18th ICCRTS

Increasing Maritime Situational Awareness with Interoperating Distributed Information Sources

Topic 4: Collaboration, Shared Awareness, and Decision Making, Topic 8: Networks and Networking, Topic 7: Architectures, Technologies, and Tools

FULYA TUNCER CETIN
ASELSAN Elektronik Sanayi ve Ticaret A.Ş. PK.30 Etlik, Ankara, 06011, TURKEY

BURCU YILMAZ
ASELSAN Elektronik Sanayi ve Ticaret A.Ş. PK.30 Etlik, Ankara, 06011, TURKEY

YILDIRAY KABAK
Software Research, Development and Consultancy Ltd., Silikon Building, No: 14,
METU Technopolis 06531 Çankaya/Ankara TURKEY

JU-HWAN LEE
GMT, 7th Fl., Pangyo W-CITY, 9-22, 255 beon-gil, Pangyo-ro, Bundang-gu,
Seongnam-si, Gyeonggi-do, SOUTH KOREA

CENGIZ ERBAS
ASELSAN Elektronik Sanayi ve Ticaret A.Ş. PK.30 Etlik, Ankara, 06011, TURKEY

ERDEM AKAGUNDUZ
ASELSAN Elektronik Sanayi ve Ticaret A.Ş. PK.30 Etlik, Ankara, 06011, TURKEY

SANG-JAE LEE
GMT, 7th Fl., Pangyo W-CITY, 9-22, 255 beon-gil, Pangyo-ro, Bundang-gu,
Seongnam-si, Gyeonggi-do, SOUTH KOREA

Point of Contact: Fulya Tuncer Cetin,
Adress: ASELSAN Elektronik Sanayi ve Ticaret A.Ş. PK.30 Etlik, Ankara, Turkey
Telephone: +905303220859
e-mail: ftuncer@aselsan.com.tr

Security Classification: Unclassified

Increasing Maritime Situational Awareness with Interoperating Distributed Information Sources

Fulya Tuncer Cetin[1], Burcu Yilmaz[1], Yildiray Kabak[2], Ju-Hwan Lee[3], Cengiz Erbas[1], Erdem Akagunduz[1], Sang-Jae Lee[3]

1 ASELSAN Elektronik Sanayi ve Ticaret A.S. PK.30 Etlik, Ankara, 06011, TURKEY

{ftuncer,buyilmaz,cerbas,erdem}@aselsan.com.tr

2 Software Research, Development and Consultancy Ltd., Silikon Building, No: 14, METU Technopolis 06531 Çankaya, Ankara TURKEY

yildiray@srdc.com.tr

3 GMT, 7th Fl., Pangyo W-CITY, 9-22, 255 beon-gil, Pangyo-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, SOUTH KOREA

{jlee, sjlee1012}@gmtc.kr

Abstract. Enhanced maritime situational awareness picture is a common need for maritime authorities interested in security, safety, border control, and marine environment protection. In order to have an enhanced maritime situation awareness picture, it is recognized that there is a need for advanced and innovative surveillance and information-sharing technologies. This study presents an open and interoperable maritime surveillance framework which utilize ontology based operations and domain rules in order to integrate different data stemming from a combination of systems and sensors; and perform behavior analysis of the detected cooperative and non-cooperative targets of any size. In this system, seamless information exchange among systems and sensors leads to better and cost effective maritime surveillance, while performing behavioral analysis enables intelligent decision making and reduces time-to-act. Within the scope of this study, a Maritime Situational Awareness Ontology is created as a common model to mediate different information sources, and a rule repository is formed for storing suspicious vessels criteria. The presented work is undertaken within the scope of RECONSURVE (Reconfigurable Surveillance System with Communicating Smart Sensors) project supported by EUREKA ITEA2 cluster.

Keywords: maritime surveillance framework, semantic interoperability, situational awareness, multi data fusion, threat analysis, vessel classification

1 INTRODUCTION

Obtaining enhanced maritime situation awareness picture is a common need to most of the maritime authorities interested in different aspects such as security, safety, border control, or marine environment protection. To have enhanced maritime situation awareness picture it is recognized that there is a need for advanced and innovative surveillance and information-sharing technologies. However, currently there are a number of different maritime surveillance systems and authorities which have different duties and responsibilities depending on their institutional role. These authorities collect and analyze data for their own purposes by means of dedicated monitoring and surveillance systems, and do not have ability to share information automatically with other organizations [1]. This situation leads to inefficiencies in their daily processes, such as, obtaining incomplete operational picture, collecting redundant data by different bodies, spending too much time or effort to identify suspicious vessels, and overlooking suspicious events.

Combining data from different sensors and reporting systems increases the success rate of ship identification, leaving fewer unknown ships in the picture, thus reducing the amount of potential risks that need closer attention. Therefore, when several authorities perform surveillance in the same area with different systems, integration of their data leads to a more complete picture and better manageable maritime traffic, to the benefit of all. However, this can cause having voluminous information coming from all the sensors and missing some important events in the flow of information. Thus, there should be some intelligent mechanisms to process this voluminous information and detect and eliminate vessels from possible targets that may pose a risk or behave illegitimately.

This paper presents an open and interoperable maritime surveillance framework in order to integrate data stemming from a combination of systems and sensors. The framework also utilizes ontology based operations and domain rules in order to perform behavior analysis of cooperative and non-cooperative vessels of any size for preventing illegal acts from being committed. This study is a part of a research and development project, RECONSURVE (Reconfigurable Surveillance System with Communicating Smart Sensors), supported by the European EUREKA Programme ITEA2 Cluster. The approach is implemented by an interdisciplinary research team composed of nine different organizations/companies, including naval officers with operational experience, experts in C4IS, sensors, sensor systems, information and communications technologies, and Service Oriented Architecture.

The organization of the paper is as follows: Second section describes the current maritime picture in Turkey and possible threats, while the third and fourth sections present available data sources and interoperability studies realized within the project, respectively. The fifth section covers threat analysis mechanism and the sixth section presents alarm generation and dissemination. Finally, the last section describes future work and concludes the paper.

2 Maritime Situational Awareness against Illegal Activities

Turkish Coast Guard Command (TCGC) [1] is the competent authority on the security of maritime jurisdiction area in Turkey, which is the main end user of RECONSURVE project. Its missions can be summarized as conducting search and rescue operations, fighting against illegal activities including smuggling and illegal migrations and preventing pollution at sea. TCGC carries out its main mission using state-of-the-art surface and air assets and mobile maritime surveillance systems along approximately 8,500 km long coastal lines of the country.

Illegal immigration has become one of the serious issues throughout the world during last decades. Due to its unique geographical location which acts as a bridge between two continents, Turkey is one the countries that has been most adversely affected by this issue. The fact that Turkish coast is extremely close to some of the Aegean Islands (1-5 miles, which can be traversed by a small vessel in 30 minutes) provides easy passage and further exacerbates the problem. Due these facts, fighting with illegal immigration is one of the priorities of TCGC.

TCGC relies on intelligence and crime analysis for risk management. There are number of national sources which provide the required resources to accomplish this. Each of these sources, namely different Ministries and State Institutions, collects and analyzes data for its own purposes by means of dedicated monitoring and surveillance systems. TCGC conducts its duties and operations in close cooperation with these institutions but combining all the available data into a coherent whole is a challenge. In order to enhance the current practices and operational capabilities regarding their missions and cope with emerging threats of maritime domain TCGC aims to assess the results of RECONSURVE project which provides the means for having persistent surveillance, utilizing background domain intelligence, and multi-source data analysis.

3 Common Operational Picture and External Data Sources

Common Operational Picture (COP) is a maritime picture which includes information about vessels within the surveillance area, their movements and, if possible to predict, their intentions in near future [1]. In addition to this, it can present details regarding environment, position of your own systems with their missions and capabilities. During operations, decisions and actions are taken based on COP.

To create a COP, you need to have reliable and trusted information sources, which are automatically harmonized/fused to present an accurate picture by eliminating conflicting data. In RECONSURVE project, information required to construct COP comes from different sources; a diverse set of sensors (such as Radar, ElectroOptic/Infrared sensor (EO/IR) and Sonar) and external sources such as Automatic Identification System(AIS), Unmanned Aerial Vehicle (UAV), Port Information Management Systems (LYBS), and online web sites. Using different types of sensors and data sources can be used for independent confirmation of threat detection. Similar to bats identify-

ing their prey by a combination of factors such as size, acoustic signature, and kinematic behavior, observation of data from multiple sensors provide complementary capabilities. If multiple observations fed by different type of data sources are correctly associated, the combination of them provides a better determination of the identity of the object which will contribute to reducing error rates, rather than observation of an object's attributes obtained by either of the independent sensors, [4].

Multi Sensor Data Fusion Component leverages complementary characteristics of these sensors and external data sources and is responsible for harmonizing the acquired data coming from different sensors in order to create a real-time, unified situation picture which encompasses all detected entities and activities in the monitored area. In order to handle this massive amount of data provided on all aspects of maritime activity, a two-level data fusion is carried out by Multi Sensor Data Fusion Component. At the first level, data fusion utilizes data collected by systems' own sensors such as EO, Radar and Sonar. Later, fused data is enriched by data retrieved from other external sources and this enables the system to have more details about the vessels such as IMO number, type of ship, and its destination etc.

The EO/IR sensors, sonars and coastal surveillance radars deployed along the sea border operate to detect vessels within a controlled area. At the first fusion level, the system unifies/fuses the tracks that are determined to belong to the same object. As the observation areas of sensors might intersect, more than one track data for an object can be fed by these sensors to the system. For example, both underwater and over water surveillance systems might form track data belonging to the same object. The decision of which tracks need to be fused is made by considering distance between tracks, and comparing course, speed, platform type, and, identification properties of the tracks. Furthermore, the fusion process takes into account the performance of the sensors, which is referred as track quality in our system, to assign values to the fused track: the data detected by a sensor with higher track quality is chosen in data fusion process. When the first level fusion has completed, the raw data from sensors are converted into a "System Track Data Model". This creates an abstraction layer between sensors and Track Management Software Configuration Unit, i.e. Track Manager. Track Manager receives sensor data represented in unified model and is not aware of hardware configuration or system specification of any sensor. Thus, Track Manager can process any sensor data in the same manner as long as their raw sensor data is converted to System Track Model (Figure 1).

At the second level data-fusion, additional data from external sources are retrieved and aggregated into the fused sensor tracks. As a result of this, track data is enriched and ready for analysis. These external data sources are identified according to the data requirements which will help the system to foresee the situation in the near future for evaluating threat level. The data sources and integration efforts are described in following sections.

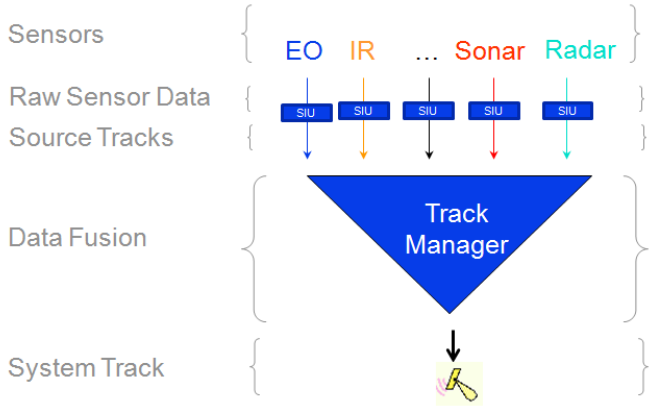

Figure 1 Sensor Data Flow

3.1 Automatic Identification System

AIS is a vessel identification system via VHF communication applying international standards designed in the first instance for maritime safety and in particular collision avoidance [1]. It is a self-reporting system and provides time and location information taken automatically from the GPS receiver in near real time (every 2 seconds to 5 minutes) depending on speed of the reporting vessel.

The carriage of AIS is mandatory on the basis of IMO's SOLAS convention since the year 2000 [5]. After the July 2007 the carriage requirements are for (a) ships of 300 gross tonnage and up on international voyages, (b) passenger ships (any size / voyage), (c) tankers (any size) on international voyages, and (d) cargo ships of 500 gross tonnage and up (any voyage) [6]. For vessels not covered by the IMO requirement, Class B AIS messages can be voluntarily reported for similar use, which are shorter and less frequent messages to save airtime. As it can be purchased at a reasonable price without additional communication costs, unlike satellite and mobile communications, AIS has easily spreaded and quickly become popular for the safety of vessels. The AIS is already installed in many vessels, especially merchant ships, all over the world and facilitates mutual information exchanges.

It is a critical technology that enables Maritime Domain Awareness in support of all Coast Guard missions. With AIS, 4S communication (Ship-to-Ship or Ship-to-Shore) becomes possible and authorities can obtain a continuous, real-time overview of the ship traffic. The international standards define AIS messages in such a way that they contain both static and dynamic information regarding the ship that originates the messages. While the static information includes vessel's MMSI/IMO number, type, and length; the vessel's speed, course, and rate of turn comprise the dynamic information. Analysis of both types of information provides invaluable clues regarding the vessels's navigational intention.

In terms of technology, there are several advantages of AIS to to other surveillance systems. Having a broader range (40-60 miles vs. 20-30 miles) and being less sensitive to waves and severe weather conditions than the radar or EO sensor can be shown as examples of such advantages. Furthermore, AIS data contains information such as destination data or estimated time of arrival which is provided by the vessel itself, which would otherwise not be collected by the authorities. This fact can also be regarded as another advantage of AIS to other surveillance systems. Having stated these, , the AIS has its own share of weaknesses. It can be spoofed; the quality of the information from AIS depends on the goodwill of participants: potential foes know how to use it, or not use it, so as to hide their intentions. To overcome these weaknesses and exploit valuable information that AIS messages carry for COP, the information obtained from these messages needs to be associated with the output of other sensors, databases, and data sharing mechanisms and analyzed together.

In RECONSURVE Project, AIS data is first processed for data-driven anomaly detection as a single data source. The AIS Analyzer cross-references received AIS messages with all logged AIS messages and builds a chronicle including all movements of a ship for a defined time period. These chronicles of ships are analyzed by separate dedicated servers such as Smuggling Analysis Server, Area Analysis Server, Sea route Analysis Server, Sailing Pattern Analysis Server and Collision Prediction Analysis Server. Later, both the analysis result and AIS messages are fed to the RECONSURVE system for further analysis with semantic models. The architecture of AIS Analyzer can be seen in Figure 2.

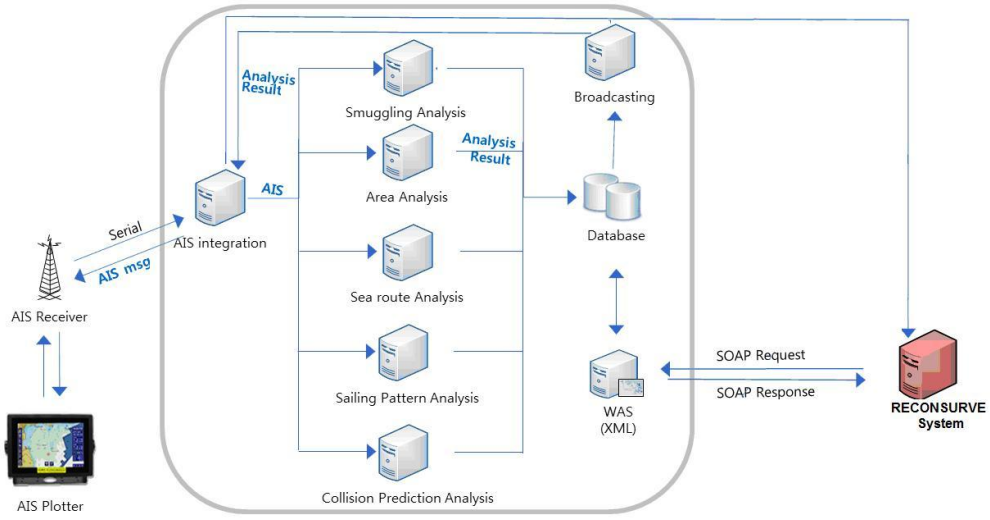

Figure 2 AIS Data Gathering and Integration

In this architecture, each server analyzes available data from a different perspective. Sea Route Analysis Server checks whether a vessel goes off its scheduled course and vessel's abnormal sailing patterns, including sudden stop and zigzag sailing. Through the monitoring at Collision Prediction Analysis Server, unusual situations, including vessel's veering off course and accident, are detected and necessary actions are rapidly taken. If a collision is predicted as a result of the analysis, an AIS Message, i.e. binary data for addressed communication, is sent to the ship and situation at the scene of the accident is monitored immediately. As a result, related parties or agencies can perform search and rescue more effectively. Area Analysis Server monitors preassigned areas, such as an environmental protection area, a military exercise area, and afrequent accident area, in real time and provides related parties with useful information so that they can take the necessary actions promptly. Smuggling Analysis Server uses AIS to monitor suspicious vessels by analyzing their tracking information in search for unusual sailing patterns to detect smuggling activity.

3.2 Unmanned Aerial Vehicle

Detection of all non-cooperative vessels under all conditions is a difficult task due to performance limitations of sensors of all kinds and enormous size of the area targeted for surveillance. This is especially true for small vessels which are frequently used for drug smuggling, illegal immigration and terrorism [1]. Terror attacks by small boats have been identified as one of the most serious threats to the maritime industry [7]. In addition to the state-of-the-art sensor networks, RECONSURVE supplements the existing surveillance systems with unmanned aerial vehicles for detection and classification of small vessels. Deployment of UAVs results in a much wider and possibly more accurate operational picture as opposed to shore-based, stationary systems. UAVs will enable TCGC to extend its surveillance functionalities beyond the range of stationary sensors.

Image processing in RECONSURVE system mainly concentrates on small vessel classification problem since these types of vessels are frequently utilized for illicit activities linked to organized crime. The vessel type information can also be provided within AIS messages. However, AIS is not mandatory for small vessels and it is open to be spoofed by potential foes. Therefore having an additional information source regarding the vessel type is very valuable. It enables the analysis of coherence between detected and declared information (if there is), detecting type of vessels which are non-cooperative and developing better awareness of, or countering, possible illegal activities by small vessels.

Vessel classification problem can be divided into two major parts. One is the construction of the image database and the other is devising the vessel classification algorithm which fits to maritime domain the best. Vessel Classification algorithm aims to work on the image which contains already detected vessel; it extracts the vessel from the image, then identifies its distinctive features and compares the extracted features with the image database.

Having a comprehensive image database is crucial since classification success depends on the information contained in it. Although there exist image databases for military vessels, the civilian counterpart of them is scarce. Thus, the first step taken towards designing the image classification system in RECONSURVE project was to construct such a database. The image database is constructed with virtual thermal images taken from various 3D civilian vessel models in simulation environment. Images are taken from 475 different angles and/or ranges to increase the reliability. Furthermore, these virtual images will be supported by images taken by an IR camera deployed on TCGC helicopters in the future.

For the problem solution, a novel silhouette-based recognition algorithm is developed after analysis of three main alternative approaches (namely, silhouette based, local features based, and global). The idea behind this approach is the fact that thermal images have an easily segmentable silhouette but not many features. The silhouette of the vessel is extracted by segmentation methods from the thermal image. Transform invariant features over the contours of the silhouette are detected by using the scale-space of curvature values. A novel descriptor to describe the silhouettes is created and named as Silhouettes Orientation Histogram Image (SOHI). The recognition performance achieved by using SOHIs is shown in Figure 3.

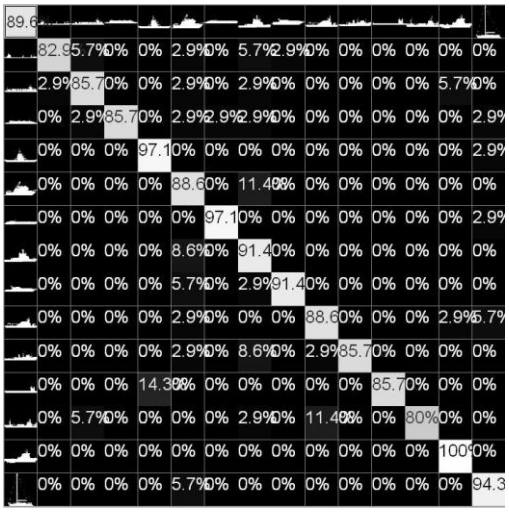

Figure 3 Vessel Classification Algorithm Performance

3.3 LYBS (Port Management Information System)

LYBS (Liman Yönetim Bilgi Sistemi- Port Management Information System of Undersecretariat of Maritime Affairs) provides online port departure and port arrival data of ships for all ports of Turkey. At Turkish territorial waters, it automatically presents Mate's Receipt (Landing Report), Vessel Voyage History Report and Port

Departure Report online. The system is also integrated with other external systems such as Inspection Targeting System, Ship Criminal Record Store, and Seafarers Document Inquiry Application, to automate the collaboration and provide required data to these systems. The collected data from LYBS is valuable for the analysis smuggling behavior among others. It can present the details of ships such as its current and previous cargo, destination, captain, crew, passengers and master data (e.g. IMO number, flag, agency, owner, width, length, etc). Furthermore, thanks to its integration with Inspection Targeting System, the details of previous oversea travels and its risk group can be identified.

3.4 Online Web Sites

There are quite a number of Web sites providing detailed information about vessels. Needless to say, the more data available for the vessels, the better situational awareness the system can provide. In order to utilize the data provided by these Web sites, they are also integrated to the RECONSURVE system. Unfortunately, most of the Web sites do not provide their data through an API. In other words, it can only be accessed through a Web browser. In order to obtain the data, screen scrapping techniques have been used. To achieve this, the HTML responses from these Web sites are parsed programmatically.

The integrated Web sites are as follows:

- VesselFinder.com [8]: This Web site provides AIS data and the last five ports visits of a ship. This is the only Web site that provides its data through an API (JSON interface). For example, if the http://www.vesselfinder.com/vessels/shipinfo?full=true&mmsi=247086200 (HTTP GET request to retrieve AIS info of ship whose MMSI number is 247086200) request is sent, the following JSON response is returned:

    - {"flag":"\/images\/flags36\/it.png","country":"Italy","imo":"9263655","mmsi":"247086200","name":"ATHARA ","type":"Passenger ship","dest":"OLBIA","etastamp":"Aug 16, 08:30","sizes":"216 x 26 x 6.7 m.","speed":"0 kn","style":"","timestamp":"Aug 16, 2012 06:05 UTC","photo_name":"9263655-247086200-24ed05f47beac69f8fb344f6b2b73bc0&uu=y","no_picture":false,"image_id":"9263655","key":"34d6466809"}

- Equasis.com [9]: This Web site provides the following information about a vessel: Master information, management detail (owner, manager, and agency), its previous inspections in the ports, its classification surveys, its previous names, flags and owners. The information is accessed through HTTP POST request.

- MarineTraffic.com [10]: The Web site provides AIS data of the vessels and shows their current position on the GoogleMaps. The Web site also provides the previous port visits of the vessels. Its data is reached through HTTP GET calls.

- AISHub.com [11]: This Web site provides only the AIS data of the ships and the data can be accessed through HTTP GET protocol.

3.5 Other Surveillance Systems

Management of crises and emergency situations requires timely and collective response by government organizations, civil agencies and military organizations. In such complex situations, effectively exchanging information about on-going events, collaboratively developing shared situational awareness and common operational picture help effectively planning and monitoring operations. One of the goals of RECONSURVE project is to create an interoperability platform to enable the exchange of situational awareness and tactical data between maritime surveillance systems. On the highest level, six main messages are modeled that will be exchanged among collaborating parties. These are Track Sharing Messages, Track Coordination Management Messages, Mission Assignment Messages, Mission Plan Messages, Acknowledgement Messages, Operation Situation Messages and Operation Result Messages.

4 Interoperating Data Sources

Series of decentralized manual processes and minimal interoperability among authorities lead to delays or inadequacies in briefing surveillance teams. This is one of the important difficulties in coordinating resources and inefficient tasking between the different operational centers.

Currently, most of the surveillance systems do not have the capability of dynamically employing available sensors in the environment and require performing a manual customization or integration effort in order to utilize the sensor observations or measurements. Systems need to have a priori knowledge on the sensor specific data such as its network protocol, data format or location. Sensor Interoperability layer addresses this problem and try to eliminate custom development efforts. At the sensor interoperability layer, this abstraction is provided by adoption of OGC-SWE standard, which resides between the sensor and the surveillance framework to provide a reliable communication interface for both producers and consumers of sensor data, regardless of the data formatting or protocols used by either. OGC-SWE standards [12] provide a set of standard web service interfaces for requesting, filtering, and retrieving observations and sensor system information. Observations & Measurements (O&M), Sensor Modeling Language (SensorML), and SOS profiles are implemented within the RECONSURVE project.

In RECONSURVE project, there are numerous information sources with different characteristics, running on different platforms and developed with different design styles and coding languages. In order to address the needs of interoperability among these complex and variable information sources of maritime surveillance, the system needs to be loosely coupled and extensible. If a new information source becomes available, it will be included into collaboration with minor integration effort. At the bottom layer of the interoperability stack, this is achieved through the adoption of a centralized approach leveraging Service Oriented Architecture (SOA). SOA model is assumed to cope with the requirements of complex and distributed environments characterized by a significant technological and managerial heterogeneity, as the one represented by the maritime surveillance domain [13]. This addresses interoperability at the message transport layer through a common set of Web-service interfaces.

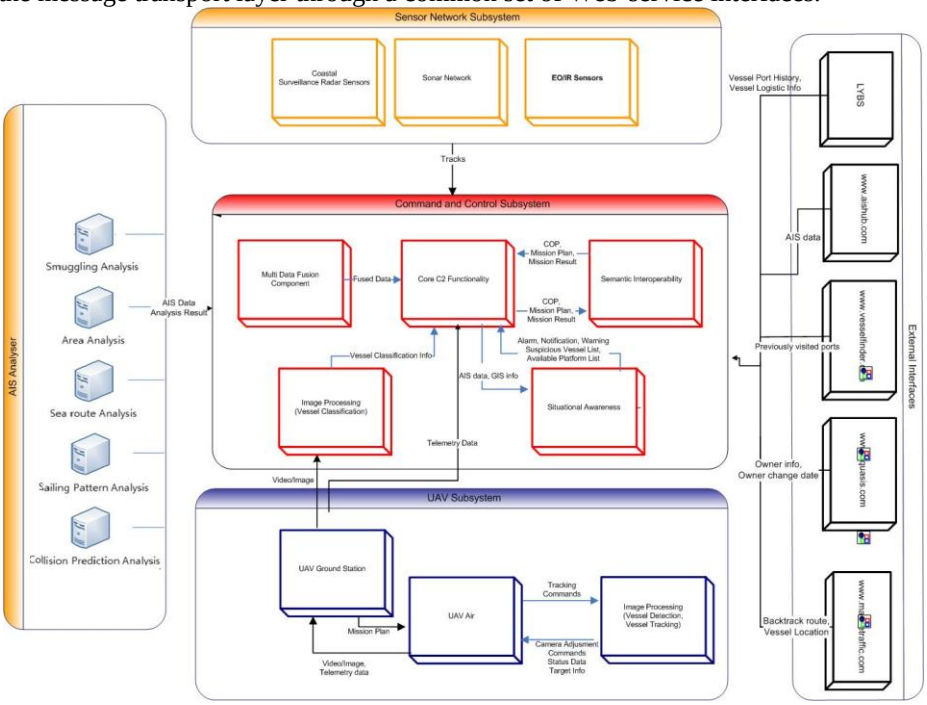

Figure 4 Interoperating Data Sources: Data Flow

Although information can technically be retrieved and collected from these data sources, in order to turn data into knowledge there is a prerequisite such that the receiver system needs to understand and process the data as intended by the provider. To capture the native semantics of those systems, it is required to have the deep meaning expressed as relationships among concepts within and across ontologies. Semantic Information Models provide a formal description of concepts, terms and relationships for specific knowledge domains. They are the optimal enablers for systems to understand, acquire and integrate information more efficiently and intelligent-

ly [14]. For this purpose, situational awareness ontology is developed to enable interoperability of these data sources. In this way, the underlying logical formalism makes it possible to "understand" the semantics of the collected knowledge from distributed information sources and process it in appropriate ways. RECONSURVE interoperability framework achieves the mediation among data source models automatically (or semi automatically) via Situational Awareness Ontology. As this ontology will be used as the common language between aforementioned data sources and maritime surveillance systems, the ontology needs to cover semantic versions of all of the information elements. The well-accepted standards constitute the base for the Situational Awareness Ontology. The standards included into the ontology are Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) [15], Open Geospatial Consortium's Sensor Web Enablement (OGC-SWE) [12], Automatic Identification System (AIS) [6], OASIS Common Alerting Protocol (CAP) [16]. The ontology harmonization details are available in [24]. Furthermore, upper ontologies such as The Suggested Upper Merged Ontology [17], Open Cyc[18], or COSMO[19] are planned to be linked to the Situational Awareness Ontology in order to cover the concepts that are not available in military domain models. These linkages will create a set of ontologies with an extended coverage.

The semantic interoperability architecture will be based on results of research initiative of the NATO RTO IST-075 & 094 working group, which includes methodologies and guidelines for the conceptual construction of the Semantic Interoperability Logical Framework (SILF) [20]. The architecture of semantic interoperability framework can be seen in Figure 5. The detail of this architecture is presented at [21].

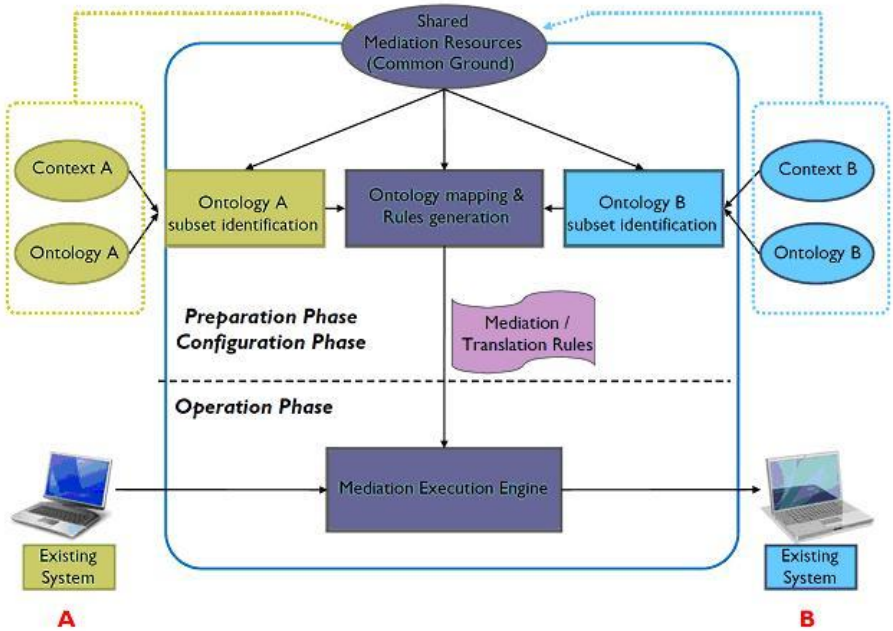

Figure 5 SILF Architecture [18]

5 Threat Analysis

Currently, threat Analysis is usually done by highly skilled operators who constantly monitor and analyze the activity in an area of interest. When sensor systems and external data sources are interconnected and the whole system becomes capable of surveying a large area containing hundreds of vessels, the operators reach their cognitive capacity and start to miss important maritime domain threats such as acts of piracy, and drug trafficking which are often "hidden" in the crowd of everyday fisheries, cargo traders, ferries and pleasure cruises, hindering situation awareness [22].

Interoperating different information sources does little more than "spam" the maritime "common operational picture" with more and more blips if there was no automated behavioral analysis and decision support to the operators [23]. The decision support system will help the operator to focus on important objects and thereby avoid information overflow. In the RECONSURVE project, we develop a system combining knowledge-based detection with data-driven anomaly detection for detecting unusual activity and anomalies. This early warning of possibly suspicious events enables the operator to be proactive and prevent unwanted situations from arising.

Two approaches have been hybridized for threat recognition in this research: an ontology-based approach that relies on the expressive features of Description Logic (DL) languages to present the context consisting of concepts and relationships, and a rule-based approach that encodes criteria to check suspiciousness of a vessel using Logic Programming rules.

Situational Awareness Component provides high-level reasoning and evaluates the threat possibilities. The individual objects and their current attributes are not enough for complete situation awareness. It is required that observables, indicators,mission a priori information and their interrelations to be represented in a meaningful manner and readily accessible to the system. Situational Awareness Ontology captures the context consisting of concepts and relationships that are relevant in our application domain, and ensures consistency and a common vocabulary across the system components. Furthermore, ontologies also provide a mechanism which allows inferencing on the data, such that an inference engine can derive new facts and conclusions implicitly represented in the data. The details related with generation of Situational Awareness Ontology are presented in [24]. We use Racer description logic inference engine, to complete the ontology consistency, concept based classification and other Ontology based Inference tasks.

For rule based mechanism, we collaborated with TCGC, i.e. domain experts, to understand how they normally analyze the data and decide on which vessel can cause a threat or perform an illegal activity. Based on this collaboration we elicited the first set of suspiciousness criteria. So far, 55 situational awareness rules are encoded as a preliminary set of rules. This type of threat analysis is referred as knowledge-based, template based, or case-based threat analysis. According to these rules, the system

searches for anomalies like “small boats on open sea” in case of illegal immigration or “a cargo vessel heading to a harbor other then the destination in the AIS message” in case of smuggling. There are also some template rules which need to be instantiated before being executed. These template rules are for guarding a special area, analyzing movement patterns and speed of a vessel or looking for temporal relations among events. For example, for the case of guarding a special area, a ship entering a specified area can cause an alarm. Boarding or sudden acceleration can also cause an alarm if user instantiates a template rule for analyzing movement patterns and speed of a vessel. As a final example of a template rule, a ship entering a specified area before a certain time can cause an alarm if there is a temporal relation defined for that area.

The number of objects and relations that constitute situational awareness are enormous considering the complexity of continuous maritime monitoring of a large region To cope with this complexity, situations should be constrained according to the user’s monitoring goals such that the situation analysis system can derive the necessary knowledge in a timely manner by focusing on just those relevant events and candidate relations. Furthermore, the rules defined on the aforementioned relations might be regionally varying. If this is not taken into account, it can result in system inconsistency and making the system alert the operator unnecessarily. For example, while boarding of two vessels in open sea can cause a threat alarm, this case is very common in a harbor area. Speed limits also differs according to region. If a user defines a rule such as “If two vessels takes a similar trajectory and approaches each others, then alert me”, this may cause a number of false alarms and overwhelm the user when this rule is executed for a harbor area. To overcome this issue, rules and regions are associated via user interface. Users can draw an area on the map, and select list of rules that he/she wants to execute for that area. In addition to this, if any rule has any adjustable parameters, he/she can specify these parameters for each area separately. This provides flexibility to the system and let the system separate rules that are valid for specific areas. As a result, it mitigates the negative effects on the operators and on other response teams by lowering the false alarm rate.

Another crucial feature of a system consisting of autonomous components is to have the adaptation capability. RECONSURVE project provide algorithms to conduct self-learning. List of applied rules and user indication of whether a threat alarm is a real threat or not are evaluated to asses the number of false-positive and false-negatives. This evaluation is later used to tune weight (or priority) of rules.

The situational awareness rules in the RECONSURVE project are implemented through Drools Rule Engine [25]. Drools is a business rule management system (BRMS) with a forward chaining inference based rules engine, more correctly known as a production rule system, using an enhanced implementation of the Rete algorithm [1]. The existence of these rules allows the system to be extended to different situations

[1] http://en.wikipedia.org/wiki/Rete_algorithm

easily without re-installation of it. In other words, these rules allow system extensibility. The rules defined in the system can be adjusted or edited based on the situtation by the domain experts. It may be cumbersome for a maritime domain expert to edit Drools rules, which is a technical work. Therefore, a Drools Rule Editor is developed to help the user to edit them through a GUI. In the following figure, a snaphsot from the Rule Editor is presented. Using this, domain experts can create new rules to adapt the system to changes in the environment and threat types without undue burden.

On the left pane, the created Drools is presented. On the "Code Blocks" pane, there are the building blocks of Drools syntax, which the user can work using drag-and-drop mechanism. The application layer specific object models are also presented to the user and these object models actually show the knowledge space such as Vessel, AIS, Location, etc.

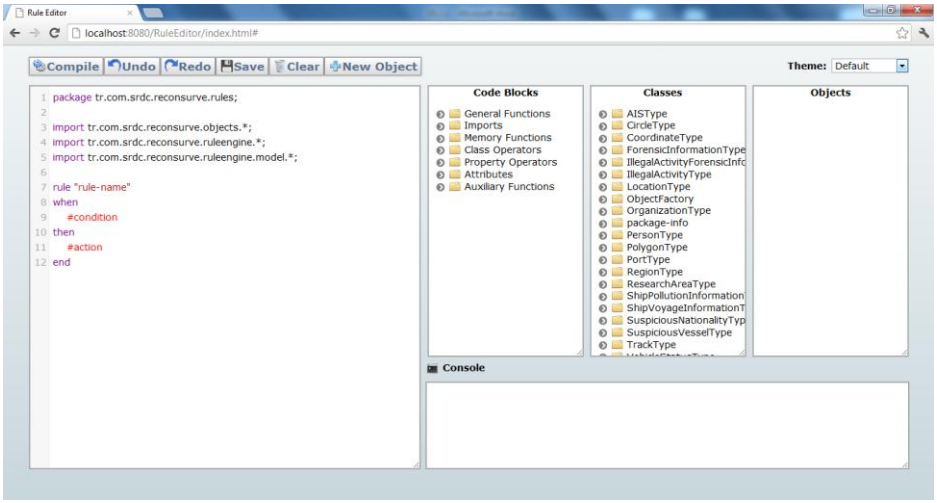

Figure 6 Rule Editor GUI

6 Alarm Generation and Dissemination

Timely and apt information is essential to prevent, anticipate, effectively respond and recover from any kind of threat [26]. Since the process of dissemination of threat detection should be done sufficiently in advance for preventive action to be initiated, one of the focus of RECONSURVE Project is early warning generation.

In rule based behavioral analysis, each rule is assigned a weighting (a kind of priority) which helps to identify associated risk level and its confidence. This weighting is calculated dynamically according to variance between thresholds in a rule and detected values. For example, a slight difference between maximum speed limit declared in

a rule and detected speed of a vessel indicates lower risk values. These weighting values can be tuned by self-learning mechanisms according to user feedbacks for reducing the false alert rate and making RECONSURVE system more robust. Furthermore, each rule has at least one type of associated risk types such as smuggling, terrorist attack etc. These risks types together with the calculated weighting define the threat level. We use three-level alerts to define the severity of the threat such as severe, moderate and minor. An alarm is disseminated with its identified level and level category is displayed on the COP with its coded colors. This gives a chance to operators for responding to the most risky threat first and hence reducing the possible damage. An effective early warning system also needs to provide details about the cause of the alarm associated with detection [27]. Alert generation system also communicates overridden rules and the level of uncertainty at the same time. Currently most of the existing systems lack a complete system providing these kinds of details related with the possible threat [28].

Common Alert Protocol (CAP) of OASIS Emergency Data Exchange Language (EDXL) is used as the data format for disseminating threat alerts. This enables to cope especially with the maritime crisis situations cooperatively by the military organizations and government agencies.

7 Conclusion

The RECONSURVE project has been motivated by and aims to address the need to control the rapidly increasing number and complexity of maritime surveillance issues, such as preventing illegal immigration, enabling interoperability between heterogeneous systems, and achieving automated, cost-effective and efficient decision support. Seamless information exchange among systems and sensors leads to better and cost effective maritime surveillance, while performing behavioral analysis enables intelligent decision making and decreases time-to-act. In RECONSURVE project, we have developed a system to interoperate a number of different data sources; a diverse set of sensors such as Radar, EO/IR and Sonar and external sources such as AIS, UAV, LYBS, and online web sites. This data sources are enriched with semantic technologies and knowledge based anomaly detection algorithms are applied to review collected data and assess likely threats. Importantly, these events may then immediately be disseminated to agencies with a vested interest in identifying potential security threats.

This study presents mid-term result of this study and details on-going work on development of threat analysis module with different number of data sources. As a future work, we aim to proceed according to the project plan and increase maritime situational awareness with interoperating distributed information sources.

Currently, the development activities are on-going and planned to be finalized at the end of year 2014. The final product will be deployed in Turkey and France for demonstration.

8 REFERENCES

1. Integrated Maritime Policy for the EU, Working Document III on Maritime Surveillance Systems, European Commission / Joint Research Centre Ispra, Italy , June 2008.
2. Turkish Coast Guard Command, http://www.sgk.tsk.tr/
3. Arciszewski, H.F.R. , De Greef, T.E. A smarter common operational picture: the application of abstraction hierarchies to naval command and control, 16th International Command and Control Research and Technology Symposium ICCRTS: Collective C2 in multinational civ-il-military operations, June 21-23, Quebec, 2011, 1-20
4. D. Hall and J. Llinas. An introduction to multisensor data fusion. IEEE Proceedings, 85(1), January 1997.
5. International Maritime Organization Web site, Automatic Idenftication System, http://www.imo.org/ourwork/safety/navigation/pages/ais.aspx , Last visited February, 2013.
6. Guidelines for the Installation of a Shipborne Automatic Identification System (AIS), International Maritime Organization, 6 January 2003
7. Christopher Doane and Joseph DiRenzo III, "Small Vessel Security Summit Initiates Constructive Dialogue," Maritime & Border Security News, July 25, 2007.
8. http://www.vesselfinder.com/, Last visited February, 2013.
9. http://www.equasis.org/EquasisWeb/public/HomePage, Last visited February, 2013.
10. http://www.marinetraffic.com/ais/tr/default.aspx, Last visited February, 2013.
11. http://www.aishub.net/, Last visited February, 2013.
12. OGC Sensor Web Enablement, http://www.opengeospatial.org/projects/groups/sensorwebdwg, Last visited February, 2013.
13. Mike P. Papazoglou, "Service -Oriented Computing: Concepts, Characteristics and Directions," Web Information Systems Engineering, International Conference on, p. 3, Fourth International Conference on Web Information Systems Engineering (WISE'03), 2003
14. Uschold M., Grüninger M., Ontologies: principles, methods, and applications, Knowledge Engineering Review, Vol. 11, No. 2. (1996), pp. 93-155.
15. JC3IEDM, Joint Consultation, Command and Control Information Exchange Data Model, MIP. "'True' JC3IEDM ratified as NATO STANAG 5255". MIP. http://www.mip-site.org/010_Public_Home_News.htm. Retrieved 2009-03-11.
16. OASIS Emergency Management TC, http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=emergency
17. Suggested Upper Merged Ontology ("SUMO"), http://suo.ieee.org/
18. Open Cyc, http://www.cyc.com/cyc/cycrandd/areasofrandd_dir/is
19. COSMO, COmmon Semantic Model, http://semanticcommunity.wik.is/
20. Bacchelli F.; Boury-Brisset A.; Isenor A.; Kuehne S.; Martinez R. B. ; Miles J.; Mojtahedzadeh V.; Poell R.; Rasmussen R.; Uzunali A.; Wunder M., Final Report of Task Group IST-075 Semantic Interoperability, July 2010
21. F Tuncer Cetin, Y Kabak, B.Yilmaz, A. DOGAC, C. Erbas, Semantic Interoperable C4I systems for maritime surveillance: The RECONSURVE Approach, NATO Information Systems Technology Panel Symposium (IST-101 / RSY-024) on Semantic & Domain based Interoperability

22. Neef, R.M. ; Hanckmann, P. ; van Gosliga, S.P. ; van Halsema, D., Improving maritime situational awareness by fusing sensor information and intelligence, Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference, July 2011
23. Boraz, Commander Steven C, U.S. Navy, Maritime Domain Awareness – Myths and Realities, Naval War College Review, Summer 2009, Volume 62, Number 3, Naval War College Press, Newport:RI, 2010
24. A Dogac, Y Kabak, A Bulca, T Namli, C Erbas, B Yilmaz, F Tuncer Cetin, RECONSURVE: JC3IEDM and EDXL based Emergency Management Service Oriented Architecture for Maritime Surveillance, To be appear on eChallenges 2012 Proceedings
25. Drools Rule Engine, http://www.jboss.org/drools/
26. Al-Khudhairy, Delilah H. A. (2010) 'Geo-spatial information and technologies in support of EU crisis management', International Journal of Digital Earth, 3:1, 16 – 30
27. Early Warning Systems: State-of-Art Analysis and Future Directions, United Nations Environment Programme (UNEP), available at: http://na.unep.net/geas/docs/Early_Warning_System_Report.pdf
28. A. Schnabel (2008). 'Improving early warning and response systems: Learning from human security, preparing for climate change'. In A. Ricci (Ed.). From early warning to early action? The debate on the enhancement of the EU's crisis response capability continues. Brussels: European Commission, Directorate-General for External Relations, and Luxembourg: Office for Official Publications of the European Communities. pp.387–98.