Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C)

Michel MOREL & Stéphane CLAISSE (DCNS)
IEEE Conference Publishing
445 Hoes Lane
Piscataway, NJ 08854 USA

Abstract

As we face varied threats of terrorism and other lucrative criminal activities, in 2015, innovative solution shall be set up to permanently track and monitor all type of ship traffics, in vulnerable trading lanes and zones in order to detect abnormal or illicit vessel behaviour to understand and to early identify threatening situations. This future generation of maritime surveillance system must allow:

- Permanent and all weather coverage of border maritime areas.
- Continuous collection and fusion of heterogeneous data provided by various types of sensors deployed on coast and on mobile platforms and other information from external sources.
- Supervised automatic detection of abnormal vessel behaviours (in track and performed activity) and generate justified alarms.
- Understanding of suspicious events and early identification of threats from series of detected spatiotemporal abnormal vessel behaviours (alarms).
- Generate electronic and formatted interpretation reports on the suspicious event to keep periodically informed decisional authorities.

No equipment and information system [1] deployed are currently able to answer all these requirements. However, in the horizon of 2015 significant technical progresses have been made in wide maritime area coverage by different sets of sensors, heterogeneous data processing and fusion, and detection of abnormal behaviours methodology that could be usefully integrated together to built up an new generation of sea border surveillance integrated system for efficient security applications in high density traffics.

---

[1] *Most advanced sea surveillance operational systems in Europe are Spationav (France), S.I.V.E (Spain) and MEVAT (Finland). All these maritime surveillance systems are limited to perform traffic picture from conventional coastal radars and collected AIS data (version 2 in implementation) over only territory waters (up to 20 nautical miles from the shore).*

The objectives of the proposed I2C integration project are:
- To build up a complete test system (end to end information acquisition and processing system).
- To test the system in a ways of integration of data from network of existing and new maritime surveillance sensors and other available intelligent information sources in order to obtain optimal maritime security awareness.

Integrating existing and advanced capacities demonstrate, in the horizon of 2015 that actual sea surveillance system can be significantly completed and upgraded with innovative technologies to build up operational solution to fulfil the main sea border surveillance requirement which is to early identify threats in order to timely react.

I. INTRODUCTION

To achieved these above objectives:
- Two coastal sites are installed with set of sensors to survey wide maritime areas. These shore based platforms provide measurements (AIS messages, radar vessel tracks and optical imageries) to build up maritime traffic picture for reporting and non reporting vessels.
- Planned exercises using mobile platforms (aircraft, vessel patrol, Zeppelin and unmanned ship with sensor payloads) to provide high resolution local node measurements to complete the shore maritime traffic picture.
- Fusion of all sensors measurement (vessel detection) with existing information on vessel characteristics (Lloyds Register data base, Traffic2000, Ship spotting, etc.), on black listed vessels (Paris and Tokyo MOUs, etc.), on meteorological conditions (wave height and surface wind speed and direction, surface current, etc.) and on geographical context (bathymetry, regulated areas, etc.), to provide intelligent maritime traffic picture.
- Applying conditional rules, based on combined elementary conditions, to allow detection of abnormal vessel behaviours, then, associated alarms are issued to operator

for analysis and validation. Examples of rules are, for example:

✓ Excessive speed (first condition) in regulated maritime area (second condition) will generate an alarm for regulation violation.
✓ Vessels boarding (first condition) during night (second condition) and with low wave height (third condition) will generate an alarm on suspect event which can be analysed as trans-boarding of drugs.
✓ Vessel stopped in international water (first condition) during less than thirty minutes (second conditions) and with low surface current speed (third condition) will generate an alarm on suspect event which can be analysed as dropping smuggling goods at sea.

• Validated alarms by operator are transferred to the group of experts for understanding and identification of threats. This task is performed from tool kit to analyse the history of the alarm elements and its evolution during time with the help of knowledge models about similar past suspicious events already identified.

The main outcomes of I2C are:

• Advanced technical capacities, algorithms and procedures on how to acquire / process / use / fuse / exploit collected information up to suspicious event understanding and early identification of associated threats.
• Statements about the added value of the various sensor types and the end to end data acquisition and processing chain assessments following various threats (i.e. drug smuggling, illegal fishing, clandestine immigration, regulation violation, etc.).
• Demonstration with exercises at sea that integrated I2C capacities fulfil operational maritime security awareness.

II. I2C ARCHITECTURE

Taking into account the previous I2C objectives, the following figure 1 provides the system architecture solution (with relevant innovative technologies / capacities) and main data flows for sea border surveillance. This integrated system (data acquisition and processing capacities) includes existing conventional and innovative sensors networks as well as new advanced functionalities to track vessel movements and activities, detect abnormal vessel behaviours and identify ongoing associated threats in order to limit human, economic and environmental impacts.

The I2C specifications and architecture are managed by DCNS (one of the world leader of warship) and all the system data bases are developed by SOFRESUD companies.
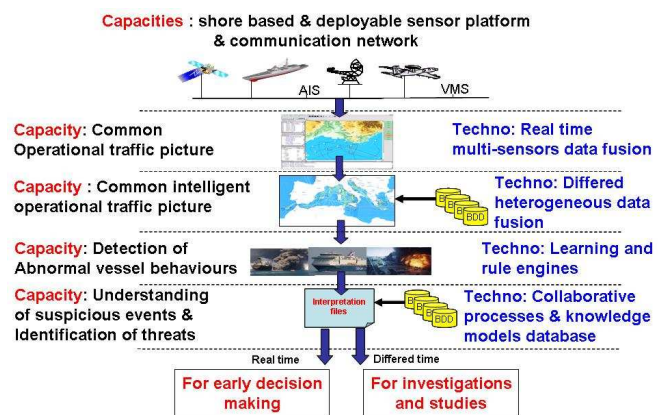

Figure 1.I2C system architecture

This architecture is structuring an end to end information chain. This chain processes, step by step, the networked sensor data up to identify threats from detected abnormal vessel behaviour associated to suspicious event. These steps are:

• The first and second steps; to collect the networked sensors data and generate the common operational traffic picture. The sensors data are fused to generate for each detected vessel (reporting and none reporting) its trajectory on a chart.
• The third step; to append the vessel track information with the vessel characteristics, identity (i.e.; flag, owner, destination, etc.), environmental conditions (i.e.; meteorological parameters) and geographical context (bathymetry, regulation, etc.).
• The fourth step; to detect in the track and appended information the abnormal behaviour such as flag hopping, boarding, propulsion failure, fishing in protected area, etc.
• The last step; for the identification of threats associated to detected abnormal behaviours such as illegal fishing, smuggling of drugs, piracy, etc. During this last step report is elaborated and forwarded to the decisional authority.

With this integrated capacities, in 2015 timeframe, scaling studies / designs can be made that propose the composition of maritime surveillance systems at any specific locations (even capacities can be installed separately such as sensors platform on shoreline and data processing capacities in remote places, even capacities for common operational traffic pictures can acquire data coming from external already existing shore sensors platform network), so authorities can commission these kinds of studies based on the I2C project results.

III. SHORE PLATFORMS

Three shore platforms are installed on coastal sites closed to Toulon in France (SESDA: Site d'Expérimentation de Systèmes de Défense Aérienne pour la Méditerranée, Iles du Levant and Séte (port in Mediterranean coast). That three shore implementations allow permanent and all weather surveillance of Mediterranean high traffic over extended zone including

maritime routes for different types of vessels (tanker, LNG, ferry, cruise, bulk, container, etc.), fishing zones and seasonal recreational vessel, yacht, etc.

On coastal sites, the deployed sensors are:

- Conventional coastal radar – FURUNO Finland – for surveillance of territory water (SESDA station).
- Optical camera (remotely controlled) – AJECO Finland – for specific sector surveillance at high resolution (SESDA).
- Long range radar (HFSWR = High Frequency Surface Wave Radar) prototype – ONERA France – for surveillance up to 200 nautical miles from shoreline. ONERA HFSWR is the only available prototype in Europe and actually is tested in Bay of Biscay (will be installed in Levant Island).
- Frequency modulation radar (FMCWR = Frequency Modulation Continuous Wave Radar) prototype – ROCKWELL COLLINS (RCF) France – for small craft detections – RCF FMCW is the only available prototype in Europe and is actually tested (SESDA station).
- AIS (Automatic Identification System) coastal stations network – DCNS France – stations network were deployed and operated in the frame of the past ScanMaris project (financed by the French Research Agency (ANR)) - for reporting vessel tracking. Note, more and more vessels are equipped with AIS transceiver on boards, not only cargos but also many private yachts and recreational crafts – stations are in SESDA, Levant Island, Séte and 4 shores communication station (Pic de l'Ours (closed to Italian border), Néoulos (closed to Spain border), Cap Siciè (closed to Toulon) and Piana (in Corsica).

The shore based platforms integrate most of existing and advanced sensors for sea surveillance. Sensors are: 3 types of radar (conventional pulse, HFSWR and FMCWR), multi-spectral camera (IR and visible domain) and AIS stations network.

AIS installed on communication station

Multi-static HFSW radar (long range up to 200 nm)

Conventional radar

HR multi-spectral and IR camera

Flat FMCW radar (small boat detection)

Figure 2.I2C shore sensors

These shore platforms allow the testing on how to optimally fuse all the acquired sensor data to generate and maintain tracks for all vessel types.

Sensor cross calibration is also performed to optimise the sensor operation, assess sensor performances and achieve the best sensor data combination / correlation / registration to generate the common operational traffic picture.

IV. MOBILE PLATFORMS

In I2C exercises the mobile platforms and sensors are:

- Instrumented Zeppelin – AIRSHIPVISION France / ZLT ZEPPELIN GmBh Germany / Deutsche ZEPPELIN Reederei GmBh Germany – for large maritime zone surveillance exercises. Sensors such as high resolution optical cameras, radars and AIS receiver can be integrated for exercises, as well as, high data rate telecommunication payload.

  Zeppelin (with crew on board) as any aircraft may not work under all weather conditions, so observation exercises will take into account meteorological forecasts.

  Zeppelin is certified as an aircraft (same legal framework), then flight plans would be prepared in advance and validated by the relevant air traffic authority.

- Instrumented aircraft – Falcon 20 ONERA France - for local node high resolution surveillance exercises. On board certified sensors are radars (X, L and P bands with different beam widths and incidence angles) multi spectral (visible and infrared bandwidths) high resolution camera. This hybrid optical and radar imaging payload can simultaneously acquire different types of data for analysing their best combination to detect cargos and small crafts (fast and slow boats).
- Instrumented vessel – DCNS France - for local node high resolution surveillance exercises. POLARIS2 console is embarked on board to perform local operational traffic picture from the navigation radar and AIS receiver data. Even, abnormal vessel behaviour can be detected from pre-defined suspicious track profiles.
- USV (Unmanned Surface Vessel) platform – SIREHNA France - equipped with an infra-red gyro stabilized video surveillance camera (9.20m, 700 HP RHIB). The USV can be remotely operated from station either on board Zeppelin or vessel patrol or on shore site.

---

[2] *Is an autonomous intelligent operational traffic picture console for patrol vessel: This DCNS prototype is in development and first prototype will be available end 2009. Input data / intelligent information are from vessel conventional navigation radar, AIS receiver and integrated data base.*

USV may not work under all weather conditions, so observation exercises will take into account meteorological forecasts.

USV, for experiment, is manned (licensed pilot) but remotely operated. The pilot is to manually take the control of the USV in any critical situations.

- Processed satellite imagery – JRC Belgium has contributed to numerous application projects in the frame of MASURE actions, to study and extract, from satellite images, useful intelligent information on maritime activities (fishing control, container tracking, etc.) – the processed satellite images is used in I2C for both to derive intelligent information and evaluate the system performances (timely comparison of vessel plots from processed satellite images with the common operational traffic picture elaborated by the shore and deployable platforms). As the extracted information is essentially position of vessel plots, the volume of data is limited and is not required large communication bandwidth for exchange.

Processing of satellite imageries (optical and microwave) to extract vessel plots are performed in I2C by JRC and SPACETEC company.

- Space based AIS – in a couple of year, AIS message services would be provided from commercial providers.

The mobile platforms are used to perform planned exercises (trials) over selected areas of interest in the I2C permanent surveillance zone and its borders. The acquired data permit to elaborate high resolution local traffic pictures which are merged with the wide common operational traffic picture elaborate from the shore platform sensors data.

In addition, the optimal best sensor data combination is also studied and defined to track different types of vessel in various meteorological conditions (night, day, sea states, raining, cloudy, etc.).

Zeppelin 2 tons of payload
(communication, remote sensing and USV guidance)

Falcon 20
3 SAR (X, I & P bands + HR pod multi-spectral & IR

USV (radar + stabilised camera)

Patrol vessel
(radar + AIS + local white picture + satellite communication payload)

Figure 3.Mobile platforms

V. COMMON OPERATIONAL TRAFFIC PICTURE

Common operational traffic picture provides and maintain all vessel tracks (reported and non-reported) in the surveillance zone:
- Generate and maintain vessel tracks (position, cap and speed) from the combination of acquired sensor data (based on tracks correlation and registration methodologies).
- HMI (Human Machine Interface) for visualisation and operator management of vessel tracks on chart and to analyse these tracks.

The challenge is to accurately correlate all vessel plots and tracks generated by all sensors (shore stations and mobile platforms) an exhaustive common operational traffic picture of the reporting (AIS, VMS and camera) and non reporting vessels (radar detections).

The innovation in this capacity is to combine 5 grouped sensors (HFSWR, FMCWR, conventional pulse radar, AIS message and camera images) data into common operational traffic picture. Actual most advanced and existing surveillance systems (SPATIONAV (France), SIVE (Spain), MEVAT (Finland), etc.) combine two sensor data; either conventional coastal radar and AIS messages or conventional radar and camera images. VMS (fishing vessels) confidential data are not combined to other sensor data in any existing systems, they are visualised in separated console in centre monitoring fishing activities. It is to be noted that, in January 2009, most fishing vessels embark AIS transceiver, then, be easily combined within the I2C common operational traffic picture.

The common operational traffic picture is developed by FURUNO Finland and AJECO companies.

VI. COMMON INTELLIGENT OPERATIONAL TRAFFIC PICTURE

From the common operational traffic picture, elaborated and maintained vessel tracks are enriched with information such as vessel activity, vessel characteristics, destinations, meteo / oceano conditions, geographic and regulation environments, etc. To do that, connexions to existing data bases are performed (TRAFIC2000, Lloyd's Register, Paris MOU, ICCAT, t2tanker, e-ship.net, etc.).

Operational weather forecasts will be provided by METEOSIM company.

Dedicated HMI is developed to visualise, to operator, the common intelligent operational traffic picture and visualize the generated alarms (see next section).

The challenge is to append to vessel tracks with heterogeneous information on vessel type, activity, destination, flag, etc. Vessel tracks and all appended information are archived in a long term data base. These data base is, then, used in the next processing step in I2C system to detect abnormal vessel behaviours from implemented rules.

The common intelligent operational picture is developed by KONGSBERG company.

VII. DETECTION OF ABNORMAL VESSEL BEHAVIOUR

From the common operational intelligent traffic picture, generate justified alarms (alarm = detection of abnormal behaviour either related to vessel track and/or ongoing performed activities and/or ambient conditions).

The challenge is to define and apply rules (based on a detection engine using an adaptive multi–agent methodology) for detection of abnormal vessels behaviours from vessel movements, activities, ambient conditions and regulations to automatically propose documented alarms to operator for analysis and validation.

The applied rules can be simple as excessive vessel speed, boarding, etc. as well as sophisticated combination of elementary conditions such as vessels boarding during night and low wave height at 10 nautical miles from shore during 30 minutes and at night.

This capacity does not exist today in any operational surveillance system. Detection of anomalies is performed either from operator analysing on spot the common operational traffic picture or from information on abnormal behaviour observed by person (semaphore operator, vessel captain, aircraft patrol pilot, etc.).

In I2C, rule engine is based on AMAS (Adaptive Multi–Agent Systems developed by IRIT (Institut de Recherche Informatique de Toulouse) and existing rule engine developed by Clear Priority company to automatically detect abnormal vessel behaviours. A tactile HMI (Human Machine Interface) is developed to visualise the justified alarms and to allow the operator to validate it. This new interface generation is developed by INTUILAB company and all geographical tools provides by ARMINES laboratory.

This capacity is based on R&D development performed in the frame of the ScanMaris project (Surveillance et Contrôle des Activités des Navires en Mer). This project has been financed in 2007 by the French Research Agency (ANR), conducted by DCNS the project ended is in January 2010.

VIII. IDENTIFICATION OF THREATS

Identify ongoing threats associated to alarms on detected abnormal vessel behaviours (under coordination of DCNS with the support of INTUILAB company, ONERA and ARMINES laboratories) is mainly an open collaborative human main machine interface and tools to expertise on going alarms, identify associated threat and elaborate periodic interpretation electronic reports. These reports files are forwarded to authorities to keep them informed on the threat evolution and for timely decision making.

The challenge is to develop supporting tools and use multi-users, multi-pointers tactile interface device (based on a first prototype developed by INTUILAB) for collaborative experts group to understand suspicious event (multi - hypothesis decision tree based on ontology methodology and archived knowledge models from past analysed suspicious events), identify associated threat and elaborate periodic interpretation reports for authorities These tools, with experts (human factor) in the loop, shall be integrated in friendly collaborative / interactive interface devices to build up periodic and standardized / classified interpretation electronic reports during the duration of the suspicious event.

That functionality does not exist at all in any current maritime surveillance operational systems. Today, for each suspicious event, peculiar crisis cell is instanced to support authority to analyse the situation and decide actions to plan.

This capacity is based on preliminary R&D development achieved in the frame of the TaMaris project (Traitement et Authentification des Menaces et Risques en Mer). This project has been financed in 2008 by the French Research Agency (ANR). Conducted by DCNS the project end is in January 2011.

IX. TELECOMMUNICATION NETWORK

Two telecommunication technologies are deployed for I2C:
- Light DVB (Digital Video Broadcast) station to demonstrate that selected sensor data can be forwarded, in quasi real time, from any one site to another.
- DSiP (Distributed Systems intercommunication Protocol) router to demonstrate that sensor data flows, traffic pictures, justified alarm, periodic threat interpretation reports, etc can be disseminated to any user centre and deployed sensor remotely operated (operating modes configuration, parameters tuning, optical camera pointing, etc.). A DSiP router can also be a telecommunication node in virtual private network.

Data exchange based on telecommunication satellite (DVB) and DSiP protocol / control is an innovative approach and concept which is a necessary first step to demonstrate system of systems secured and protected interoperability.

The deployed telecommunication network to transfer justified alarms and periodic interpretation reports, on detected suspicious events / identification of threats, to external user organisations (i.e. FRONTEX, EMSA, DAM Operational Centre, etc.) is also demonstrating future secure links, useful decisional information exchange for future (2015) common multi national / European trans border missions.

X. USER COMMITTEE

To support the industrial consortium an active and permanent end users committee is settled to:

- Express operational needs and detail applications to be performed in 2015 horizon.
- Advice the I2C engineers.
- Define testing scenarios (abnormal vessel behaviours and suspect events).
- Support exercises.
- Deeply participate in the 1.5 year exploitation of the integrated capacities and assess the system outcomes.
- Provide end user feedbacks on I2C performances and usefulness for 2015 sea border surveillance and situation awareness.

The permanent committee includes the following participants (end users):
- FRONTEX (To Be Confirmed) representative (Consortium letter will invite FRONTEX to assist to the end user committee meetings when I2C will be kick-off; expected date is July 2010).
- French DAM (Direction des Affaires Maritimes). DAM is operating five regional centres (CROSS) monitoring the French territory waters (Channel, Atlantic and Mediterranean).
- ScanMaris and TaMaris other end users (Gendarmerie Maritime, CETMEF and Centre des Opérations de la Marine (COM)).

During the project other country organisation (Portugal, Spain, Greece, etc.) end users will be invited to participate. European plenary meetings will be organised, at least at each project phases (specification, architecture, development and exercises) to disseminate the project results and collect add on operational requirements, as well as potential improvement requested by the end users. The following list provides these end user organisations:
- Portugal GNR (Guardia National Republicana).
- Spain GC (Guardia Civil).
- Italy MbSAS (Ministry of Internal Affais)..
- Finnish Border Guard (Rajavartiolaitos)
- Hellenic Coast Guard MRCC (Maritime Rescue Coordination Centre).

In addition, during the project, two large plenary conferences will be organised with end user communities.

JRC (the Institute for the Protection and Security of the Citizen of the Joint Research Centre –European Joint Research Centre) and ECOMER company will manage the user committee for user requirements specification and to organise the two large conferences.

Acknowledgment