SWJ – use case

Source:

> [1] ETSI ISG (Industry specification group) on European Common Information Sharing Environment Service and Data Model (CDM); Use Cases definition; Release 2. ETSI Group Report (GR) CDM 001 v.2.1.1, 11-2022. https://www.etsi.org/committee-activity/activity-report-cdm

The event type selected is an Anomaly. According to [1], this event is typical in the case of detecting anomalies and conducting risk assessment cross-border with multi-Member State exchanges. The report mentions that this represent a potential improvement with sharing anomalies and detected risks throughout sectors and borders.

The table below lists the use cases described in [1]. The highlighted use cases (in green) are those that can be used as an example.

Table: Use cases based on CISE and eCISE.

Use Case	Description
1	Inquiry on a specific suspicious vessel (cargo related).
2	Inquiry on a specific suspicious vessel (crew and ownership related).
3	Investigation of antipollution situation (law enforcement).
4	Monitoring of all events at sea in order to create conditions for decision making on interventions.
5	Request for any information confirming the identification, position and activity of a vessel of interest.
6	Knowledge of surveillance capacities of partner authorities in a given sea area to plan basic tactical surveillance.
7	Suspect Fishing vessel/small boat is cooperating with other type of vessels.
8	Anti-Piracy Maritime Surveillance and free navigation control: Merchant vessels at sea (outside Territorial waters) sends an alert that it is under Piracy attack.
9	Detection and behaviour monitoring of IUU listed vessels.
10	Detection and behaviour monitoring of illegal border crossing activities.
11	Detection and behaviour monitoring of illegal border crossing activities along a river or in a river estuary.
12	Search and rescue after illegal border crossing activities.
13	Detection and behaviour monitoring of illegal smuggling activities on land border/river.

The selected use cases represent a typical scenario chain, in the following sequence: 4, 5, 1, 3. This could start by monitoring events in a particular dense or risky zone. Then an anomaly is raised and request of information regarding elements concerned by the anomaly, inquiry on a particular vessel involved, investigation on an antipollution situation.

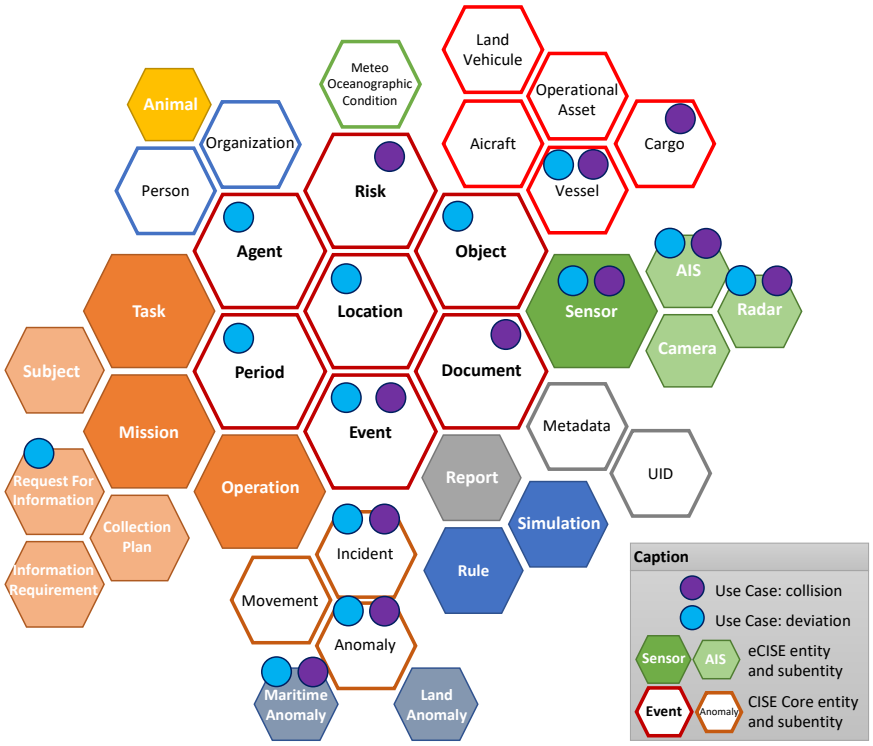


Figure: CISE and eCISE entities used by the use cases. Regarding the specifications, note that some entities contain other entities (e.g. RFI—Request for information requires the Agent performing the request and the Period of time covered by the request).

Use case #1 – Anomaly triggering requests for information

Summary of the use case: an anomaly is triggered by a legacy system of one Member State. The anomaly is located on a border zone with another Member State. The anomaly is passed to the other Member State's maritime surveillance authority which analyze it. The analysis will then trigger other complementary exchanges retrieving interesting information.

Technical architecture. In an attempt to simplify our example, let us consider that each maritime authority has a legacy surveillance system that monitors maritime traffic within their national waters and have a CISE system that records the exchanges they have with other authorities that are members of the CISE network. The legacy system stores, for example vessel characteristics and positions while the CISE system stores information sent to or received from other maritime authorities (knowing that some information may be fully redundant with existing within the legacy system). Both Member State's maritime authorities are also connected to the CISE exchange network, allowing to exchange messages and information.

Title of the use case: a ship with supposed damaged equipment is leaving traffic lane in a border area between two CISE partners (such as two Member States).

Context of the use case: the situation is events happening in a location within the proximity of a maritime border between two Member States (Country 1 and Country 2) were both Member State could be called upon for intervention on possible search and rescue operations. Within each of these member states a maritime authority is monitoring the area (MAC1—Maritime Authority of the first country—and MAC2—Maritime Authority of the second country).

Initial setup: A vessel has previously traveled across the monitoring area of MAC1. During this voyage, the vessel has had two severe technical difficulties (engine and navigation equipment failures) but both were solved without assistance. As these difficulties were announced using radio MAC1 has a trace of them within their legacy system. Later, the vessel is returning home and is navigating again within the monitoring area of MAC1 (see figure with map below). While navigating this vessel has had issues which have raised anomalies such as vessel deviating from route (exiting a monitored traffic lane) and vessel with erratic movements. However, as these anomalies represented only temporary situations and as there was no consequence the vessel did not alert the authorities and the authorities dismissed the anomalies (and the local legacy surveillance system recorded them). This represents a typical situation of a vessel having technical difficulties that are annoying but not necessarily critical.

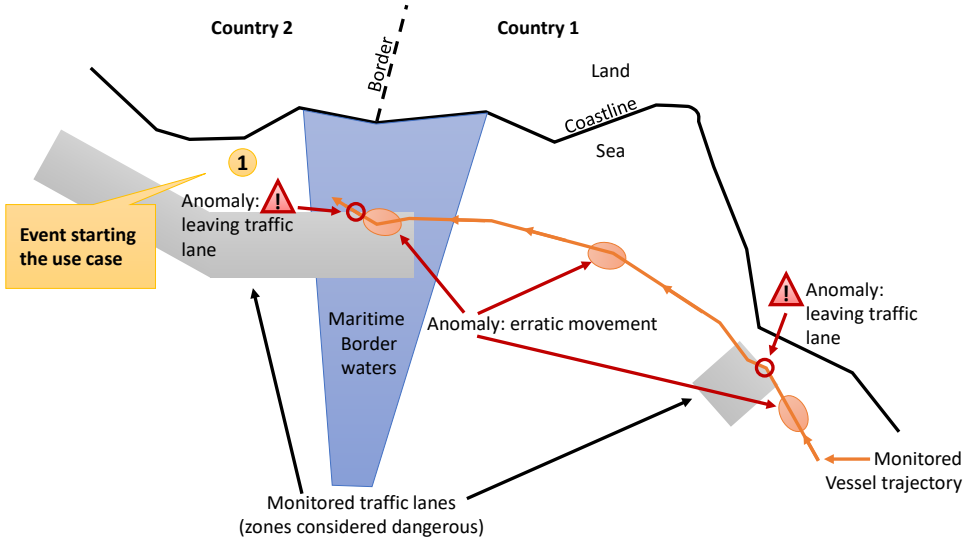


Figure: (initial setup) a vessel with erratic movements and exiting twice a monitored traffic lane.

The rest of the use case follows the BPMN schema in the following figure.

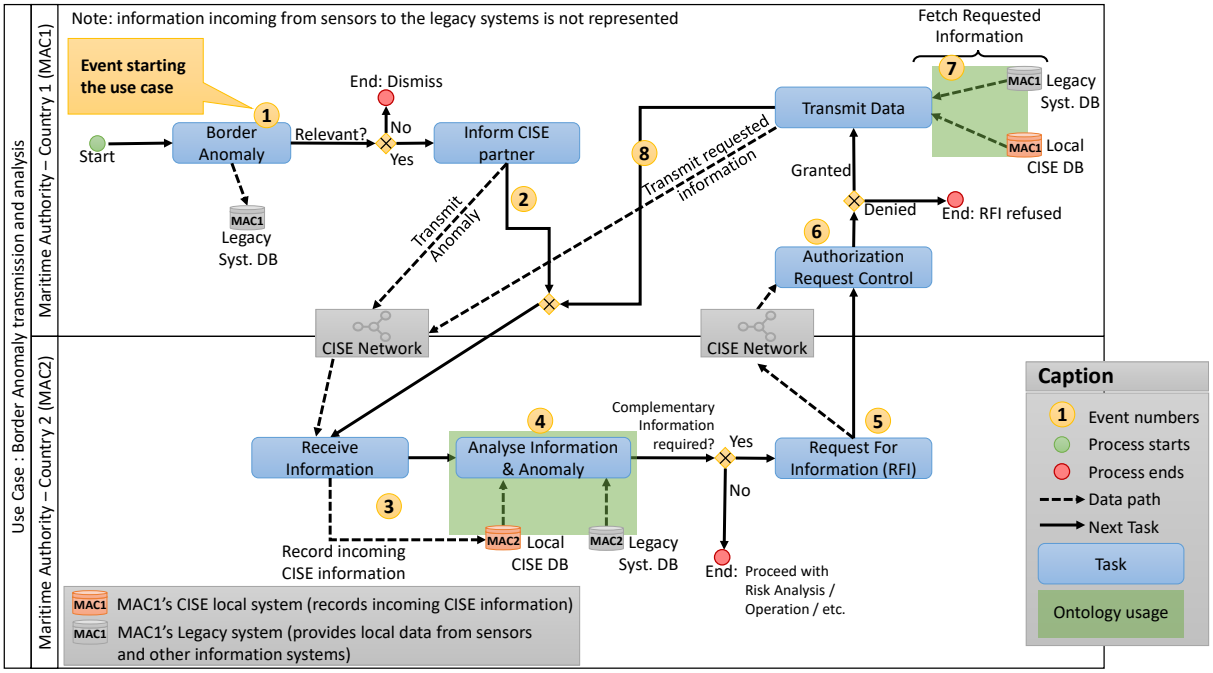


Figure: use case process in BPMN notation (events are noted with numbers)

Unfolding the use case. Later as the vessel is crossing a maritime border within a traffic lane, the legacy system raises again similar anomalies (see event 1 in BPMN figure). The maritime authorities (MAC1) decide to warn their neighboring partners (MAC2) were the vessel is heading and send the anomalies through the CISE network (see event 2). The CISE message and the associated information is received by the other maritime authority (MAC2) which processes the data and stores it in the local CISE system (3). In order to process this information, the maritime authority (MAC2) will have to analyze information related to the received CISE message, previously received CISE messages (that would concern the same vessel or the same location or even similar anomalies) as well as data related to the same elements but within their own legacy system (4). This step happens between two very different systems although both have similar data and may produce or record CISE data. Describe here how the ontology helps. If more information is required, the maritime authority (MAC2) may request information (5) using CISE to the maritime authority that initially provided the anomaly (MAC1). Upon receiving and accepting the information request (6), the first maritime authority (MAC1), can fetch data from (7) both their legacy system and previous CISE messages (that would concern the monitored vessel, as this vessel might have been in similar situations and would have generated alerts and other messages between MAC1 and a third maritime authority). Describe here how the ontology helps. Then information gathered is then transmitted (8) to the requesting maritime authority (MAC2) that now has an enhanced awareness and more information in order to decide which action take (or they could request even more information).

CISE (eCISE) elements generated. During the use case, the following eCISE elements are triggered either automatically (by the legacy system that then generates an eCISE message) or manually (by the operator of one of the two maritime authorities MAC1 or MAC2):

- Anomaly.MaritimeAnomalyType.VesselWithErraticMovements: an Event (anomaly) that represents a vessel sailing with an erratic pattern. This event would be triggered 3 times (during the initial setup). Events are saved in the legacy system and will be sent as CISE messages to MAC2 in reply to the request for information.

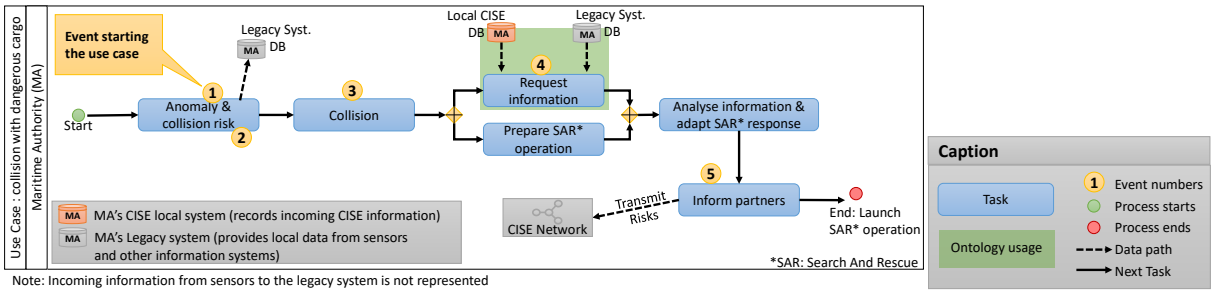
- Anomaly.MaritimeAnomalyType.VesselDeviationFromRoute: an Event (anomaly) that represents either a vessel deviating from a route or from a shipping lane. This event is triggered a first time but dismissed because the vessel quickly returned within the traffic lane. It will be triggered a second time and will initiate the use case. Events are recorded in the legacy system of MAC1 and the second will be sent to MAC1 as a CISE message. Later when replying to the request for information, MAC1 will send the first one as a CISE message.
- Anomaly.MaritimeAnomalyType.VesselEnteringRoute: this Event (anomaly) is triggered when the vessel will be re-entering the shipping lane. This event is recorded within MAC1's legacy system. It will be sent to MAC2 when replying to the request for information.
- RequestForInformation.Requestor(Agent): MAC2 upon analyzing the initial CISE message received from MAC1 will request for complementary information regarding the vessel. This request will have as Requestor MAC2, the vessel (an Object) as InformationRequirement and a ValidityPeriod long enough to have relevant information. All authorities registered to MAC2's requests will receive it and may replay with information. For simplicity, only MAC1 will reply.
- MaritimeSafetyIncidentType.EngineFailure: an Event (incident) used to record an incident at sea. This event will be generated by an operator of MAC1 during the initial voyage of the vessel to keep track of the technical difficulty the vessel had. This event is stored in MAC1's legacy system and will be sent to MAC2 as a CISE message during the reply to the information request.
- MaritimeSafetyIncidentType.NavigationEquipementFailure: same as above.

Use case #2 – Incident revealing unnoticed information

Title of the use case: vessel collision involving unexpected and unknown dangerous cargo.

Context. A maritime authority of a member state monitors border regions of its national waters where there are shipping lanes. A vessel in transit within a shipping lane will collide in an unpredicted manner with another vessel.

Initial setup: a vessel transporting cargo has had issues in declaring the cargo content. This content, although dangerous was not declared correctly. The maritime authority of the port of origin of the vessel pushes the information that the vessel has a cargo composed of dangerous goods within a report through the CISE network to other member states whose monitored waters will be crossed by the vessel during its voyage. This type of information unless flagged with a very high priority can easily go unnoticed.



Note: Incoming information from sensors to the legacy system is not represented

Figure: use case process in BPMN notation (events are noted with numbers)

Scenario. The vessel transporting the dangerous goods is navigating in a shipping lane. Unexpectedly it collides with another vessel. The monitoring maritime authorities were able to monitor the collision with their legacy system: first an anomaly was generated (1) which escalated into a risk (2) and then escalated in a collision incident (3). In order to anticipate and initiate as soon as possible an adapted search and rescue operation, the maritime authority request information regarding the vessels taking part in the collision (4). The legacy system will return general information about both vessels, but the local CISE system will return the cargo document. Describe here how the ontology helps. With this information, the maritime authority will adapt its search and rescue response and preventively push to the CISE partners (5) potential risks related to dangerous goods and the collision (pollution and fire risks—which could potentially escalate in an explosion risk if more information can be gathered regarding the cargo).

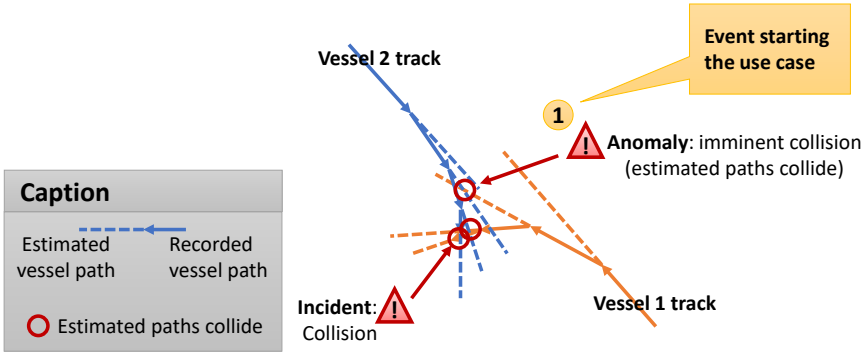


Figure: tracks of the vessels involved in the use case.

CISE (eCISE) elements generated. During the use case, the following eCISE elements are triggered either automatically (by the legacy system that then generates an eCISE message) or manually (by the operator the maritime authority) but also possibly returned by the system (legacy or CISE) in reply to queries:

- Vessel (Vehicule): is a maritime moving object (Object). A vehicule has a cargo (Vehicule.VehiculeCargo). A Cargo has a type, but this type does not represent the dangerousness level. Vessels (Objects) will represent the moving objects tracked by MA's legacy system and reported by the sensors (whether radar or AIS).
- Anomaly.MaritimeAnomalyType.ImminentCollision: an event (anomaly) that can be raised automatically by monitoring systems upon imminent collision between large generally poorly maneuverable vessels whose movements can be anticipated by algorithms. The event is generated by the MA's legacy system and saved within its database.
- Risk.RiskType.COLLISION: an event (risk) raised automatically with certain anomalies such as an imminent collision. Risks are events that are escalated from anomalies. This event is generated by MA's legacy system and saved within its database.
- MaritimeSafetyIncident(incident).MaritimeSafetyIncidentType.Collision: an event (incident) representing a collision between two objects such as vessels. Incidents are events that are escalated from risks. This event is generated by MA's legacy system and saved within its database. This event will be converted to a CISE message to be propagated to the CISE network.
- CargoDocument(Document).CargoDocumentType.NotificationOfDangerousGoods: a cargoDocument (a Document) that describes the cargo of a vessel (such as goods transported). The document has been generated by a CISE partner and is saved within MA's CISE message database. Il will be retrieved when the MA will require information to prepare the SAR—Search and Rescue—operation following the collision event.
- Cargo.objectDescribedByDocument: Cargo (an Object) that is attached to a Vessel (also an Object) is the freight transported by a vessel. It can be described by a document (such as a manifest). The cargo is
- Risk.RiskType.POLLUTION: an event (risk) representing a potential pollution, such as a pollution at sea.
- Risk.RiskType.FIRE: an event (risk) representing a potential fire, such as a fire on board a vessel.

A faire (Ronan) : détailler les éléments CISE ci-dessus comme dans le premier use case.

Advantages compared to existing solutions

Current systems would require the development of several query interfaces and query vocabularies to manage existing systems (legacy systems) on one side and on the other, another interface would have to be designed either to query past data that was received from the CISE network. A costlier solution would be the design of an interface that would directly integrate CISE information within the legacy system which, in terms of data sovereignty, might not be recommended by some Member States.

Our solution only requires a mapping with each existing legacy system database and a unique generic mapping with a system that would store CISE messages (and that could be identical across all CISE members).

The CISE model is based on a XML text data serialization. The authors in [Riga-21] have demonstrated the it was possible to query CISE data with a SparQL endpoint. We extend this proposition showing how such an endpoint could be extended to query both CISE and existing legacy systems in order to retrieve data not only exchanged through the CISE network but also within the existing legacy system.

Related projects are project members of the BES cluster (Border External Security), such as: TressPass, Mirror, ITFlows, Perceptions, Persona, Effector, D4Fly, BorderUAS, iMars, Roborder, Isola, Nestor, Promenade, Criteria, Aligner, Odysseus, Melchior, I-Seamore, Flexi-Cross.