) Lack of decision support leads non-optimal management of resources.	1) Poor information sharing. 2) Request not directed to the correct Authority. 3) Request not clear. 4) Restricted information.
	2) Failure to respond to suspicious cargo shipments.	1) Cargo reaches destination. 2) Excise duties not paid.	1) Lack of decision support leads to non-optimal management of resources. 2) Operational resources not deployed effectively to verify cargo.
	3) Failure to adequately address security levels.	1) Poor information security procedures.	1) Inadequate or faulty security information guidelines/rules.
Flow of Events	The actor responsible for detecting illegal cargo gets an information alert signal from one or more systems. The information alert may come from e.g. anomaly detection services, other actors' systems or other intelligence sources. The actor queries the system to get replies from other sources of information in order to confirm own sources. The outcome of this process will be a decision on intervention or not. It will also initiate the sharing of additional information.		
Alternative Scenarios	1) Uncertainty if cargo is illegal: the decision to control is based on targeting cargo (Pre-arrival data) with a view to enrich intelligence and justify intervention as described in the "flow of events". 2) Unwanted effects on society: solving the unwanted effects on sector could be achieved by improving tools, enhancing the organization of customs services and multiagency cooperation (medium term process).		
Procedures	**Scope:** anti-smuggling and commercial fraud (mis- declarations of goods), and any other cargo related illegal activity. **Case:** Crew Fraud or Vessels Search. **Type of intervention:** search of vessels at sea or in port (once ship docked). **For risk analysis exclusively:** - Risk indicators: composition of crew, type of vessel, routine checks (Are crew-members known to the Authorities? What is the ship's history?). - As far as possible: coordination with other Member States Customs services to prevent search the same parts of the vessel in case of calls in two European seaports successively -- commodities targeted: cigarettes, narcotics, fake white goods, fake clothing, etc.		
Traceability	A database of suspicious vessels, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the relevant authorities.		
Inputs Summary	- Vessels "flagged" by anomaly detection. - risk analysis from own or other authority. - Shared pre-arrival data, Knowledge of resources for intervention. - Basic Ship Data (position, voyage and permanent data). - Additional data (cargo and crew/passenger).		
Output Summary	- Inspection report including follow up activities. - Detailed report regarding cargo, persons on board. - Lessons learned.		

Use Case ID 1	Description
Potential improvements	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). - Common standard operating procedures across sectors and borders. - Common entity services (as many as possible) across sectors and borders. - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders.

6.3 Use Case ID 2

Table 10

Use Case ID 2	Description		
Goal	Inquiry on a specific suspicious vessel (crew and ownership related).		
Operational situation/ Trigger	Intelligence sources alert that persons on board a vessel could be illegal or have criminal background. Uncertainty over the ownership of the vessel.		
Lead Actor(s)	Defence, Border control, General Law Enforcement.		
Supporting Actor(s)	Defence, Border control, General Law Enforcement.		
Activity category	Baseline, Targeted, Response operations.		
Post-conditions	In case of positive response, relevant authorities alerted. Make an inspection as soon as possible. Seek additional support from other Agencies/countries as necessary.		
Failure/Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	Failure to receive the requested information, not relevant or not provided in a timely manner.	The inspection of the crew is not done, the ship continues its voyage. 1) Criminals achieve their objective. 2) Law is not upheld.	1) Restricted information. 2) Request not directed to the Lead organization/Agency. 3) Request not clear.
	Information is not precise.	1) Poor decision making process. 2) Intelligence is compromised. Information on crew and/or ownership suspect.	1) Request not clear. 2) Information received not relevant.
Flow of Events	The actor responsible of detecting illegal crew activities gets an alert triggering a response. This alert may come from different sources e.g. from an intelligence source or from an information or alarm from any Sector Authorities or from another Member State. The outcome of this process will be a decision on intervention or not. It will also initiate sharing of additional information.		
Alternative Scenarios	1) Uncertainty if crew is illegal: the decision to control is based on targeted vessel (Pre-arrival data) with a view to enrich intelligence and justify intervention as described in "flow of events". 2) Unwanted effects on society: solving the unwanted effects on sector could be achieved by improving tools, enhancing the organization of customs services and multiagency cooperation (medium term process).		
Procedures	Identify the origin of the ship and gather all relevant information about the ship, port of departure, cargo, and crew. Seek additional information about the ship from other Member States. (Personal data information sharing needs to be compliant with law.) State precisely what information is needed and give a brief explanation about why the information is required. Be sure the information is encrypted or sent in a secured way. Information sharing between user needs to be by secured means. Confidence building is critical between users.		
Traceability	A database of suspicious vessels could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the relevant authorities.		

Use Case ID 2	Description
Inputs Summary	- Vessel "flagged" by anomaly detection. - Risk analysis from own or other authority. - Shared pre-arrival data. - Knowledge of resources for intervention. - Basic Ship Data (position, voyage and permanent data). - Additional data (cargo and crew/passenger).
Output Summary	- Inspection report including follow up activities. - Detailed report regarding cargo, persons on board. - Lessons learned.
Potential improvements	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). - Common standard operating procedures across sectors and borders. - Common entity services (as many as possible) across sectors and borders. - Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders.

6.4 Use Case ID 3

Table 11

Use Case ID 3	Description		
Goal	Investigation of antipollution situation (law enforcement).		
Operational situation/ Trigger	A vessel is suspected of polluting: - Sighting by satellite. - Sighting by aircraft. - Sighting by surface vessel. - Sighting from coast line. - Detection by AI (e.g. interferometry, video analysis, etc.). - Reported by vessel polluting. - Reported by other sources.		
Lead Actor(s)	Marine pollution preparedness and response/Marine Environment.		
Supporting Actor(s)	General law enforcement, Maritime Safety.		
Activity category	During Baseline, Targeted and Response operations (in case of environmental disaster such as The Prestige), a pollution sighting is verified.		
Post-conditions	In case of positive response, relevant authorities alerted. Make an intervention as soon as possible. Seek additional support from other Agencies/countries as necessary: 1) Pollution contained and analysed to determine source for possible prosecution. 2) Database feed for lessons learned, action taken reporting.		
Failure/Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	1) Pollution not contained. 2) Analyses not satisfactory.	1) Polluter not prosecuted. 2) Environmental damage to sea life and shoreline.	1) Insufficient number of sensors or poor quality. 2) Insufficient anti-pollution resources. 3) Insufficient operational coordination. 4) Insufficient law enforcement procedures
	1) Failure to receive the requested information.	1) Pollution not detected. 2) Environmental damage to sea life and shoreline. 3) Environment affected, polluter not prosecuted.	1) Poor information sharing. 2) Request not directed to the correct Authority. 3) Request not clear. 4) Restricted information. 5) Poor sensor quality. 6) Inadequate Alert systems.

Use Case ID 3	Description
Flow of Events	Responsible authorities alerted of a suspicious pollution event. (System alerts to each member state of the presence of a suspicious vessel in their territorial waters). The alert may come from a number of sources e.g. AIS system, all-source intelligence, from other member states or from a vessel that has observed some irregular activities. The own member state asks to the system for any additional information about the vessel. If the system has any important information regarding the vessel, the complete information is reported: name, cargo, ownership, activity, position, previous pollution problems. Other information exchanged: - Containment plan initiated. - Response vessels mobilized. - Response aircraft mobilized. - C2 in place. - Interagency coordination group meet and decide on best course of action. - Actions carried out. - Event close.
Alternative Scenarios	During this use case, the following events may occur: - Time lag in reporting. - Response vessels and aircraft not available. - Poor C2. - No pollution response plan. - Inter-Agency rivalry.
Procedures	- System detects the presence of a vessel suspicious of polluting. - The actor introduces the identification number, or the name of the vessel in the system. - The system looks for any relative information and asks for the other users about this issue. - The information is given to the Lead Actor.
Traceability	A database of suspicious vessels suspected of polluting, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected of (or have caused) pollution should alert the operator to report presence of vessel to the relevant authorities.
Inputs Summary	- Report or sensor input on pollution. - Drift model usage. - Pollutant data (type, substance, volume, etc.). - Ship data (basic and additional, cargo, ownership). - Response resources (national and cross border). - C2 structure cross border and cross sector.
Output Summary	- Alert to shipping and shore authorities. - Successful prosecution of polluter. - Financial claims settled. - Database input (lessons learned, Pollution reports).
Potential improvements	- Improvement of availability of information. - Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). - Common standard operating procedures across sectors and borders. - Common entity services (as many as possible) across sectors and borders. - Sharing of best practises and results in anomaly detection and risk analysis, applied cross sectors and borders.

6.5 Use Case ID 4

Table 12

Use Case ID 4	Description		
Goal	Monitoring of all events at sea in order to create conditions for decision making on interventions.		
Operational situation/ Trigger	Sensor information e.g. coastal radars and cameras, aerial sensor information and AIS relaying information in real time or delayed, and other information services (anomaly detection services, databases) and systems such as local VTS, PCS, MS VTMIS, EUROSUR, or MARSUR.		
Lead Actor(s)	All User Communities.		
Supporting Actor(s)	All User Communities.		
Activity category	Baseline.		
Post-conditions	Recognized maritime picture.		
Failure/Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	1) Technical failures.	1) No data input. 2) Less than optimum response.	1) Low quality sensors/systems. 2) No redundancy in systems. 3) Lack of contingencies.
	2) Operators fail to detect threats.	The threat is not identified.	1) Lack of training. 2) Lack of common SOPs.
	3) The event is not detected hence remains unknown.	No intervention possible.	1) Training and/or operational posture. 2) Technical faults.
	4) The event is detected but the information is not integrated into the system.	No intervention possible.	1) System integration not adequate.
	5) The information is integrated but not sent to the relevant authority(-ies).	No intervention possible.	1) Operator fault. 2) System integration/ architecture inadequate.
	6) Failure to detect Contact of Interest.	Contact of Interest is not detected.	1) Incomplete Recognized Maritime Picture. Poor interagency cooperation. Inexperienced operators.
Flow of Events	Monitoring systems are always sending information (e.g. sensor readings, tracks and pictures), that needs to be interpreted by a trained operator. If monitoring systems send aggregated information (also in the shape of alarms), they are expected to be validated by a trained operator. In case of anomalies in vessel behaviour, the operator triggers a process for intervention. This use case requires: - Services to deliver information on basic, additional and restricted information with a high level of reliability. - Tools and functional services to process basic ship data in order to produce risk analyses and anomaly detection. - Sharing of alerts to other cross sector and borders. - Operators and decision-making procedures to be able to act if necessary. - Sharing of information in accordance with SOPs and agreements cross border- and sector. - Sharing of history input.		
Alternative Scenarios	None.		
Procedures	The reports are processed and related information is fused with other data/information in accordance with SOPs of authorities involved.		
Traceability	Data coming from all available sensors are displayed and fused together for operators or the evaluation is done automatically.		
Inputs Summary	Sensor input (radar tracks, AIS, Cameras, satellites, UAVs, etc.).		
Output Summary	Anomalies related to vessel movements detected and operational intervention considered.		

Use Case ID 4	Description
Potential improvements	This is the use case which basically describes "Everyday Operations". Improvements in this area will affect all other activities. It will allow for better indications of unlawful, unsafe and unsecure activities, better planning, better use of operational assets and quicker response times. It is closely related to the High-Level Use Case "Baseline Operations". The other following improvements are expected: • Improvement of availability of information. • Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). • Common standard operating procedures across sectors and borders. • Common format for information and/or data from sensors. • Common entity services (as many as possible) across sectors and borders. • Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. • Common rules for history input to e.g. databases.

6.6 Use Case ID 5

Table 13

Use Case ID 5	Description		
Goal	Request for any information confirming the identification, position and activity of a vessel of interest.		
Operational situation/ Trigger	Member state authorities have an interest in knowing the current position of a vessel, its activity, identification, etc. The information could be requested because: • The vessel is subject to police investigation. • The vessel is suspected of involvement of irregular migration, drug smuggling or other cross border crime. • There are evidences of pollution from the vessel. • The vessel owner is subject to an adverse legal judgement. • The vessel is subject to an investigation from an intelligence agency.		
Lead Actor(s)	All user communities.		
Supporting Actor(s)	All user communities.		
Activity category	Baseline, Targeted and Response operations.		
Post-conditions	The information can support an intelligence process, a police investigation or even confirm (in a positive or negative way) a suspicious track. It supports decision on intervention or not.		
Failure/Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	1) The information is not provided in a timely manner.	1) The investigation is compromised. 2) Relevant Authorities not notified in a timely manner leading to non-intervention. 3) An environmental disaster occurs.	1) Request not directed to correct authority. 2) Classification mismatch. 3) Incomplete Recognized Maritime Picture. 4) Poor SOP's. 5) Inexperienced operators.
	2) Information not provided.	1) The investigation does not take place. 2) Relevant Authorities not notified in a timely manner leading to non-intervention. 3) An environmental disaster occur.	1) Failure to communicate through agreed lines of communications. 2) Classification mismatch. 3) Incomplete Recognized Maritime Picture. 4) Poor SOP's. 5) Inexperienced operators.

Use Case ID 5	Description		
	3) Incorrect and not complete response.	1) Time delay verifying request. 2) The investigation cannot continue. 3) Relevant Authorities not notified in a timely manner leading to non-intervention.	1) Failure to communicate coherently. 2) Lack of sensor- or database information. 3) Lack of proper information sharing functions. 4) Lack of SOPs. 5) Incomplete Recognized Maritime Picture. 6) Inexperienced operators.
	4) The information is not updated.	1) decision making process compromised. 2) Poor utilization of resources.	1) Communication failure. 2) Lack of proper information sharing functions. 3) Lack of SOPs.
Flow of Events	User needs to know the position of a vessel. The system checks the AIS signals, radar tracks and other resources (such as local VTS and PCS) and the vessels position is verified. Additional information is provided by other sensors or Regulatory authorities.		
Alternative Scenarios	-		
Procedures	User seeks information for the position, activities or the identification of a suspicious vessel. The system checks and provides the position (and other related basic maritime data - e.g. from AIS). Additional available information (additional and restricted data) is provided by functional services, e.g. current identification, former names, current activity, historical activities.		
Traceability	A shared database of suspicious vessels, could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of vessel to the relevant authorities.		
Inputs Summary	All available information services concerning a specific vessel.		
Output Summary	• Vessel position, identification and activity. • Decision support on intervention or not. • Input to historic databases.		
Potential improvements	• Common correlation services. • Improvement of availability of information. • Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). • Common standard operating procedures across sectors and borders. • Common entity services (as many as possible) across sectors and borders. • Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. • Common rules for history input to e.g. databases.		

6.7 Use Case ID 6

Table 14

Use Case ID 6	Description
Goal	Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance.
Operational situation/ Trigger	• Need for enhancing or complement surveillance in areas where surveillance is poor or there is a specific surveillance need. • Support for decisions where to deploy additional surveillance assets.
Lead Actor(s)	All user communities.
Supporting Actor(s)	All user communities.
Activity category	Baseline, Targeted and Response operations.
Post-conditions	Sectors/ Nations share information on own surveillance capacities and capabilities.

Use Case ID 6	Description		
Failure Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	1) Information not shared.	1) Decision making process compromised. 2) Poor Recognized Maritime Picture. 3) Uncertainty about surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance. 4) Lack of decision support leads non-optimal management of resources. 5) Operational potential not achieved. 6) Less effective planning of operations.	1) Lack of inadequate procedures for sharing information. 2) Classification levels. 3) Request not directed to the correct Authority. 4) Request not clear. 5) Restricted information.
	1) Incomplete Recognized Maritime Picture.	1) Higher risks for illegal maritime events and accidents.	1) Inadequate information transferred.
Flow of Events	• Request for information received through agreed lines of communication. • Request is comprehensive in nature. • Information transferred through agreed lines of communication in a timely manner. • Information transferred is comprehensive in nature. • Information transferred is pertinent to the request.		
Alternative Scenarios	None.		
Procedures	• Each sector/Actor monitors their own surveillance needs for baseline operations. When surveillance situation needs enhancement, operators send request to others (cross sector and/or border) for sharing and coordination of surveillance results/ assets. • When a planned operation is to occur (targeted operations), the lead organization/agency liaise with other actors in the operation to ensure conformity to agreed actions/timelines Information exchange only made through secure channels.		
Traceability	Shared knowledge of surveillance capacities.		
Inputs Summary	• Request from actor in need of enhancement of surveillance. • Surveillance needs for a planned operation.		
Output Summary	• Answer to request of surveillance enhancement. • Surveillance plan for planned operations. • Deployment plan for surveillance assets. • Coordination of surveillance assets.		
Potential improvements	• Common correlation services. • Improvement of availability of information. • Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). • Common standard operating procedures across sectors and borders. • Common entity services across sectors and borders. • Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. • Common rules for history input to e.g. databases.		

6.8 Use Case ID 7

Table 15

Use Case ID 7	Description		
Goal	Suspect Fishing vessel/ small boat is cooperating with other type of vessels.		
Operational situation/ Trigger	A fishing vessel/small boat is suspected to have suspected activities with another vessel.		
Lead Actor(s)	General Law enforcement, Customs, Fisheries control, Defence, Maritime Safety, Border Control.		
Supporting Actor(s)	General Law enforcement, Customs, Fisheries control, Defence, Maritime Safety, Border Control.		
Activity category	Baseline, Targeted, Response operations.		
Post-conditions	• All available information collected. • Support for intervention decision provided. • Operational assets alerted. • Event recorded. • Lessons learned and other information provided to databases.		
Failure/Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	1) Information is not provided in a timely manner.	1) The investigation is compromised. 2) Relevant Authorities not notified in a timely manner leading to non-intervention.	1) Request not directed to correct authority. 2) Classification mismatch. 3) Incomplete Recognized Maritime Picture. 4) Poor SOP's. 5) Inexperienced operators.
	2) Information not provided.	1) No Investigation takes place. 2) Relevant Authorities not notified.	1) Failure to communicate through agreed lines of communications. 2) Classification mismatch. 3) Incomplete Recognized Maritime Picture. 4) Poor SOP's. 5) Inexperienced operators.
	3) Incorrect and/or not complete response.	1) Time delay verifying requests. 2) Relevant Authorities actions compromised.	1) Failure to communicate coherently. 2) Lack of sensor- or database information. 3) Lack of proper information sharing functions. 4) Lack of SOPs. 5) Incomplete Recognized Maritime Picture. 6) Inexperienced operators. 7) Availability of operational assets.
Flow of Events	Intelligence alert to the presence of a fishing vessel/small boat suspected of collaborating with other suspected vessels. The track of the fishing vessel is monitored and, if it is possible, an inspection should be carried out.		
Alternative Scenarios	None.		
Procedures	• Identify the origin of the fishing vessel and gather as much information as possible about the vessel, port of departure, catch, and crew details. • Same procedure with the other collaborative vessel if the identification is known. • Draw historical and current information on the vessel for input to the decision making process. • Specify the type of information required and the reasons why it is required. • Information exchange by secure means. • Alert the relevant authorities.		
Traceability	A database of suspicious vessels could be useful for checking vessels inside a given area (territorial water/sea basin for instance). Cross checking ship information per AIS signals with a register of vessels suspected should alert the operator to report presence of a vessel to the relevant authorities.		

Use Case ID 7	Description
Inputs Summary	Basic, additional and restricted maritime traffic and additional information such as: • Identification number of the fishing vessel. • Identification number of the collaborative vessel if possible. • Catch. • Flags. • Crew if possible. • Last AIS signal. • Last known verified position. • History of both vessels.
Output Summary	• All the identification data required. • Tracks and other data over the event to feed databases.
Potential improvements	• Common correlation services. • Improvement of availability of information. • Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). • Common standard operating procedures across sectors and borders. • Common entity services (as many as possible) across sectors and borders. • Sharing of best practises and results in anomaly detection and risk analysis, applied cross sectors and borders. • Common rules for history input to e.g. databases.

6.9 Use Case ID 8

Table 16

Use Case ID 8	Description		
Goal	Anti-Piracy Maritime Surveillance and free navigation control: Merchant vessels at sea (outside Territorial waters) sends an alert that it is under Piracy attack.		
Operational situation/ Trigger	An alert is received by MS designated authority regarding a piracy attack of a ship entitled to fly its flag outside territorial waters.		
Lead Actor(s)	Defence/Maritime Safety/General law enforcement.		
Supporting Actor(s)	Defence/Maritime Safety/General law enforcement.		
Activity category	Response Operation.		
Post-conditions	Pirates fail to hijack ship. Pirates seized and brought to justice. All available information collected: • Support for intervention decision provided. • Operational assets alerted. • Event recorded. • Lessons learned and other information provided to databases.		
Failure/Outcomes	**Failure**	**Outcome**	**Condition leading to outcome**
	1) Insufficient amount of correct information available.	1) Slow decision-making and reaction time. 2) Pirates board vessel. 3) Human lives at risk.	1) Information sharing in real time insufficient. 2) Poor sensor /data availability. 3) Improper SOPs. 4) Security levels/agreements. 5) Poor interagency cooperation.
	2) Difficulties to exchange restricted information in time.	1) Slow decision-making and reaction time. 2) Pirates board vessel. 3) Human lives at risk	1) Improper sharing mechanisms for restricted information. 2) Improper SOPs.
	3) Slow decision-making.	1) Slow decision-making and reaction time. 2) Pirates board vessel. 3) Human lives at risk.	1) Poor interagency cooperation. 2) Poor SOPs for interagency decision making under time pressure. 3) Inadequate means of communication and interaction between authorities.

Use Case ID 8	Description
Flow of Events	• The Alert is received and immediately an operational emergency order is activated. • Interagency cooperation is an immediate need - cross border and sector. • Information flow to be very near real time with operations. Two-way information flow.
Alternative Scenarios	None.
Procedures	When a competent Administration receives notification of a ship security alert, that Administration needs to immediately notify the State(s) in the vicinity of which the ship is presently operating. When a MS (Contracting Government) receives notification of a ship security alert from a ship which is not entitled to fly its flag, that MS needs to immediately notify the relevant Administration and, if appropriate, the Member State(s) in the vicinity of which the ship is presently operating. When the vessel that sends the security alert is located, the rest of the users of the system should activate an agreed common operational rescue plan. This operational plan should be similar for all members, over all in the case that the vessel is out of the territorial water. The responsibility for rescuing the vessel depends on the SAR (search and rescue) area in which the vessel is located. This country should provide an immediate response and seek additional assistance if required. If the vessel is in the SAR area of a third country. Several actions can be contemplated: • Communicate the situation to that third state to ensure that it is alerted to the situation and has control of the situation. • Alert other actors to the possibility of supporting the third country in the operation.
Traceability	The Ship Alert Security System when activated, transmit a ship-to-shore security alert to a MS competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised.
Inputs Summary	• Security alert. • Plans and SOPs.
Output Summary	• Support to decision making. • Communications. • Record events. • Database feed for history log and lessons learned.
Potential improvements	• A common system for rapid operational/ tactical planning and co-ordination of assets reaching across sectors and borders. • Common correlation services. • Improvement of availability of information. • Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). • Common standard operating procedures across sectors and borders. • Common entity services (as many as possible) across sectors and borders. • Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. • Common rules for history input to e.g. databases.

6.10 Use Case ID 9

Table 17

Use Case ID 9	Description
Goal	Detection and behaviour monitoring of IUU listed vessels.
Operational situation/ Trigger	Surveillance of EU waters and ports, increased behaviour monitoring when target is found to be listed as IUU vessel.
Lead Actor(s)	Fisheries Control.
Supporting Actor(s)	Defence, General Law Enforcement, Border Control, Customs.
Activity category	Baseline.
Post-conditions	Vessel refused port services, landing of fish, blockage of landed cargo.

Failure Outcomes	Failure	Outcome	Condition leading to outcome
	Failure to detect presence of IUU listed vessel.	1) Illegal fishing activity performed. 2) Weakened deterrent effect for IUU activities.	1) Poor RMP. 2) Poor sharing/ knowledge of IUU list.
	Failure to detect IUU vessel landing in EU port.	1) Depletion of stock. Negative Economic effects. Negative effect on consumer rights. 2) Illegally caught fish will be commercialized. Multiplication of resources needed to trace illegal commercialization following landing.	1) Poor information exchange between actors (e.g. fisheries control and general law enforcement). 2) Poor levels of information security. 3) Poor interagency cooperation.
Flow of Events	Actors should be aware of the existence of the IUU list and have an updated list of IUU vessels. Upon detection of vessel, the vessel is cross checked with the IUU list. Action will be triggered when there is a positive cross check. Action can consist of: • Intensified monitoring for decision making. • Sea inspection to check cargo and activity. • When in port, alert services and landing of cargo.		
Alternative Scenarios	• Intelligence gathering and mapping of organized illegal import chains. • Enhanced monitoring of target vessel activities.		
Traceability	Identify work products, models or documents that this use case is traceable to, for example, business rules, functional requirements, prototypes, etc.		
Inputs Summary	Details on detection (identification) and activity of target. Proposed actions and results of actions.		
Potential improvements	• Common correlation services. • Improvement of availability of information. • Clearer rules for sharing mechanisms inter- and intra-sector (access rights and security levels). • Common standard operating procedures across sectors and borders. • Common entity services (as many as possible) across sectors and borders. • Sharing of best practises and results in anomaly detection and risk analysis. Applies cross sectors and borders. • Common rules for history input to e.g. databases.		

7 Nature of the information exchange

7.1 General

Clause 7 defines the nature of the information exchange by describing the maritime surveillance high level activities, the core category of information involved as well as the condition of exchange.

7.2 Potential cross sector information exchanged

7.2.1 General

Clauses 7.2.2 to 7.2.4 below provide a list of information type managed by the different sectors identified in clause 6 and which presents an interest for cross-sector exchange using CISE. This list is not exhaustive and does not impose a structuration of the information.

7.2.2 Category A: Maritime Traffic Data

Table 18: Identified Maritime Traffic Data for exchange

Information type ID	Information type
A.1	**Ship positional data (NEAR REAL TIME)**
A.1.1	Ship position reports data
A.1.1.1	Commercial ships position reporting (including fishing vessel's AIS reports)
A.1.1.2	Fishing ships VMS position reporting
A.1.1.3	Military ships position reporting data
A.1.1.4	Governmental ships position reporting data (law enforcement missions)
A.1.1.5	Other position reporting ships (yachts, etc.)
A.1.2	Ship detection data (non-cooperative position data)
A.1.3	Fishing Activity additional near real time data
A.2	**Ship voyage data (actualized at every Port call or for the whole journey of goods)**
A.2.1	Voyage-related Route data
A.2.2	Voyage-related Goods on board data
A.2.3	Cargo Logistic and Customs Data (for their whole journey, possibly several ships/port Calls)
A.2.3	Voyage-related Persons on board data
A.2.4	Voyage-related Fishing data
A.3	**Ship data**
A.3.1	Ship Characteristics (PERMANENT)
A.3.1.1	Commercial ships Characteristics (PERMANENT)
A.3.1.2	Fishing ships Characteristics (PERMANENT)
A.3.1.3	Other ships (yachts, etc.) Characteristics (PERMANENT)
A.3.2	Ship ownership and operation data (UP-DATED)
A.3.2.1	Commercial ships ownership and operation data
A.3.2.2	Fishing ships ownership and operation data
A.3.2.3	Other ships (yachts, etc.) ownership and operation data
A.3.3	Ship identification data (UP-DATED)
A.3.3.1	Commercial ships identification data
A.3.3.2	Fishing ships identification data
A.3.3.3	Other ships (yachts, etc.) identification data
A.3.4	Ship Historical data
A.3.4.1	Commercial ships Historical data
A.3.4.2	Fishing ships Historical data
A.3.4.3	Other ships (yachts, etc.) Historical data
A.4	**Other non-permanent off-shore infrastructures (Sea positioned objects)**
A.4.1	Off-shore rigs data (position, operations, goods and persons on board, characteristics, ownership and operations, identification, historic, etc.)
A.4.2	Energy production plants (above or below water) idem
A.4.3	Fish farms, fish cages (idem)
A.4.4	Dredging barges, floating cranes, etc.

7.2.3 Category B: Maritime Geospatial Data

Table 19: Identified Maritime Geospatial Data for exchange

Information type ID	Information type
B.1	**Charts and Maps (permanent data)**
B.1.1	Hydrographical maps (standard mandated)
B.1.2	Maritime infrastructures
B.1.3	Meteorological maps (winds, rain, squalls, visibility, etc., per season)
B.1.4	Oceanographic maps (tides, wave height, direction, period) per season
B.1.5	Legal maps (SRR, EEZ, TW, ICES areas, RFMO areas, etc.)
B.1.6	Marine resources (exploited)
B.1.7	Marine resources potential
B.1.8	Remnant pollution (from shore, from wrecks, etc.)
B.1.9	Possible seabed hazards (incl. possible ancient mines, wrecks with dangerous goods, dumped ammunitions, etc.)
B.1.10	Protected Areas

Information type ID	Information type
B.1.11	Protected/endangered species
B.2	**Dynamic data**
B.2.1	Meteo-oceanic data
B.2.2	Biochemical data
B.2.3	Real Time Closure (RTC) of fishing areas

7.2.4 Category C: Maritime Event Management

Table 20: Identified Maritime Event Management Data for exchange

Information type ID	Information type
C.1	**Resources localization for Maritime interventions**
C.1.1	Position and tracking of assets (ships, aircrafts, etc.)
C.1.2	Characteristics of assets
C.1.3	Contact details of assets
C.1.4	Ports of refuge data
C.1.5	Pre-established SAR Coordination Plans
C.2	**Data on demand**
C.2.1	radar tracks from coast or ships
C.2.2	EOS pictures from coast or ships
C.2.3	radar tracks from airplanes or drones
C.2.4	EOS pictures from airplanes or drones
C.2.5	Satellite Imagery - RADAR
C.2.6	Satellite Imagery - OPTIC
C.2.7	Acoustic signature(s), voice recordings…
C.2.8	Underwater detection and tracking (sonar)
C.2.9	Electromagnetic signal localization and interception (phones, VHF, etc.)
C.2.10	Meteorological forecast/very specific zone
C.2.11	Samples
C.2.12	Intelligence
C.3	**Security of commercial shipping**
C.3.1	Security alert
C.3.2	Security measures taken
C.3.3	Security certification (ISSC, initial ship sec asset report, last verification report, expiring date)
C.3.4	Company security officer
C.3.5	Ship security officer
C.3.6	Security level
C.3.7	Declaration of Security (DoS)
C.3.8	Ship Security Plan (ISPS)
C.3.9	Ship specific security equipment
C.3.10	Alert/ expiry of ISSC (incl. possible grace period)
C.4	**Search and rescue**
C.4.1	Accident/ incident report
C.4.2	Information associated with other distress situations
C.4.3	Ship security and evacuation equipment (slides, life rafts, etc.)
C.4.4	Rescue plans
C.4.5	Evacuation plan
C.4.6	Passengers and crew lists, Survivors found and rescued
C.5	**Ship-borne pollution response**
C.5.1	Pollutant
C.5.2	Anti- pollution resources
C.5.3	Position and/or extent of pollution on/ above/in the sea
C.5.4	Initial pollutant properties
C.5.5	Emulsion properties
C.5.6	Behaviour of pollutant (floats, sinks, evaporates, dissolves, etc.)
C.5.7	Hazards related to the polluting substance
C.5.8	Characteristics of pollution
C.5.9	Source and cause of pollution
C.5.10	Drift of pollution (past/expected)
C.5.11	Impact forecast

Information type ID	Information type
C.5.12	Identity of observer/reporter. Identity of ships on scene
C.5.13	Action taken
C.5.14	Photographs or samples
C.5.15	Names of other states and organizations informed
C.5.16	Pre-arrangements for the delivery of assistance
C.5.17	Intervention resources availability and location
C.5.18	To where assistance should be rendered and how
C.5.19	Interfacing with existing Sector Information portals
C.6	**Maritime Law Enforcement**
C.6.1	Maritime Illegal migration
C.6.2	Organized crime
C.6.3	Terrorist threat
C.6.4	IUU Fishing
C.6.5	Maritime Customs frauds
C.6.6	navigation safety infringements
C.7	**Anti-Piracy**
C.7.1	Initial Attack Report (IMO MSC1/circ 1333 [i.2])
C.7.2	Follow-up Attack Report (IMO MSC1/ circ 1334 [i.3])
C.7.3	Information about past piracy incidents (location, time, description of boats, what happened, etc.)
C.7.4	Maps (annotated) of piracy incident distribution per season
C.7.5	Maps of ship traffic distribution per ship type and per season
C.7.6	Shore bases of pirates and their current activity level
C.7.7	Actual locations of merchant and fishing ships
C.7.8	Actual locations of naval patrol ships and a/c
C.7.9	Pirate ships/ attacks locations
C.7.10	Locations of bases of patrol assets
C.7.11	Maps (annotated) of past non-piracy incidents distribution per season (trafficking, smuggling, illegal fishing, terrorism, etc.), not only on sea but also on the shores
C.7.12	Data base that couples ship ID to ship description
C.8	**Shore-borne Pollution incident**
C.8.1	Environmental INCIDENT (BASIC DATA)
C.8.2	Oil recovery and surveillance
C.8.3	Sample collection
C.9	**Sea bed threat neutralization**
C.9.1	Explosive ordnance device detection/neutralization
C.9.2	Required restricted area for shipping
C.10	**Coastal Evacuation (additional to C4)**
C.10.1	Reasons of the evacuations (tsunami, etc.)
C.10.2	Pre-existing contingency plans
C.10.3	Decisions done
C.10.4	Alarm systems
C.10.5	Reaction actions
C.10.6	Movement to an area of refuge or an assembly station means
C.10.7	Transportation systems put on place
C.10.8	Evacuation orders
C.11	**Humanitarian assistance and disaster response by sea (additional to C4)**
C.11.1	Pre-existing contingency plans
C.11.2	Hazards mapping and tracking (chemical or nuclear clouds, etc.)
C.11.3	Sealift planning and management
C.11.4	Hospitals
C.11.5	Medical care
C.11.6	Relief aid logistic management

7.3 Core information types

A high-level information categorization, or Core information types, that structures the information described in the list provided in clause 7.2 is as follows:.

- Maritime Object:
  - Vessel.
  - Operational Asset.
  - Cargo.
- Agent:
  - Person.
  - Organization.
- Event:
  - Movement.
  - Action.
  - Incident.
  - Anomaly.
- Risk.
- Meteo-Oceanographic Condition.
- Location.
- Document.

Annex A:
Relationship of Use Case ID CR CDM 001 with Use Case ID EUCISE2020/CoopP

Table A.1 below provides a mapping between the use cases described in the present document and use cases defined in the EUCISE2020 and CoopP projects.

Table A.1

CR CDM 001 Use Case ID	EUCISE2020/CoopP Use Case ID
Use Case ID 1	Use Case 13b
Use Case ID 2	Use Case 13c
Use Case ID 3	Use Case 25b
Use Case ID 4	Use Case 37
Use Case ID 5	Use Case 44
Use Case ID 6	Use Case 57
Use Case ID 7	Use Case 70
Use Case ID 8	Use Case 85
Use Case ID 9	Use Case 93

History

Document history		
V1.1.1	January 2021	Publication