Appendix 5
to Tender Specifications

Requirements for the Provision of Services

- **STAR ABM Corrective Maintenance and Operational Support**
- **STAR ABM Release 3.0**

Invitation to tender No. EMSA/OP/05/2017 for ICT services related to Software Maintenance and further Development of the Automated Ship Behaviour Monitoring and Anomaly Detection application (STAR ABM)

EMSA

Contents

1 Introduction

The aim of this document is to define the Requirements for the services that the Contractor shall provide to EMSA within the scope of the **Module 1** and **Module 2** of the EMSA/OP/05/2017 Framework Contract (FWC).

The Tendered shall take into account also the definitions and requirements provided in the Appendices 1, 2, 3, and 4 to the Tender Specifications.

1.1 Scope

Scope of the FWC is the maintenance, operational support and further development of the Automated Behaviour Monitoring (ABM) software application, including the STAR ABM Release 3.0.

The ABM application was developed as part of the IMDatE system at EMSA. The technical name of the ABM component is “SA-VAS”, a module that interfaces with the central data processing system of IMDatE (IMDatE Core) and its database. The main functions of ABM are the analysis of the ship position data stream and the alerting of the user under particular conditions.

This document contains the following main sections:

- **Overview of IMDatE and ABM**: an overview of the IMDatE system and the Automated Behaviour Monitoring (ABM) application;
- **Corrective Maintenance**: the software maintenance services to be provided within the scope of Module 1;
- **Operational Support**: the support services to be provided within the scope of Module 1;
- **STAR ABM Release 3.0**: the requirements of the future release of the ABM application to be developed within the scope of Module 2.

1.2 Reference Documentation

This document provides an overview of the ABM components.

For more technical details on the ABM software and the whole IMDatE system refer to the following documents:

- IMDatE - SA-VAS technical description
- IMDatE - Technical Design Specification
- IMDatE - Template Environment
- IMDatE - Interface Control Document
- ABM User Manual
- SA-VAS sample SoapUI projects (Template and Surveillance Instance services)
- SAVAS-MPAE Interfaces

The source code of the ABM components is available except for the underlying data processing and monitoring engine (MPAE) which is a proprietary library of the Company CLS[1].

[1] https://www.cls.fr

1.3 Requirements structure

A requirement comprises a list of functionalities to be implemented, or services to be provided, by the Contractor.

Each requirement in this document has an identification based on this structure: REQ-*MOD*-{progressive number}, where *MOD* is either MOD1 for Module 1 and MOD2 for Module 2 of the FWC, e.g. “REQ-MOD2-11”.

2 Overview of IMDatE and ABM

The ABM service provides the users the possibility to create a ship monitoring task, called *Surveillance instance* or simply *Surveillance*, that continuously runs as a background process. A Surveillance instance analyses the behaviour of the ships based on their positions, provided by the ship tracking systems available at EMSA. When a Surveillance instance is configured, the user can define a set of criteria that allow ABM detecting a specific ship behaviour and thus triggering an alert. Alerts reports are then dispatched to the user on several channels (web application, mobile app, e-mail).

The logical diagram showing the interaction between ABM (SA-VAS) and the IMDatE Core modules is depicted in Figure 2.1.

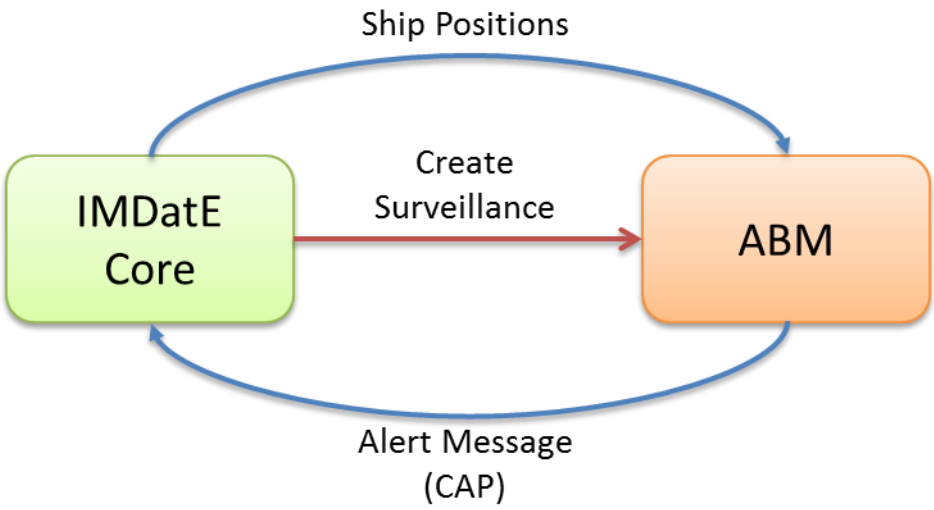


Figure 2.1 – IMDatE Core-ABM Interaction Diagram

The “Ship Position” message stream constantly provides to ABM the input data for behaviour analysis purposes. Through a graphical web interface the user creates new Surveillance instances or edits existing ones. The Surveillance parameters are then communicated to ABM which accordingly starts the monitoring tasks.

ABM triggers an Alert as soon as the behaviour of a ship matches the criteria set by the user. Under these circumstances an Alert message is generated and sent back to the IMDatE Core. The format of the Alert message is CAP[2].

2.1 Surveillance

In the current system, the user creates a Surveillance instance in the IMDatE web application. The user selects the behaviour type from a list of pre-defined algorithms, called *templates*. The user then sets the generic criteria (e.g. Area of Interest – *AOI*, Vessels of Interest - *VOI*) and more specific configuration parameters that define the characteristic of the ship behaviour (see Figure 2.2). See also the ABM user manual for further details.

[2] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

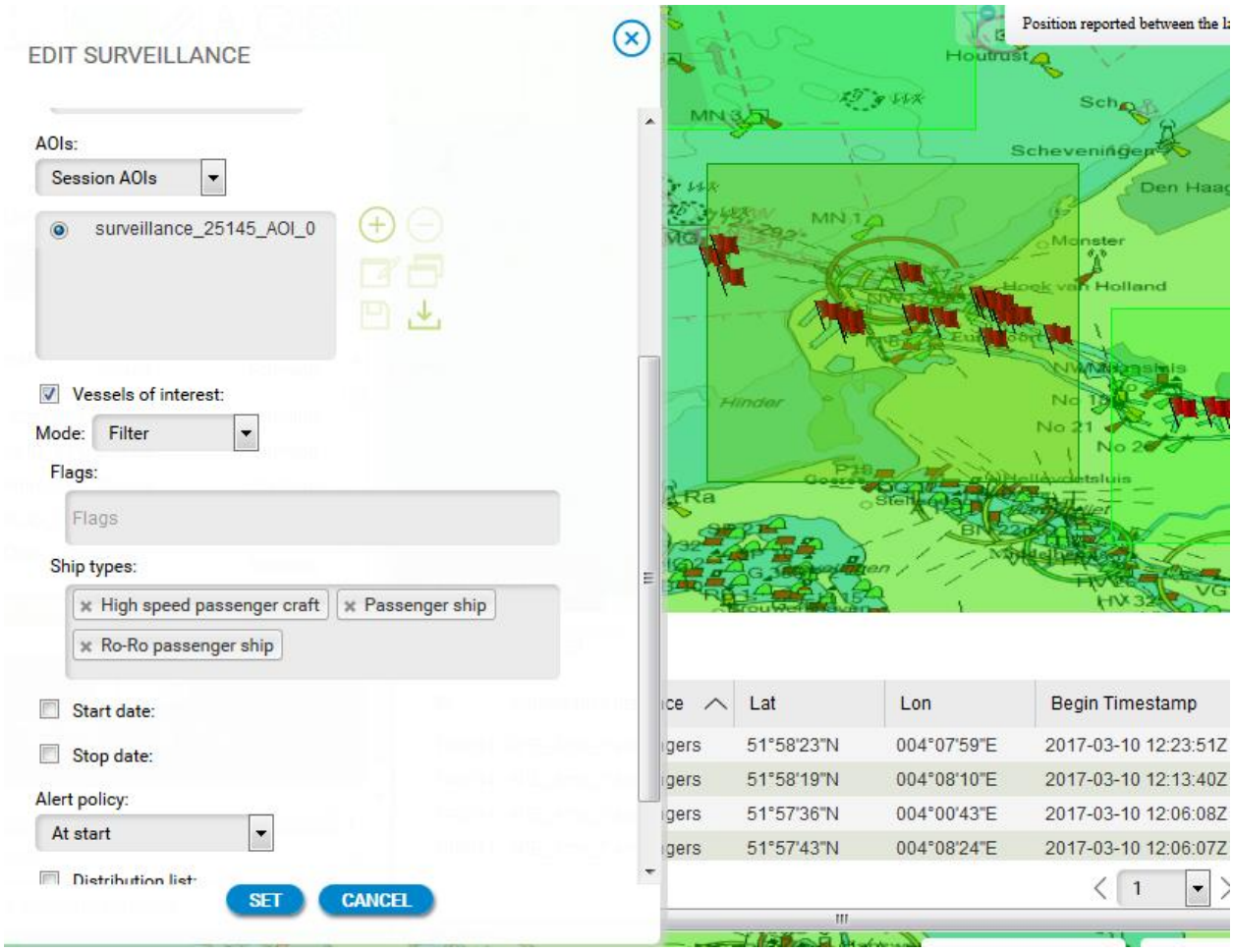


Figure 2.2 - ABM configuration form

All Surveillances have the following generic configuration parameters (the mandatory parameters are in bold):

- **Name**
- Description
- **Type**
- **Area of Interest (AOI)**
- Vessel of Interest (VOI)
- Activation Period
- **Alert Policy**
- Distribution List
- E-mail Notification

The Name helps the user identifying the Surveillance instance and it typically indicates the aim of the monitoring, e.g. “High Speed in Lisbon Port”.

The Surveillance Type indicates the type of ship behaviour that the user wants to detect. Each Surveillance Type corresponds to an algorithm template implemented by ABM. The list of ABM Surveillance types is shown in Figure 2.3.

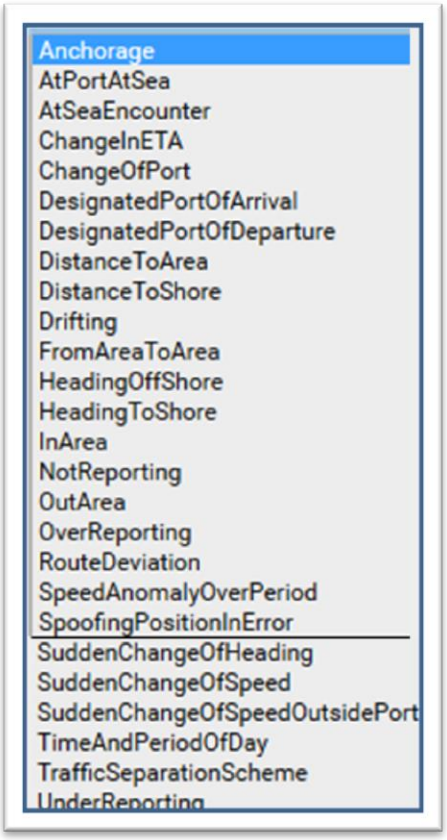


Figure 2.3 - ABM Types of Surveillance

The AOI sets the geographical boundary of the Surveillance.

If a ship behaviour matches the Surveillance criteria, ABM triggers an alert that is displayed on the map of the IMDatE web application. The Alert Policy, shown in Figure 2.4, indicates at which moment ABM should trigger an Alert with respect to the event, e.g. “At end” only raises an Alert when the ship stops behaving in a particular way.

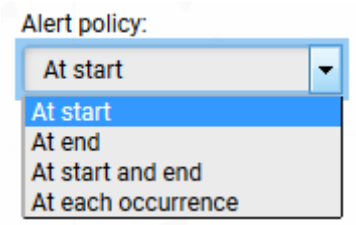
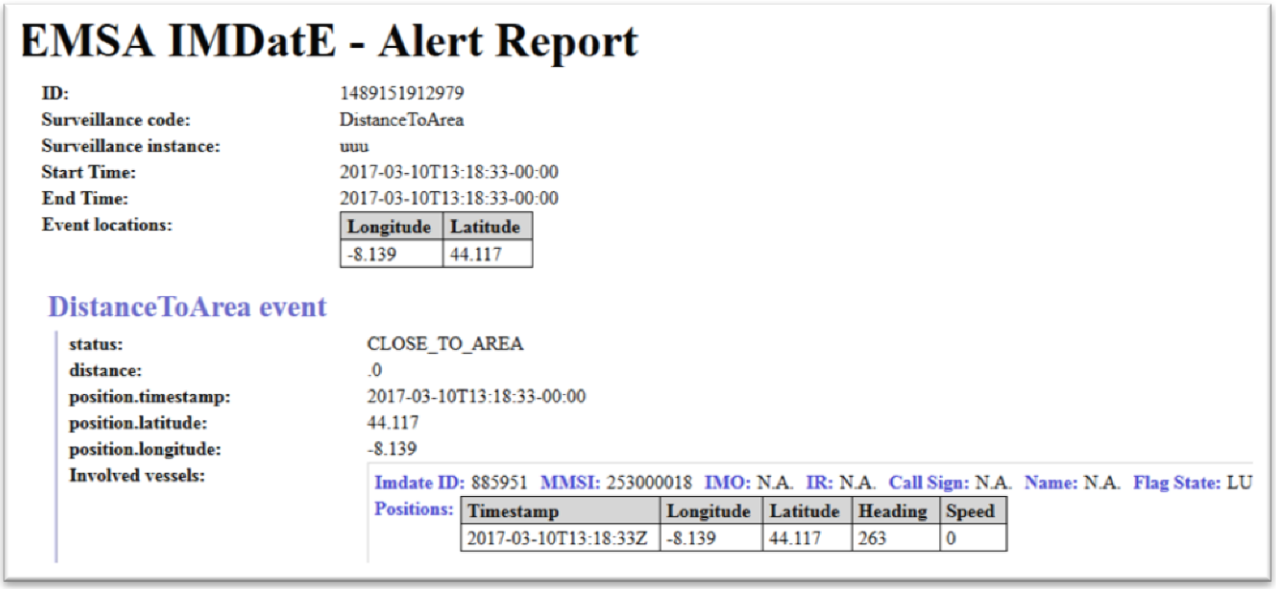


Figure 2.4 - ABM Alert Policy

The Alert can also be dispatched by e-mail, in form of a HTML report, if the user has checked the E-mail notification option. See a sample Alert Report in Figure 2.5.



EMSA IMDatE - Alert Report

ID: 1489151912979
Surveillance code: DistanceToArea
Surveillance instance: uuu
Start Time: 2017-03-10T13:18:33-00:00
End Time: 2017-03-10T13:18:33-00:00
Event locations:

Longitude	Latitude
-8.139	44.117

DistanceToArea event

status: CLOSE_TO_AREA
distance: .0
position.timestamp: 2017-03-10T13:18:33-00:00
position.latitude: 44.117
position.longitude: -8.139
Involved vessels:

Imdate ID: 885951 MMSI: 253000018 IMO: N.A. IR: N.A. Call Sign: N.A. Name: N.A. Flag State: LU

Positions:

Timestamp	Longitude	Latitude	Heading	Speed
2017-03-10T13:18:33Z	-8.139	44.117	263	0

Figure 2.5 - ABM Alert Report

2.2 On-event Surveillance

In addition to the Surveillance requests made by the users through the IMDatE web application, SA-VAS also provides a so called “on-event” Surveillance mechanism.
In this context, an *event* is some kind of maritime related occurrence, for instance the reception of a Port Notification message from a ship which is bound to a EU port.
SA-VAS allows the activation of a series of Surveillance instances linked to a specific event and for a given list of ships. When the event occurs, the running on-event Surveillances generate a Report that is dispatched to the requesting user.

As an example the BlueBelt on-event surveillance reacts to a Notification Message from a ship that has called to a particular port. When the Notification Message is received by ABM, the past Alerts associated to that ship and triggered by the BlueBelt surveillances are collected from the database and delivered to the user by e-mail in form of a BlueBelt report.

2.3 SA-VAS

The SA-VAS module that provides the ABM service is composed of the components shown in Figure 2.6.

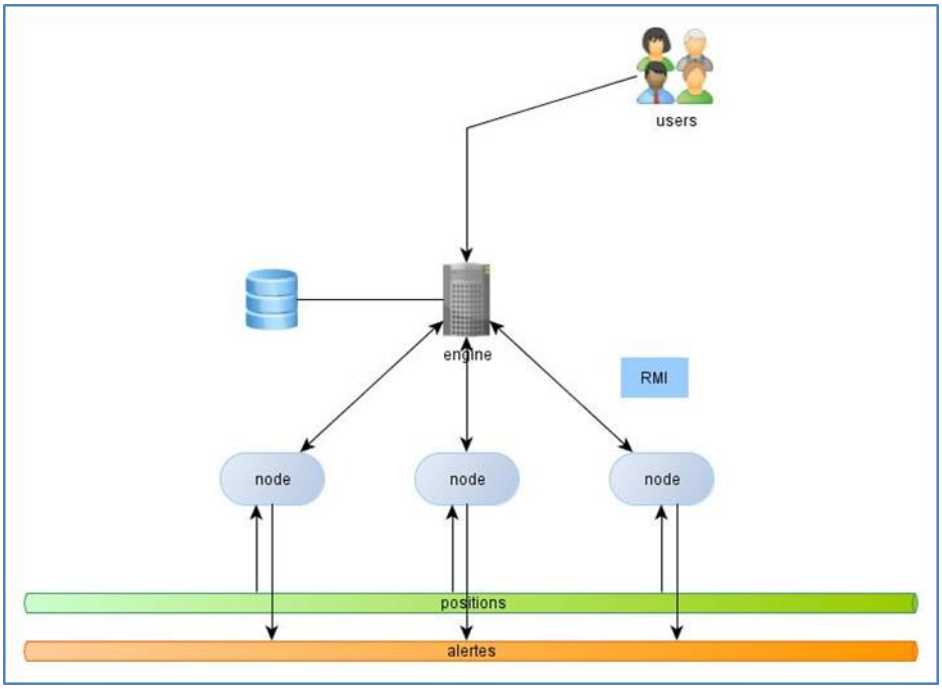


Figure 2.6 - SA-VAS Components

The SA-VAS Engine is responsible for the management of the Surveillances, following the user's input. The tasks of the Engine include the execution of new Surveillance requests, the removal of existing ones and their activation or deactivation.

The SA-VAS Nodes are responsible for the effective processing and analysis of the incoming data stream and the generation of alerts. A user's Surveillance request corresponds to a Surveillance instance running on a physical Node of the SA-VAS platform. The decision of which Node should run a given Surveillance instance is taken by the SA-VAS Engine based on the load of all Nodes at the moment of the Surveillance activation.

The current configuration of SA-VAS in the EMSA Production Environment has 2 Nodes. From a physical point of view, SA-VAS is currently deployed on 2 (virtual) machines of the EMSA data center. One machine hosts the Engine and the first Node. The other machine hosts the second Node (see Figure 2.7).

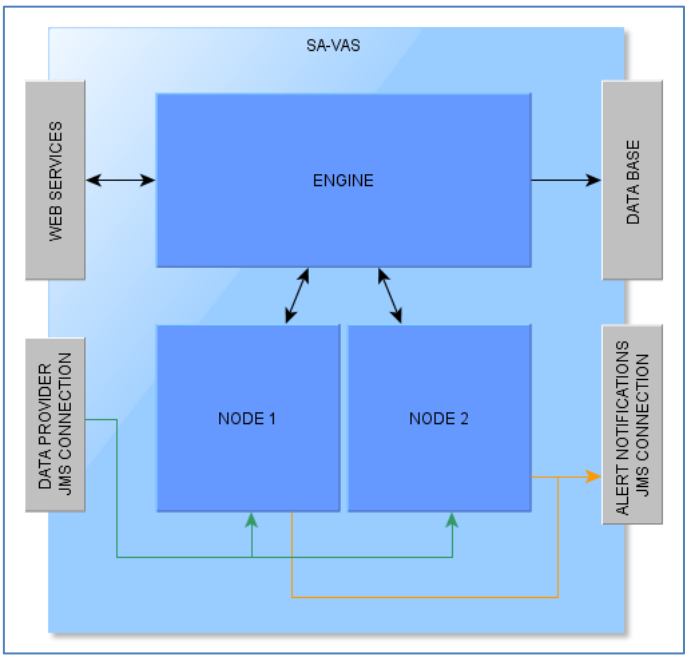


Figure 2.7 - SA-VAS Engine, Nodes and Interfaces

2.3.1 SA-VAS Interfaces

The interfaces between SA-VAS and the IMDatE Core are also shown in Figure 2.7.

The *Data Provider (JMS Connection)* interface receives the incoming data stream from the IMDatE position data processing module, a JMS topic, and distributes the position messages to the Nodes.

The *Alert Notifications (JMS Connection)* interface writes the Alerts generated by SA-VAS to a JMS queue in form of CAP messages.

The other interfaces provide the following services:

Web Services

SA-VAS provides a set of SOAP Web Services[3] for the management of the Surveillance algorithm templates as well as the activation of Surveillance instances. These services are called by the IMDatE Core according to the user requests.

Database

SA-VAS reads and writes on the IMDatE Database through a JDBC connection. The database is used to store the Surveillance algorithms definition (templates), the Surveillance instances, the generated Alerts, and other relevant information.

System Health Monitoring Interface

In addition to the above mentioned interfaces, SA-VAS also provides a JMX-based system health monitoring interface that allows the measurement of real-time performance metrics.

2.3.2 Authorization

An additional interface to an external system is the link between SA-VAS and the Oracle Entitlement Server (OES). OES is responsible for authorizing access to the position data. The authorization call is executed by means of an OES Wrapper Java class which is also considered part of SA-VAS.

[3] See sample SoapUI project in annex.

2.4 ABM Functions provided by the IMDatE Core

The following ABM related functions are currently implemented as part of the IMDatE core, i.e. outside the SA-VAS module:

- Surveillance Management GUI Tool (Web Application)
  - Configuration panel to manage Surveillances (view, create, edit, activate, etc.)
- Alert CAP message processing
  - The reception and analysis of an Alert message sent by SA-VAS in the CAP format
- Dispatch of Alerts
  - The creation and distribution of Alert reports by e-mail and through the getAlerts web service
- SA-VAS Monitoring Console (SMC)
  - The console used by an EMSA Operator to verify the status of the SA-VAS module and intervene to restore the service or prevent malfunctions (see Figure 2.8).

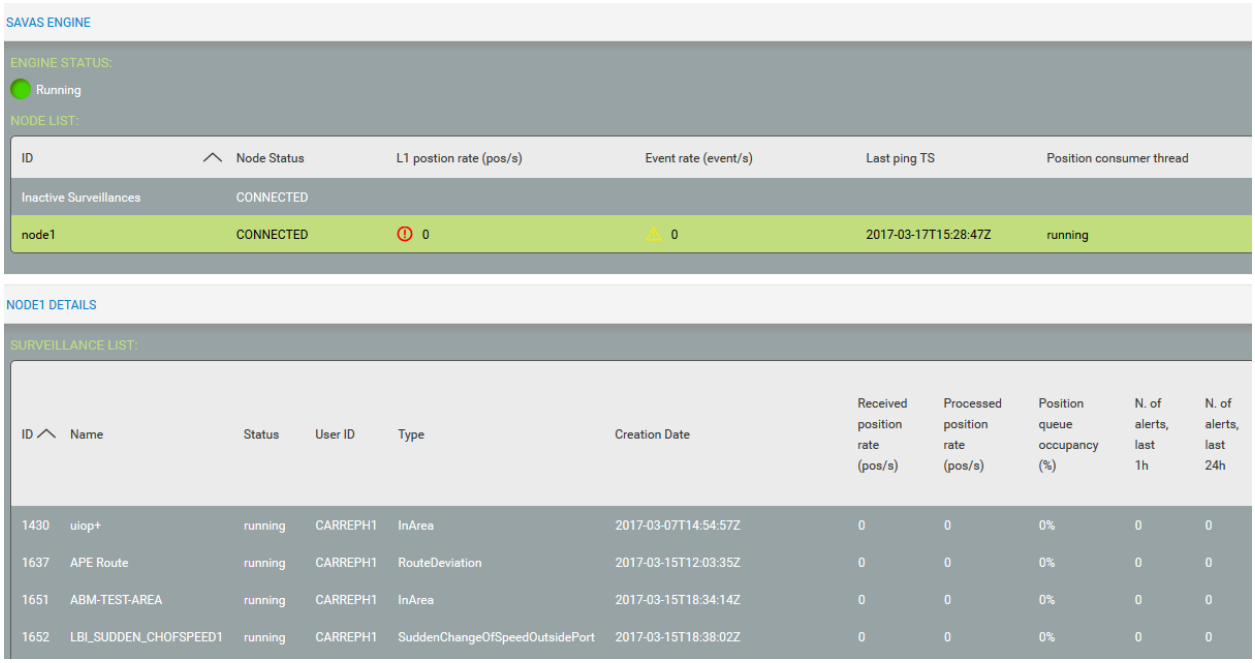


Figure 2.8 - SA-VAS Monitoring Console (SMC)

3 Corrective Maintenance

REQ-MOD1-1	Code Maintenance

The Contractor shall maintain the source code of the ABM (SA-VAS) software module developed for EMSA within the context of the IMDatE project.

The ABM code has been developed in Java (JDK 1.7).

The overall number of lines of code of the most recent version (v. 2.1), including comments and empty lines, is 271,000 lines.

The source code is organized in one Package Manager (RPM) file which also includes the library MPAE and other COTS.

The source code to maintain will be delivered to the Contractor after the signature of the contract. The information provided within this tender about the lines of source code could be slightly different when the contract will be signed.

The Contractor shall set up and configure a complete Development Environment at their premises, including a replica of the interfaces between ABM and external systems (WebLogic topics and queues, OES authorization service, IdM user database) and a position data stream simulator for testing purposes. The cost of the Development Environment and the effort to become familiar with the code to maintain shall be included in this module as part of the fixed yearly price.

The Contractor shall provide the code maintenance services (bug fixing) within 1 month from the signature of the contract.

REQ-MOD1-2	STAR ABM Documentation

The Contractor shell maintain and update the following documents to reflect the changes included in the latest delivery:

- Technical Design Documents
- Interface Control Document
- Operational and Maintenance Manual (including Service Monitoring)
- Incident Handling Procedures
- Installation Manual

REQ-MOD1-3	Releases and Deployment Management

Requests For Change (see REQ-MOD1-7) will be grouped in releases.

EMSA can request at maximum 3 Standard releases per year, usually one every 3 or 4 months, and a maximum of 10 Emergency releases to fix urgent issues (see REQ-MOD1-8). Note that the average number of Emergency releases of the ABM/SA-VAS module in the past was 1 per year. Within the scope of releasing a new version of the system, the Contractor shall update the documents listed in the requirement REQ-MOD1-2. The installation of a new release is an incremental installation, either standard or emergency release. The Contractor is in charge to prepare the "Release Notes" for installing a new release. EMSA is in charge to deploy a new release in all the environments (see REQ-MOD1-5). The Contractor shall include in the yearly price of Module 1 a total of **10 days per year of on-site support** at EMSA for installation, configuration, testing and commissioning purposes. EMSA will request the service at least 2 weeks in advance, with a minimum of 3 consecutive days of on-site support for each intervention.

REQ-MOD1-4	**Full Installation**
The Contractor shall assist EMSA in deploying a full installation of STAR ABM in any platform compliant with the EMSA Technical Landscape. EMSA is in charge of setting-up the infrastructure as specified in the Technical Landscape, the Contractor shall be able to perform a full installation and configuration of STAR ABM in order to have the service operationally ready in less than 5 working days. EMSA can request a maximum of 2 full installations per year.	

REQ-MOD1-5	**STAR ABM environments**
The Contractor shall support EMSA for the installation of the STAR ABM service in 4 different environments: Test, Pre-Production, Production and Business Continuity Facility (BCF). The configuration of the STAR ABM system, e.g. the number of data processing nodes, in each environment may be different.	

4 Operational Support

REQ-MOD1-6	**Issues Management**
EMSA is in charge of providing a system for managing issues (the ticketing system currently in use at EMSA is TeamForge). The Contractor shall address the issues opened by EMSA through the ticketing system according the Service Level Agreement (SLA) as defined in requirement REQ-MOD1-8. Compliance with the SLA will be measured based on the timestamp recorded by the ticketing system.	

REQ-MOD1-7	Type of Issues

The classification of the issues to be addressed is as follows.

Change Management

A Request For Change (RFC) shall be applied to any change in the system.

A RFC can be: (i) a new functionality, (ii) a defect to be fixed or (iii) a change of the system's configuration.

Each RFC in the system is described in a Change Request Form. The Change Request Form can be a document (i.e. a Technical Specification), or a ticket in the ticketing system.

A defect (ii) and change of the configuration (iii) shall be addressed by the Contractor within the context of the information provided of REQ-MOD1-1. Any new functionality shall be addressed as part of Module 2 or 3 and is **not included** in the yearly price of Module 1.

Incident Management

Incident Management shall include the resolution of incidents and the handling of service requests (e.g. requests for information/support, requests for sending specific notifications to end users). The key objective is to guarantee that incidents and requests are handled accurately, completely, and in a timely manner ensuring therefore adherence to the agreed service levels specified in REQ-8.

The Contractor shall be in charge to provide this service.

The tenderer shall provide a clear approach of the incident management process that includes as a minimum the following activities:

- Incident detection and recording,
- Classification and initial support,
- Investigation and diagnosis,
- Resolution and recovery,
- Incident closure,
- Incident ownership, monitoring, tracking and communication.

Problem Management

Problem management shall include the resolution of problems in response to one or more reported incidents with unknown cause.

The Contractor shall be in charge to provide this service.

The tenderer shall provide a clear approach to the problem management process that includes as a minimum the following activities:

- Problem Analysis, Categorisation, and Prioritisation,
- Problem Investigation and Diagnosis,
- Provision of the Solution.

REQ-MOD1-8	Service Level Agreement

The following definitions are to be taken into consideration:

- Time to acknowledge – the time the Contractor is informed of the problem until the Contractor provides an initial investigation and analysis of the issue;
- Time to solve – the time the Contractor is informed of the issue until the moment the issue is solved and the service is available again to the end user.
- Type of incident priorities (see Annex VII to the Framework Contract):

Priority	Definition
1: Critical	An incident causing total loss of the primary functions of the service (s) covered by the specific contract for help-desk and corrective maintenance.
2: Urgent	An incident with blocking effects on the work-flow of an individual or a small group of users of the service (s) covered by the specific contract for help-desk and corrective maintenance.
3: Normal	An incident affecting an individual user or a small group of users causing interruptions to the normal work-flow of the service (s) covered by the specific contract for help-desk and corrective maintenance.
4: Low	A minor incident affecting only an individual or a small group of people with minor consequences to the work-flow of the service (s) covered by the specific contract for help-desk and corrective maintenance.

For the execution of the issues defined in this contract (see REQ-MOD1-7), the Contractor shall meet the service level as defined in Table 1 – SLA.

Priority of the issues	Time to acknowledge and provide a preliminary analysis	Resolution time
1: Critical	2 working hours	1 working day
2: Urgent	4 working hours	5 working days
3: Normal	2 working days	15 working days
4: Low	5 working days	30 working days

Table 1 – SLA

EMSA is responsible to classify the issues (priority, issues type, etc.).
In case the Contractor disagrees with the EMSA's classification, the Contractor can propose a different classification within the acknowledge time. In case of conflict EMSA has the rights to take the final decision.
This SLA is applicable to the STAR ABM Production environment only.
For all the types of issues REQ-MOD1-7 the Service Level Agreement reported in this requirement is applicable. The working procedures and basis for calculation of SLA are further defined in Annex VII to the Framework Contract.

REQ-MOD1-9	**Number of issues to be solved**
The Contractor shall provide operational support according the SLA specified in the requirements REQ-MOD1-8 for a maximum of 10 Critical issues per year, 20 Urgent issues per year, 100 Normal	

issues per year.

As an example from July 2015 to October 2016 (15 months period) the following issues have been addressed.

Incidents and problem
2 Critical issues, 8 Urgent issues, 13 Normal issues.

Request For Change
(only correction of defects and configuration changes, not new functionalities)
3 Normal issues.

There are currently (April 2017) 120 Surveillance jobs running in Production.
As an indication of the high level of stability of ABM, the 1-month CPU Usage statistics of the nodes show an average of 3% with a few peaks of approximately 13% and no downtime.

REQ-MOD1-10	**Configuration Management**
EMSA is responsible to configure all the STAR ABM environments. If requested by EMSA the Contractor shall support EMSA for the configuration of STAR ABM and the troubleshooting in any environment.	

REQ-MOD1-11	**Pro-active analysis**
Every two weeks the Contractor shall issue a highlight report by e-mail to the EMSA STAR ABM Project Manager summarizing possible issues and propose solutions. This task shall be performed, but not limited, on the grounds of an analysis of the STAR ABM's application log files, system features status (as for example CPU consumption, hardisk consumption, etc.) and a test that the Contractor shall perform on the system. Any test needs prior authorization by the Project Manager.	

REQ-MOD1-12	**Monthly Report**
Each month, within the first 7 days, the Contractor shall provide a report to EMSA assessing the status of open issues. The report shall at least contain the following information: - Total number of open tickets per issue types; - Number of tickets open in the last month per issue types; - Number of tickets closed in the last month per issue types; - Number of tickets that are not compliant with the requirement REQ-MOD1-8; - Status of the issues identified within the context of requirement REQ-MOD1-11.	

REQ-MOD1-13	Bi-annual report and meeting
The Contractor shall draft a bi-annual report, every 6 months from the signature of the contract. The report shall contain: - Brief description of the Activtites performed; - SLA compliance and breaches, if any - Summary of the major incidents/problems occurred; - Lessons learned - Proposals to Improve the Service The report shall be submitted within 14 calendar days from the end of the six-months. Bi-annual (twice a year) meetings shall take place at EMSA premises. If requested by the Contractor and accepted by EMSA the meeting can be held by a phone or video conference. Maintenance will be invoiced every six months following the acceptance by EMSA of the report provided by the Contractor at the end of each six-months indicating all maintenance performed during the six-months and a supporting invoice. The Contractor shall provide 2 weeks before the bi-annual progress meeting updated versions of the documents described within REQ-MOD1-2.	

5 STAR ABM Release 3.0

The ABM (SA-VAS) version number is currently the same as the IMDatE core considering that both modules have been developed under the same contract. The most recent Release of ABM is v. 2.1.

The **Release 3.0 of ABM** shall implement the requirements described in the following sections.
ABM Release 3.0 shall maintain or, whenever possible, improve the level of service of the current ABM features (v. 2.1), in particular with regard to:

- Surveillance management (response time to requests less than 5 s)
- Alerting performance (data throughput of 200 messages/s and response time less than 60 s)
- ABM Service monitoring and recovery.

REQ_MOD2_1. ABM Release 3.0 Features and Performance: ABM Release 3.0 will maintain and, when possible, improve the current features and performance of ABM.

5.1 Stand-alone ABM

ABM is currently coupled with the IMDatE Core and some essential functions are not provided by the SA-VAS module.

The main requirement of Release 3.0 is to **make ABM independent of the IMDatE Core**.

5.1.1 ABM Database and Configuration

ABM Release 3.0 shall not use the IMDatE database, configuration and other services anymore.

The Contractor shall design and develop a separate, independent ABM module, with database and configuration files dedicated to the ABM application.

The ABM database will respond to the needs of the ABM service, like the storage of the Surveillance algorithm templates, the management of the Surveillance instances, the Alerts, the dispatch of the Alert Messages etc. As a starting point, the Contractor can refer to the logical model and data structure of the current IMDatE database, in particular the tables and relationships used by SA-VAS.

Any ABM configuration item that is currently part of the IMDatE Core shall also be included in the ABM database or dedicated configuration files.

REQ_MOD2_2. ABM Database and Configuration: ABM Release 3.0 database and configuration shall be independent from the IMDatE Core and any other module.

5.1.2 ABM Management Web Services

ABM Release 3.0 shall provide a set of Web Services for the management of the algorithm templates, the Surveillance instances and any other ABM configuration function. The Web Services shall make it possible for a "client" application to configure ABM, for instance create or update templates and activate Surveillance instances.

As a reference, IMDatE provides a web based graphical tool ("ABM Management Tool") for Surveillance configuration purposes that makes use of the existing Web Services of SA-VAS. The main features of the Tool and some screenshots are presented in this section and shall be supported by the ABM Management Web Services.

Note: the development of the ABM Management Tool is not within the scope of ABM Release 3.0.

The Tool provides the functions to view, create, clone, edit, start, stop, and delete Surveillances.
The Tool shows to the user the details (Area of Interest - AOI, Vessels of Interest - VOI, specific parameters, etc.) of the Surveillances created by the user and their current status.
The Tool highlights to the user any malfunction, e.g. blocked Surveillances.

The Tool provides the manual input of the vertices of an AOI (see Figure 5.1), the drawing on a map of new areas, the upload of the boundary in form of a polygon (KML, Shape file) or the selection of pre-defined areas (see Figure 5.2). Pre-defined areas can also be retrieved from the EMSA Central Geo-Registry Database (CGD).

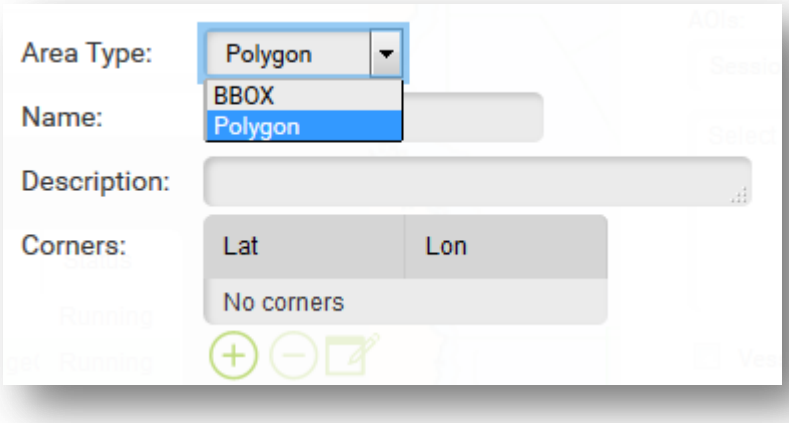


Figure 5.1 - Manual input of AOI

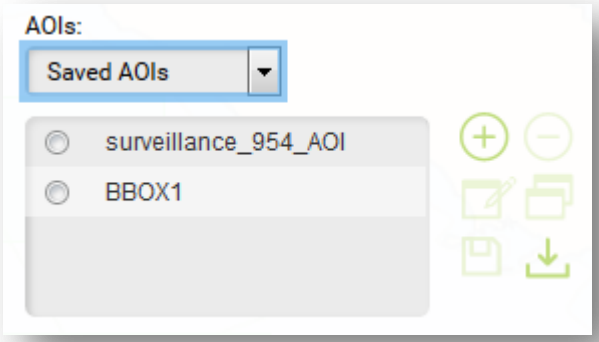


Figure 5.2 - List of Saved AOIs

The Tool provides the possibility to save/load VOI criteria.
The Tool provides the definition of a VOI based on:

- Filter by Flag and/or Ship Type (see Figure 5.3)
- Additional filters may be added in the future, e.g. vessel length, cargo, etc.
- Positive/negative criteria, e.g. all non-EU ships of type Tanker
- Include or ignore ships with empty attribute, e.g. no Flag or no Ship Type
- Upload of a list of ships identified by MMSI

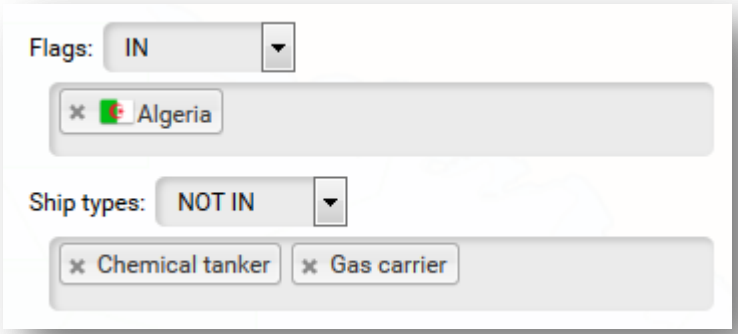


Figure 5.3 - Filter by Flag and Ship Type

The data entry form of the Tool adapts itself in a dynamic way to the different ABM algorithms, i.e. the type and format of the input fields shall reflect the definition of the selected ABM algorithm template (see Figure 5.4 and Figure 5.5). Any input field should be labelled by a title and the unit of measure.

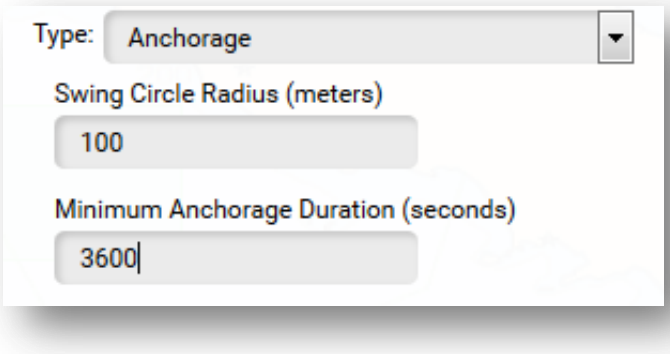


Figure 5.4 – Algorithm with Two input Parameters

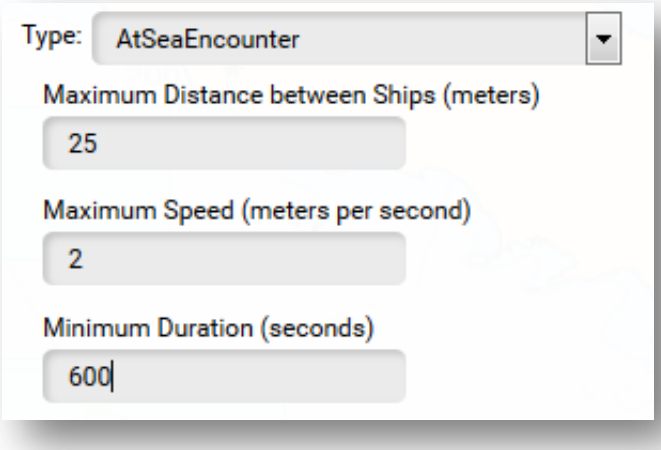


Figure 5.5 - Algorithm with Three input Parameters

The ABM engine works with the international metric system (SI). The unit of measure of the parameters in the data entry form of the Tool shall be configurable and it may be different from those of the SI, e.g. the

user enters the speed value in knots instead of m/s or the duration in hours instead of seconds. The Web Services of ABM Release 3.0 shall allow the input of a unit of measure different from the one used by the ABM engine and provide for the conversion. The units of measure shall be configurable for each ABM algorithm template separately.

REQ_MOD2_3. ABM Management Web Services: ABM Release 3.0 shall provide a set of Web Services to be used by an external application to configure ABM and manage the Surveillance instances.

5.1.3 CAP Message Processing

ABM shall parse and analyse the CAP messages corresponding to the alerts generated by the behaviour monitoring algorithms. The parsed content of the CAP message shall be stored in the database for Alert dispatching and further analysis.

REQ_MOD2_4. CAP Message Processing: ABM Release 3.0 will process CAP Messages and store the Alert information for dispatch and further analysis.

5.1.4 Distribution Lists

ABM shall provide the management of Distribution Lists that define who is entitled to see the ABM generated Alerts.

A Distribution List is identified by unique code and has a name and a description. Members of a Distribution List are users registered in the EMSA IdM system.
The user that creates a Distribution List is a “List Administrator”. A List Administrator can edit and delete his/her lists. A List Administrator can grant the role of Administrator for the same list also to other users. EMSA Operators are Administrators of any list.
When a List Administrator creates a Surveillance instance, he/she can associate the Surveillance instance to the lists that he/she administers. A Surveillance instance may be associated to only one Distribution List.
Users to be added to a distribution list shall be selected with a filter by:

- Country
- User name (substring)
- Organization

An EMSA Operator can select any user. A List Administrator can select only users belonging to his/her Organization.

The ABM Release 3.0 shall provide Web Services for the management (CRUD) of Distribution Lists, for instance by another application.

The ABM Release 3.0 shall also provide a Distribution List management tool, accessible by authorized users through the EMSA Liferay portal.

REQ_MOD2_5. Distribution Lists: ABM Release 3.0 will provide Web Services and a tool to manage Distribution Lists.

5.1.5 Alert Reports and Dispatching

ABM Release 3.0 shall provide the Alerts generated by the ABM Surveillance algorithms as reports (Alert Reports) in the following formats:

- Plain text
- HTML/CSS

to be chosen by the user during the configuration of a Surveillance instance.

The content (titles, labels, surveillance instance details, alert parameters, ship details, behaviour details, units of measure) and format of the Alert Reports shall be configurable by EMSA for each ABM algorithm template separately.

ABM shall dispatch the Alerts with the following mechanisms:

- getAlerts Web Service
  - Provide a getAlerts Web Service that returns the Surveillance instance and Alert details in JSON format to authorized users (see IMDatE ICD)
- E-mail
  - Send an e-mail to the address of the recipient(s) with the Alert Report in the message Body; the Subject of the e-mail shall be composed of 2 parts: a fixed prefix defined by the user plus a unique alert ID.

ABM shall dispatch the Alerts to the creator of the Surveillance if no Distribution List is present.
If a Distribution List is associated to a Surveillance instance, then ABM shall dispatch the Alerts to all the members of the List. In this case, ABM does not dispatch the Alerts to the creator unless the creator is a member of that List.

In addition to the getAlerts and E-mail dispatch mechanisms, ABM Release 3.0 shall also provide to the EMSA Administrator the possibility to associate a particular existing Surveillance instance with a remote REST Web Service end-point. Whenever an Alert is triggered by that Surveillance instance, ABM invokes the remote Web Service and sends the Alert details in JSON format (POST call).

REQ_MOD2_6. Alert Reports and Dispatching: ABM Release 3.0 shall create and dispatch Alert Reports to authorized users through the getAlerts Web Service, E-mail and remote REST Web Service invocation.

5.2 Service Monitoring

The ABM Release 3.0 shall be compatible with the existing Surveillance Monitoring Console (SMC) and provide to the EMSA Operators the means to monitor the ABM service and stop, restart, or delete any Surveillance.
If deemed necessary and subject to EMSA approval, the Contractor may modify the SMC or provide an equivalent console to perform the same monitoring functions as in the SMC.

REQ_MOD2_7. Surveillance Monitoring: ABM Release 3.0 shall be compatible with the SMC and provide the same service monitoring features.

5.3 Use of Central Databases

ABM shall make use of the existing EMSA Central Databases to retrieve reference data (e.g. user logins and e-mails, Country codes, Geographical areas, Ship details etc.).
ABM shall be connected to the EMSA Central Databases to support the user during the setting of the Surveillance parameters:

- Central Geo-Registry Database (CGD): for the selection of pre-defined shared geographical areas, e.g. geographical areas of Portuguese ports
- Central Country Database (CCD): for the selection of Flags or group of Flags, e.g. “non-EU Flags”
- Central Location Database (CLD): for the selection of Ports or group of Ports, e.g. the list of Irish ports.
- Central Ship Database (CSD): for the selection of ships or groups of ships and the retrieval of ship details.

REQ_MOD2_8. Central Databases: ABM Release 3.0 shall make use of the EMSA Central Databases to retrieve reference data.

5.4 Logging and Standards

ABM Release 3.0 shall keep the same type of logging currently active in the Production environment. The log files shall allow the monitoring of the ABM service as well as the investigation in case of incidents or other problems (“who did what and when?”).

An exact plain-text copy of the following items shall also be kept in order to support troubleshooting:

- Surveillance Management request messages received from external systems, e.g. Surveillance create or update requests
- CAP messages
- Alert Reports sent to external systems (e-mails and web service messages)

REQ_MOD2_9. Logging: ABM Release 3.0 shall maintain the current logging capability and store a copy of the exchanged messages in order to support service monitoring and troubleshooting.

5.4.1 Time keeping

All time values stored, logged and published by ABM shall be in UTC.
The representation format of a timestamp must be according to ISO 8601, e.g. **2017-03-17T13:55:25Z** if one second precision is sufficient, or **2017-03-17T13:55:25.000Z** in case of one millisecond precision.

REQ_MOD2_10. Time keeping: ABM Release 3.0 shall use UTC and record time in ISO 8601 format.

5.4.2 Geographical coordinates

Geographical coordinates (Latitude and Longitude) shall be stored and logged in decimal degrees with 4 decimal digits, e.g. -23.4567.

ABM shall publish geographical coordinates, for instance in an Alert report, in any of the following formats:

- DMS, e.g. 33º30'10''N 111º21'13''E
- DM, e.g. 33º30.16'N 111º21.22'E
- Decimal Degrees with 4 decimal digits

An Alert report shall be configurable to show the coordinates in a different format for different algorithm templates.

REQ_MOD2_11. Geographical coordinates: ABM Release 3.0 shall store and log the latitude and longitude values in decimal degrees and publish them in DMS, DM, and Decimal Degrees.

5.5 Performance

ABM Release 3.0 shall provide or possibly improve the level of performance of the current ABM service in the Production environment.
As a reference, the average number of position messages per second processed by an ABM Node is 95. In case of an Alert, the average delay between reception of a position and the corresponding Alert is less than 1 second.

REQ_MOD2_12. Performance: ABM Release 3.0 shall provide the same level of performance of the current ABM service or better.

5.6 Data Housekeeping

ABM Release 3.0 shall provide an data housekeeping function that regularly deletes data items from the ABM database and log folders. The housekeeping shall be configurable in terms of execution frequency, for instance "run once per day", and data retention, e.g. "delete data items that are older than 6 months".

REQ_MOD2_13. Houskeeping: ABM Release 3.0 shall provide a housekeeping function that automatically deletes old data.

5.7 Project Plan

The Project Plan is briefly described in this section. The detailed version of the Project Plan will be agreed with the Contractor at Kick-off (to be held at date T0).

5.7.1 Deliverables

All deliverables shall be packaged according to the requirements set by EMSA (see Appendix 1).

First Intermediary Release

This release shall include the new version of the ABM module, working with an independent database and configuration files. To be installed in the Test Environment only.

Second Intermediary release

This release shall also include the ABM Management Web Services with connection to the Central Databases and Alert dispatch (getAlerts and E-mail). To be installed in the Test and Pre-Production Environments only.

Final Release

The Release 3.0 of ABM with all features, to be installed in all Environments

5.7.2 Milestones

Milestone#	Date	Milestone
M1.	**T0+1.5 months**	Detail Design Document and Test Plan
M2.	**T0+4 months**	First intermediary release
M3.	**T0+6 months**	Second intermediary release
M4.	**T0+7.5 months**	Factory Acceptance Test (FAT)
M5.	**T0+8 months**	Final Release
M6.	**T0+9 months**	Go live in Production Environment, start of commissioning period
M7.	**T0+12 months**	End of commissioning period, Project Closure

5.7.3 Meetings / On-site Support

Date/Milestone	Event
T0	Kick-Off at EMSA
Every 2 weeks	Progress status report by phone or video conference
M2	**5 days on-site support** at EMSA during installation and configuration of the First Intermediary Release
M5	**5 days on-site support** at EMSA during installation and configuration of the Final Release
M6	**5 days on-site support** at EMSA during the Go-Live
M7	Final Meeting at EMSA

--- End of the Document ---