SECMAR - Harbor Protection System

Patrice MISTRETTA
THALES UNDERWATER SYSTEMS SAS
525 route des Dolines - BP 157 - 06903 Sophia-Antipolis Cedex - FRANCE
patrice.mistretta@fr.thalesgroup.com

OCOSS 2010 Conference Publishing
Brest – FRANCE

Abstract - Thales Underwater Systems, with about twenty French industries and laboratories, is leading a consortium called SECMAR (SECurity system to protect people, goods and facilities located in a critical MARitime area).

The main objective of the SECMAR project is to provide an awareness picture for the “close sea-side” area in order to facilitate the task of the harbor surveillance and intervention teams. The designed system for the strategic harbor of Fos-sur-Mer (Marseille, France) will be described.

The detection is provided by multiple passive sensors (Sonar, Radar, Electro optic, AIS receiver). These detections plus other data, coming from the port systems or external agencies, are brought to an inshore centre which manages a multiple sensor fusion and a behavior analysis so as to detect automatically any threatening target. The system should also have a reporting function so that the operator can capture and memorize all elements of interest.

Major SECMAR features are surveillance with multiple sensor technologies, data fusion, anomaly detection taking into account sensor data and harbor management data, data dissemination at multiple organization level for analysis and decision, assistance to the intervention, and multi media reporting. Extra missions are Mission of Safety of Navigation and Law enforcement

SECMAR demonstrator is operational at FOS SUR MER, FRANCE from June to December 2010.

I. INTRODUCTION

The Competitiveness Centers were initiated by the French state at the end of 2004. In July 2005, the "Pôle MER PACA" was labeled as a worldwide centre. The SECMAR project was labeled by the "Pôle MER PACA" on Friday 13th January 2006 and selected by the FCE in May 2006.

The SECMAR project has been split in two phases:

- Phase 1 dedicated to a phase of studies for each SECMAR partners. The main objective were to define the full set of requirements for a SECMAR prototype and to select the most appropriated set of sensors.

- Phase 2 objective is to realize the SECMAR prototype, and to deploy it on the site of FOS SUR MER (FRANCE) for a period of harbor trials over 6 months time. The SECMAR Phase II has been labeled the 3rd of June 2008. The duration of the PHASE II is 30 months, until December 2010.

II. OBJECTIVES

The main objective of the SECMAR project (SECurity system for property, life and installations present in a sensitive MARitime zone) is to provide a tangible solution to detect a terrorist threat that would occur on or underneath the surface of the sea, as a preferred line of attack for a vitally important coastal site.

In a second objective, SECMAR will be used to increase the safety of the navigation in the vicinity of the Harbor (Maritime interdiction and Law enforcement)

An initial level of organization is intended to group together industrialists and laboratories working in the same activity area in one subsystem. A Leader is identified for each subsystem.

The SECMAR project aims to study a solution for a surveillance system that takes into account:

- Asymmetrical threats, clandestine threats, vague and stealth threats (propelled divers, lightweight high-speed boats, Jet skis…).
- Illegal traffic (theft, damage…)
- Major surface traffic related to commercial and port activities
• Highly disrupted electro-optic and acoustic underwater environments,
• The need to merge multi-sensor and high-level automation data.
• To increase the safety of the navigation in the vicinity of the harbor (Maritime interdiction and Law enforcement)

Faced with these terrorist threats hanging over targets as varied as oil terminals and gas terminals, LPG tankers, oil tankers lying at anchor or docked, the project's objective is to develop a surveillance system based on:
• Using complementary detection means,
• Pooling information from basic combined detection means in an Inshore Center to be able to produce a global and summarized vision of detected intrusions,
• Adapting (type, number, locations) these detection and protection means: to match site geography and facilities, regulations, means of action...
• Grouping together and distributing data to improve the security vision of monitored areas and in particular, with the development of an interoperability function with other systems involved in the surveillance and security of these zones (navigation radar, VTS/AIS).
• Anomaly Detection by analyzing the behavior of the detection provided by the Tracking and fusion capability in order to raise an alarm if the behavior is not categorized as a normal/usual behavior
• To give automatically a first level of classification and identification of a detection when sensors information are enough accurate

Although the final goal is to design a generic solution for the surveillance of any critical maritime areas, the SECMAR prototype has to take into account the local constraints of the Gulf of Fos-Sur-Mer. Fos-sur-Mer is located in the South East of France, next to Marseille (Cf. figure 1). It is a strategic harbor, which controls half of the French oil and gas supply. There are one oil terminal and one gas terminal (Cf. figure 2).

![figure 1: Location of Fos-Sur-Mer](image)

The Mixed sensors, with complementary detection performance, are used in order to increase the detection probability of a terrorist attack:
• Underwater sonar surveillance
• Above water radar surveillance
• Electro Optical systems

There are two advantages to mix different sensors into a unique detection and analysis system:
• To be able to detect different type of threats and different intrusive scenarios
• To be efficient in complex environmental conditions (shallow water, noisy environment, commercial and tourist traffic, threats with low-level signatures ...)

The fusion processing is rather complex since the association has to be realized between heterogeneous data with different time rate, different detection performance characteristics, different measurement error probabilities etc.

The surveillance system takes into account:
• reaction times that are compatible with the planned means of action,
• environmental constraints,
• operational constraints related to actual site activity,
• measures already in force concerning both defensive protection of sensitive points and the site manager's responsibility.
• Navigation Rules and restricted Areas (Law enforcement)
• An Interface to a Non Lethal Response System to give a first level of response against an intrusion.
III. SECMAR PACKAGE FOR FOS SUR MER

The SECMAR version installed in FOS SUR MER is composed of the following subsystems:

**Optronic detection:**
- A set of wide angle cameras that provides a large field of view of the protected zone: 60°/LOS.
- A long range, narrow field of view camera fitted on a pan and tilt adjustable platform, able to automatically follow a target and provide efficient zoomed picture for visual target identification and classification, 360°rotation / 5° field/LOS.

**Radar detection:**
- A radar specifically designed to work in a short range harbor context and able to detect and discriminate small target with a radar cross section: 360°/10nm.

**Underwater detection:**
- A passive sonar, composed by a network of matrix of hydrophones, able to detect sub surface and surface object, specially when the line of sight of the other subsystems is blocked by large obstacle (hidden zone): 120°/4000m.

**Inshore Center Control and Command:**
- A command and control processing that collects sensors information, performs specific processing (mainly: multi sensor fusion and behavior analysis) and acts as a data server.

An operational room composed of one overview screen that displays the global situation, and two consoles, one for operational use and one for crisis management. Both consoles may be moved in surveillance rooms located in the watchtower of the harbor.

**Link to Patrol Interception boat:**
- An Interception Support device to assist the Harbor authorities to intercept the intruders.

**Others equipments :**
- An AIS receiver (automatic identification system) equipment able to identify and localize collaborative target (which send AIS signal by itself).
- A GPS sensor able to provide the clock reference to synchronize the sub-systems and to provide accurate sensor position when the sensor node becomes mobile.
- A METEO sensor able to provide the current meteorological information (wind characteristics).

**Data dissemination:**
- A bridge to the external services using web technology to broadcast and receive maritime safety and security information
- A bridge to the Homeland security network if such legacy system are in use on site, and capability to merge information to the Maritime security and safety system.
- An interface to the “Non Lethal Response System”. This interface will transmit the tracks linked to the treats to allow the “Non Lethal Response System” to be locked on.
IV. MISSIONS

SECMAR System provides a help to the safety of the port for the following missions:

- Mission of surveillance
- Mission of analysis and decision
- Mission of assistance to the intervention
- Mission of Safety of Navigation and Law enforcement
- Mission of report
- Mission of record and replay

Mission of surveillance:
Surveillance mission gives to the operator a maritime picture situation awareness as a clear and interactive picture of the harbor zone, system effectiveness and monitoring, tracks which evolve in this zone.
For each track the operator is informed of the nature (classification/identification when it is possible), the kinematics and of the level of threat, which is automatically given or manually decided.

Mission of analysis and decision:
Analysis tools give to the operator a way to evaluate manually and to specify the level of threat of naval objects present in the harbor zone.
Decision aids gives to the operator and harbor authorities a way to evaluate very quickly the level of threat of a track and all potential targets.
In order to help the operator in this mission a set of comprehensible tools of navigation is provided to the operator such: ETA (Estimated time of arrival), CPA (Closest Point of Approach), CTS (Course to steer) and others.

Mission of assistance to the intervention:
Mission of assistance to the intervention allows preparing a series of documents and real time picture facilitating the work of intervention team in charge of the harbor security.

Mission of Safety of Navigation and Law enforcement
The system will provide detection of boats committing an offense against the navigation rules to enforce the safety on the area under control.

Mission of report:
Mission of report allows operator and harbor authorities to examine any event and its context and to prepare a series of documents adapted to the formalism of the port.

Mission of record and replay:
Mission of record and replay to allow operator to store all the events occurring during the analysis phase, snapshots, operators actions, tracking events, etc.. The capability of recording will be defined in accordance with the regulation laws of the authority.

V. SECMAR OPERATIONAL CONCEPT

The SECMAR processing follows these steps:

A. STEP 1:
The surveillance sensors disseminated on the port performs detections and calculate sensor tracks. The sensor tracks consist of geographical positions; kinematics attributes and specific signature/identifier provided by each type of sensor: RADAR, SONAR, DOP & Ais. Plus Harbor VTS track which are also considered as input.

B. STEP 2:
A track fusion process merges the sensor-tracks and provides system-tracks.

C. STEP 3:
A classification and identification ( if possible) processing, are performed on the system tracks to give to the operator further information about the characteristics of the detection in order to help the Behavior analysis phase.

D. STEP 4:
An Anomaly detection module processes track information and harbor management data on two specific directions. To detect a threat ,based on behavior analysis, the module automatically gives a threat evaluation to each system-track. There are 3 levels of threat: «Abnormal», «Undefined» and «Normal». «Abnormal» system-tracks will raise an automatic alarm. The operator will be informed of the reasons that conclude to this level of treating. To raise an alarm if the system track has broken specific navigation law, the infringement will be detailed and provide to the operator.

E. STEP5:
The operator may use manual analysis tools on any system or sensor track, of his choice, and in particular those, which are evaluated threatening. The operator can take the control of analysis sensors in order to complete and form an opinion about the system-track. Any analysis done by the operator is the subject of the automatic creation of an analysis folder, which will support the decision phase.

F. STEP6:
In case of critical risk analysis the operator creates a decision context. The operator in agreement with the proper authorities can then decide or not to start an alert by using the chain of command of the harbour. The management of alert does not form part of the system itself; on the other
hand, the system prepares automatically an intervention context to support intervention team.

G. STEP 7:
The system allows supports an intervention team by broadcasting in real time the elements of the intervention folder. In case of multiple alarms, multiple intervention channels are available in the same time

STEP 8:
The system allows recording and reporting facilities at any level of work according to the harbour definitions and laws of country.

VI. THREATS ANALYSIS

The Threats analysis method addresses:

• The definition of the surveillance area
• The list of Asymmetric threat identification retained for SECMAR.
  • The list of potential scenario defined for SECMAR
  • A list of Sensor type versus Threat type

A. Definition of the surveillance area

The five surveillance areas, centered on the area defined for SECMAR, are classified from A to E, according to possible reaction time and level of emergency.

These areas give the constraint of Threat detection within each zone.

• Area A: Sensitive area: immediate exclusion of all non "operational" ships 0 < Area < 100m
• Area B: Maximum Alert Area: threat detection in this area is essential. It corresponds to a minimum restricted navigation area around port facilities. 100 < Area < 2 000m
• Area C: High alert: threat detection in this area is important. 2000 < Area < 5 000m
• Area D: Medium Alert Area: threat detection in this area is desirable. 5 000m < Area < 10 000m
• Area E: All coastal areas. Outside surveillance sensor range (except for the radar) Area > 10 000m

Figure 3 Sensible areas

The following schema summarizes the areas on the deployment site of SECMAR

Figure 4 Reaction time area

The following analysis of reaction time zone is based on a Fast boat sailing at 30 kts.
B. Asymmetric threat identification

Identified threats are divided into two groups, Surface threats and Underwater threats.

These threats have been characterized in terms of Type, and Characteristics.

- **Threat Type**
  - Above Water Threats
    - RHIB or Inflatable dinghy
    - Jet Ski
    - Small boat / motorized vehicle
    - Canoe/kayak
    - Fake Fishing Ship (length < 15 m)
    - Cargo Ship in coastal water (length < 50 m)
  - Under Water Threats
    - Transport vehicle with diver
    - Diver with assisted propulsion
    - Snorkel diver
    - Unmanned undersea vehicle (UUV)
    - Free Diver (not taken into account in the SECMAR system)
    - Marine animal with explosive charge (not taken into account in the SECMAR system)

C. Above Water attack

- RHIB / Small boat / motorized vehicle / Fake Fishing Ship / jet ski
  
  These types of boats loaded with explosives will reach its target quickly and use the explosives, either in close proximity to a ship or on impact.

  These type of boats could be armed with machine guns, rocket propelled guns or shoulder fired missiles. Armed attackers embarked on small, fast moving craft such as a RHIB or pleasure boat. Small arms such as a machine gun would have relatively limited impact but could result in fatalities on board, an RPG or other small missile device would allow for longer range and a larger impact.

- Canoe/kayak
  
  The Canoe will get slowly closer to its target, land on it to plant the explosives on the hull and get away.

  An armed intruder on these small platform such as a canoe or kayak could potentially achieve a very close approach and even board a ship carrying small quantities of explosive or other weapons.

- Tanker / Cargo
  
  A ship taken hostage by a terrorist group. The ship can be run aground on a route, strike a critical area, or strike other ships.

D. Under Water attack

- Transport vehicle with diver / Diver with assisted propulsion
  
  The Diver carrying a small quantity of explosives will get slowly closer to his target to plant the explosives on the hull.

- Snorkel diver
  
  Armed swimmer on the sea surface could also potentially make a close approach without detection and deliver small quantities of explosive or other weapons.

- Unmanned undersea vehicle (UUV)
  
  UUV with explosive payload that could under remote control sail directly into a moored ship.

  Sensor type versus Threat type
  
  The table below shows an exercise to place the threats in order according to their probability of occurrence in a civilian port surveillance context.

  This table clearly shows that above water go-fast threats are the most likely.

  Even though underwater threats are less destructive, they are considered as being threats that are potentially possible and therefore, detection of them is taken into account in the SECMAR system.

  For each threat, the contribution by each subsystem in detecting the threat is indicated.

<table>
<thead>
<tr>
<th>THREATS</th>
<th>PASSIVE</th>
<th>EOS</th>
<th>RADAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fake fishing boat</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CARGO TANKER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RHIB Inflatable dinghy</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>JET SKY</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Small boat Motorised vehicle</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Canoe, Kayak</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Snorkel diver</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Diver with assisted propulsion</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Or transport vehicle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmanned Undersea vehicle</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Tableau 1 Threat detection versus subsystem performance
VII. SYSTEM ISSUES

To cover the size of the harbor area multiple sensor node, which contains a set of sensors are deployed on many places. All nodes are gathered together in a central processing room.

Multi sensor track fusion need to process data from different sensor technology. Processed data includes position and kinematics, bearing only track, AIS input, radar shape, sonar sound signature, optical shape including shape recognition.

Anomaly detection, includes moderator and false alarm reduction. uses harbor logistic information for prediction.

The system is integrated in the harbor chain of command.

One operator survey a 10x10 Km2 area. Operation room is composed by four screens. A large survey, an interactive survey, an analysis screen and a video control screen.

For decision making, a secured web access provides a set of read only information accessible at multiple decision places.

VIII. THE BEHAVIOUR ANALYSIS MODULE

Port and coastal areas can be very crowded and the reaction time must be very short (typically less than 5 minutes for a threat detected at 5000 m). Therefore the operator work must be limited to the analyze of suspicious objects whereas the surveillance system task consists in recognizing every “normal” behaviors. It is expected that more than 90% of the detected tracks will be automatically classified as normal.

A possible display of these automatic classification is the use of different colors: green if the tracks are classified as
“normal”, red for the “dangerous” ones and orange for the suspicious behaviors.

The figure 5 corresponds to an example based on arbitrary simulated trajectories.

This automatic threat level classification will be performed by the behavior analysis module.

Two complementary approaches have been considered:

• Formal rules stated in a specific mathematical language;
• Statistical methods based on Hidden Markov models.

The achievement of the statistical approach depends on the quality of the machine learning. Since the SECMAR product is a prototype which will be tested at sea only at the end of the project, no real data are available yet.

That’s why for the moment we have given the priority to the formal approach.

For each detected track, the behavior recognition algorithm is divided up in the following way:

1) a set of instantaneous information is estimated thanks to the current analyzed track data (especially position and speed);
2) those observations allow to outline a set of behaviors;
3) if a behavior is considered as a threat, an alarm is raised.

The designed behavior can be either instantaneous (it depends only on the current instant) or temporal (the analysis requires many instants).

“The vessel goes too fast” or “the vessel is in a no-admittance zone” are a few examples of instantaneous information that can be estimated from the tracks.

“The vessel goes too fast for more than 15 seconds” or “the vessel is heading for a critic point for 10 seconds” are examples of temporal behaviors.

The “instantaneous behaviors” are simple Boolean combinations of instantaneous information. The “temporal behaviors” are more complex to specify and need to use synchronous programming language.

The scenarios of the temporal behaviors can be compared to synchronous reactive systems. To implement these scenarios, we take benefit of reactive synchronous languages. The selected programming language is the Esterel language (Cf. [2] for an introduction to this language).

Each scenario can raise a set of alarms. For the same vessel, a scenario can raise a low level warning whereas another scenario raises the strongest one. The different alarms raised for a same vessel have therefore to be combined to provide a unique alarm level for each track. For each raised alarm, the information suite leading to this alarm can be retrieved.

The figure 6 sums up how the behavior analysis module allocates a threat level to each track.

Each scenario can raise a set of alarms. For the same vessel, a scenario can raise a low level warning whereas another scenario raises the strongest one. The different alarms raised for a same vessel have therefore to be combined to provide a unique alarm level for each track. For each raised alarm, the information suite leading to this alarm can be retrieved.

The figure 6 sums up how the behavior analysis module allocates a threat level to each track.
Figure 10 Anomaly detection

Figure 11 Anomaly detection result
ACKNOWLEDGMENT

For his scientific support in anomaly detection:
Marie GEHANT marie.gehant@fr.thalesgroup.com

The SECMAR consortium is composed by theses companies:

- THALES UNDERWATER SYSTEM
- THALES SURFACE RADAR
- THALES D3S
- GPMM Grand Port de Marseille
- NAVFCO
- CETMEF
- Communication & Systèmes
- BERTIN Technologies
- CESIGMA
- DIGINEXT
- CHRISAR
- Ecole des MINES de Paris, Centre de Mathématiques Appliquées
- ISEN

REFERENCES


Marie Géhant, Patrice Mistretta
THALES UNDERWATER SYSTEMS SAS 525 route des Dolines - BP 157 - 06903 Sophia-Antipolis Cedex - FRANCE
marie.gehant@fr.thalesgroup.com,

Valérie Roy, Jean-Paul Marmorat, Marc Bordier
Ecole des MINES de Paris, Centre de Mathématiques Appliquées Rue Claude Daunou BP 207 - 06904 Sophia-Antipolis Cedex - FRANCE
valerie.roy@cma.ensmp.fr;
jpml@cma.ensmp.fr; marc.bordier@cma.ensmp.fr