« SARGOS »
Securing Offshore Infrastructures Through a Global Alert and Graded Response System

Marie-Annick GIRAUD[1], Benjamin ALHADEF[1], Franck GUARNIERI[2], Aldo NAPOLI[2], Michel BOTTALA-GAMBETTA[3], Denis CHAUMARTIN[4], Michel PHILIPS[4], Michel MOREL[5], Christophe IMBERT[6], Eric ITCIA[6], David BONACCI[7], Patrice MICHEL[7]

[1] SOFRESUD, 777 av. de Bruxelles, 83500 La Seyne sur Mer
[2] ARMINES/CRC, Rue Claude Daunesse, 06904 Sophia Antipolis
[3] CDMT, 3 avenue Robert Schuman, 13628 Aix en Provence Cedex 1
[4] CS Communication & Système, 230 Rue Marcellin Berthelot, 83130 La Garde
[5] DCNS Division Systèmes d'Information et de Sécurité, BP 403, 83055 Toulon Cedex
[6] ROCKWELL COLLINS France (RCF), 6 avenue Didier Daurat, BP 20008, 31701Blagnac Cedex
[7] TéSA, Télécommunications Spatiales et Aéronautiques, 14-16 Port Saint Etienne, 31000 Toulouse.

magiraud@sofresud.com ; benjamin.alhadef@sofresud.com ; Franck.Guarnieri@crc.ensmp.fr, Aldo.Napoli@crc.ensmp.fr ; denis.chaumartin@c-s.fr; michel.philips@c-s.fr ; secretariat.cdmt@univ-cezanne.fr ; michel.morel@dcnsgroup.com ; cimbert@rockwellcollins.com; eitcia@rockwellcollins.com; david.bonacci@tesa.prd.fr; patrice.michel@tesa.prd.fr

Abstract The purpose of the project SARGOS is to develop a global alert and graded response system to answer the recent but strong need for securing critical civilian offshore infrastructures, vulnerable to piracy or terrorist actions from the sea.
The challenge of protecting these infrastructures against malevolent intrusions requires to develop innovative strategies so as to ensure in a coordinate way the whole processing line: automatic surveillance, robust detection, continuous adjustment of the reaction plan and graded implementation of the relevant set of reactions.
The system handles

- Automatic and robust detection and classification of small size maritime targets in rough sea;
- Detection of suspicious behaviors in a security zone around the platform;
- Formalization and modeling of graded internal and external reactions, adapted to the dangerousness of the detected intrusion and taking into account security rules in force on the platform, geopolitical environment and legal aspects;
- Activation of progressive and reversible reactions, according to an intelligent situation analysis process. Reactions can go from a simple alert up to bringing non lethal reaction means into play.

The project will materialize with the implementation of all the processing line in a single platform that will be used to carry out experimentations and to validate the overcoming of critical issues and the appropriateness of the proposed concept with regards to users needs.
SARGOS has been selected by the French National Research Agency (ANR) in the frame of their 2009 global safety program (CSOSG).

1. Introduction

Offshore oil installations are critical energy infrastructures worldwide. They so constitute privileged targets for terrorist or piracy actions coming from the sea.

After the events of September, 2001, the strengthening of maritime security has become a top priority for all governments. This materialized with the definition and the ratification of the international ISPS code, a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. But even in this context, setting up appropriated security measures for direct protection of each oil platform is still a matter for oil & gas industry responsibility.

Offshore platforms are currently equipped with conventional navigation radars used for surveillance purposes. These equipments are not suited to detect small threats (such as dinghies, speedboats, or jet-skis) which might look for colliding with or grappling platforms or ships undergoing loading in oil or gas terminals. Besides, when facing a real intrusion, there are no or few formalized rules so as to react using safety procedures and setting up autonomous dissuasive means.

It thus turns out essential to increase the degree of protection of these infrastructures by developing a new system capable of generating alarms and of setting off appropriate internal and external reactions in case of a confirmed intrusion.

The project SARGOS aims to satisfy this new need of protecting civilian offshore infrastructure vulnerable to terrorist or piracy actions led from sea

The objective is to propose an innovative global system allowing surveillance and protection of strategic offshore infrastructures, by taking into account the whole processing line, from threat detection up to bringing into play reaction procedures adapted to the intrusion dangerousness.

2. Issues

2.1 Stakes

« Clearly, energy security is among the most serious security and economic challenges both today, and in the future. As the economies of the World grow and societies develop, so does the importance of energy. And so does the importance of the infrastructures that produce and supply this energy. Critical energy infrastructures provide the fuel that keeps the global economy moving and our societies working.

These are the very words addressed by the OSCE (Organization for Security and Cooperation in Europe) in the starting speech of the reinforced NATO Economic Committee Meeting held on September 22nd 2008 in Brussels.

Several disasters have already demonstrated the vulnerability of energy production infrastructures and the pressing need for a high rigor in system conception and procedures respect. As regards to offshore facilities, one must remember events such as "Piper Alpha" (July 1988) in which only 62 of the 229 crew members survived the consequences of explosions worsen by a series of human errors, or more recently "Macondo" (April 2010) with the explosion of oil rig Deepwater in Mexico Gulf.

Offshore oil activity already supplies a third of the world supply and is still growing, unlike the same activity onshore. Oil companies currently concentrate their efforts on exploration and offshore production activities, which go rising : In the mid term, more than half of the extracted oil and gas will come from offshore or deep offshore fields (up to 2000 meters and soon 3000 meters)

In 2010, there are approximately 3300 offshore oil wells throughout the world and about 420 fixed and floating offshore platforms have been built. The oil drilling market represents about 40 G$ and that of engineering, equipments and offshore construction counts for approximately 50 G$

One must admit that even though offshore infrastructures are designed to face extreme natural environments, they are not sufficiently protected against deliberate malevolent actions. Offshore platforms constitute an accomplished industrial network with regards to exploitation but as far as safety /security aspects are concerned, they represent isolated targets exposed to intrusions from the sea.

The preservation of offshore oil installations integrity is thus a major stake at the word level. This leads to wonder about the consequences that could follow from the conjunction of terrorism and piracy, nowadays active even in remote maritime areas, on the energy supplying chain.

2.2 Context

Faced with the increasing scarcity of resources onshore, oil companies have first made a tactical repositioning in offshore production units.

When Jenkins established in 1988, using return of experience at that time, the first typology of threats straining on oil platform, the risk of hostage taking was considered as particularly low because of the nature of the needed means and of the difficulty to reach a platform on the open sea.

Since 1988, piracy has taken a considerable extent. Kashubsky (2008) led a very detailed survey on Nigeria which shows that the hypothesis according to which the offshore installations would be protected from the very fact of their remoteness does not stand any more. Events such as the attack in June, 2008 of Shell offshore infrastructures 120 km off Nigeria coast ("Bonga" oil field) or the attack in May, 2009, of TOTAL platform in the "Amenan" oil field demonstrate that the distance doesn't guarantee a complete security any more.

While ship boardings are multiplying (2008 and 2009 are marked by an unprecedented increase of ship hijackings at sea), examples of offshore energy infrastructures attacks remain for the moment less frequent and get less media attention. But they are extremely worrying as they reveal a high vulnerability. For example, between mid 2006 and mid 2008, Jenkins finds more than twenty act of piracy only on Nigeria. Since then, we can in particular mention:

- 19th June, 2008: Attack of "Bonga" oil field by armed men with speedboats. Several persons wounded. Closure of the field which counts for 10 % of the Nigerian production with approximately 225 000 barrels a day. Impact felt on the rise in prices worldwide.
- 31st October, 2008: Attack of "Sagitta", an offshore supply ship (owned by Bourbon) by heavily armed pirates in Cameroon - 10 persons kidnapped.
- 07th January, 2009: Attack of an Exxon Mobil oil platform by armed men in a flat bottom ship "Money and valuables theft.
- 23rd January, 2009: Attack of an offshore supply ship by 10 armed men in 2 speedboats " Money and valuables theft.
- 26th May, 2009: Attack against an installation of the French company TOTAL on "Amenam" oil field in Nigeria.
- 22nd September, 2010: 3 French employees of Bourbon are taken hostage off Nigeria ("Addax" oil field).
- November 2010: 19 hostages taken in the delta of Niger during a raid on a boat and an oil platform of Afren company (among whom appear two French people, two Americans, two Indonesians and a Canadian) " 8 Nigerians kidnapped during an attack on an ExxonMobil installation
- 17th November, 2010: pirates embarked on a speedboat attacked a boat of the French company Perenco which transported Cameroonian security forces, near an oil platform in the Gulf of Guinea (6 people killed).

2.3 Need

The few examples above reveal the incapacity of the systems currently available and implemented on offshore infrastructures to protect them against hostile intrusions such as piracy.

Offshore installations security is nowadays ensured by "classic" means (lookout, radio identification, AIS, traffic surveillance radar and resort to surveillance boats generally operated by subcontracting companies)

Traffic surveillance radars are intended to detect first and foremost cooperative mobile of large or intermediate sizes. Their performances are considered insufficient to detect small marine targets with small radar or optronic signature, of course not cooperative (absence of radar reflector or AIS), and moving around in rough sea. They are also penalized by a blind zone closed to the carrier.

VTS (Vessel Traffic Surveillance) systems allow to secure the commercial navigation by supplying a real-time image of ships movements in a given surveillance zone. Although they are widely operational, on the one hand their usual modes of detection are more particularly adapted to "cooperative" boats and on the other hand their maritime traffic management purpose is very different from the concept of protection against small boats hostile intrusion.

The operational need is thus to have (as an applicative layer over VTS's systems) a response-making system dedicated to offshore platforms protection, while being integrated within the existing systems both those of production infrastructures management and those of various means management: **this is the purpose of SARGOS system**.

SARGOS exploits all detection means among which VTS information associated with other information specific to the platform and its internal (topology, staff, operations in progress, etc.) as well as external (political context, expected ships, meteorology, local and international events, etc.) environment.

SARGOS brings in real time to operators a decision-making support by informing of threats and by running predefined reactions procedures adapted to the context.

3. SARGOS

SARGOS system aims to ensure protection of crucial offshore infrastructures (such as oil platform) against surface threats. This encompasses:

- Detection of threats using a specific frequency modulated continuous wave (FMCW) radar and other sensors;
- Processing of the detected threat in order to estimate its dangerousness and to define the appropriate response;
- Implementation of a gradual and reversible reaction process;

according to the following block diagram (cf. Figure 1).

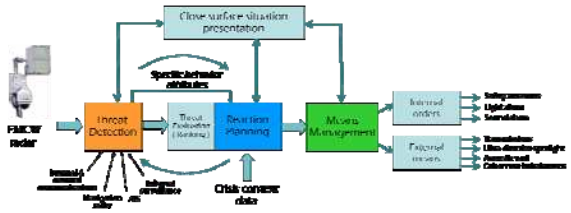

Figure 1 : SARGOS block diagram

It should be noticed that SARGOS supplies the alert from a system core based on its innovative FMCW radar technology but SARGOS is also capable of taking into account all other available external data (navigation radar tracks, AIS information, thermal images, external communications, etc.) as and whenever needed, in order to set up a planned and gradual reaction process.

3.1 General design

SARGOS system includes sensors, processing and reaction. It is set up on an offshore platform and is adapted to the specific platform configuration. It is made available to the person in charge of the platform safety.

3.1.1 Sensors

The main sensor is a FMCW radar specifically designed to detect small marine targets at ranges up to 4 nautical miles. A detailed analysis of the radar echo allows classifying it. A degree of dangerousness is deducted using additional information collection.

It should be noticed that the system is capable of taking into account external data supplied by internal and external communications means, navigation radars, AIS systems and infrared sensors.

3.1.2 Processing

The information provided by the FMCW radar and associated sensors is processed to define the degree of dangerousness of the target, to activate a possible alert with an appropriate priority and to define the protection means to be operated from the SARGOS "reaction planning" .

SARGOS operating station is used to display the maritime traffic picture with suspicious tracks on the relevant cartographic map, and to carry out general administration of the system.

3.1.3 Implementation

The reaction means management module commands and controls internal and external alerts, passive safety / security means and non lethal deferent reaction means, such as light projectors, sound artillery, etc.etc.

3.1.4 Detection and processing logic

SARGOS addresses the challenge of closed maritime protection against small boats. The problem is characterized by (a) the difficulty to detect such intrusions with classical surveillance means and (b) a short response time

SARGOS proposes an innovative approach to characterize an alert, by developing a behavior analysis logic based on the gradual crossing of stages in a real-time universe.

The logic of detection and processing of an intrusion is presented on figure 2.

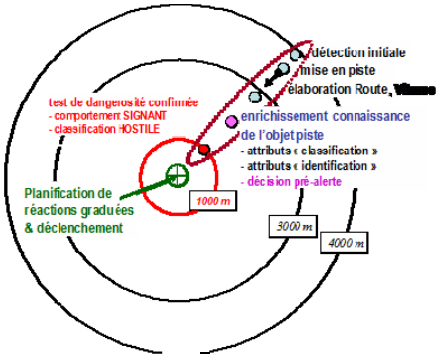

Figure 2**:** Intrusion detection and processing

Mobiles detected in a predefined perimeter around the platform are tracked to elaborate kinematic information. The knowledge of each object "track" is gradually enriched using classification attributes (characterizing the nature of the detected object) and identification attributes (characterizing the class of identity of the same object), on the basis of which the dangerousness represented by the mobile is estimated

3.2 Functional architecture

SARGOS system consists of several functional blocks (cf. Figure 3).

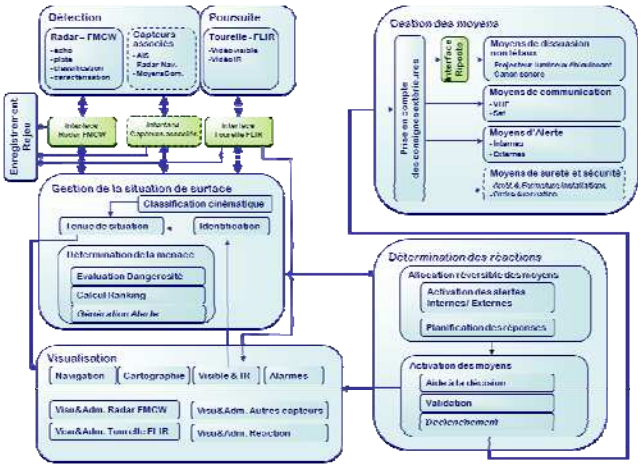

Figure 3: System architecture

3.2.1 Detection

Surveillance of the areas surrounding the offshore platform is carried out by using:

- detections obtained with the specialized FMCW radar of the SARGOS system, when facing with small crafts, skiffs, specific floating machines (over-motorized dinghies) and regular ships;
- Information collected by sensors associated to SARGOS FMCW radar: conventional navigation radar, IR PTZ camera, AIS system, communication means.

The FMCW radar ensures in particular the localization of detected echoes, their tracking and the calculation of the tracks kinematics, their classification, the transmission of the various attributes of the tracked objects to the preferential radar subscribers (radar technical function, operational station) and data exchange with the "surface situation management" function.

The "surface situation management" function ensures acquisition and association of information needed to establish a closed operational picture, information processing so as to define the "identity class" of the detected echo and to determine the threat according to the three following stages:

- dangerousness evaluation , based on a crossed analysis of the identity class of the detected mobile and the position of the detected intrusion with regard to the safety perimeter defined around the offshore platform;
- threat ranking calculation using detected mobile parameters such as distance, speed and route,
- analysis of the threat characterization parameters in order to assess the need for activating or not a "dangerous intrusion" alert

3.2.2 Reactions

The "dangerous intrusion" alert generated by the "surface situation management" function is forwarded to the "reactions determination" function which implements:

- Possible reactions planning calculations according to the level of knowledge acquired on various detected threats (behavior criteria, identity classes, and comparison of the current real time situation with previous situations met and stored by the system). These calculations take into account possible limitations due to the territorial situation or the legal status of the platform;
- Recommendation for activating reaction means, proposition subjected to the validation of the operating station operator. The role of this operator is to state on the relevance or non-relevance of sending a retort instruction to the "means management" module;
- Activation of an in-house alert broadcasting process;

- Activation of an outside alert broadcasting process using normalized message generation in order to inform onshore authorities about the nature of the intrusion and the corresponding degree of nuisance.

3.2.3 Means management

The point is to elaborate operative sequences from the received retort orders:

- Blocking of the entry points;
- Putting goods and persons under protection;
- Carrying out of non lethal deterrent effectors (sound orders, spotlights);
- Carrying out of non lethal neutralization means (paralyzing acoustic system or other);
- Carrying out of outside communications (VHF, satellite links) in order to transmit alerts related to real threats and information on their nature

3.2.4 Visualization and Actions

The operating station is the interface between SARGOS and the offshore platform manager. It enables the panoramic display of system tracks on the close platform surface situation. It gives the operator decision-making means as well as action means (validation of the gradual responses proposed by the system and authorization of setting off the recommended set of reactions).

3.2.5 Record &Replay

The operational functions of SARGOS are completed by recording and replay capacities.

Replay allows the analysis of functioning logic based on operational test scenarios, especially during the development phase.

Detections and reactions recording has several purposes:

- To distinguish real threats from false alarms by retrospect analysis;
- To provide proof;
- To pass data to other entities for prevention purposes,
- To evaluate the efficiency and the relevance of activated reactions (internal / external)

Such a posteriori data based on feedback are quite valuable for insurers or financiers who need objective statistics in order to quantify risks.

3.3 System implementation

SARGOS proposes an automated process to analyze situations, to set off alerts and to elaborate plans with progressive and reversible reactions to be implemented. The system brings three phases into play:

- Stage 1 : Automatic surveillance

At first, the system is stand-alone. SARGOS monitors the surface situation with tracks provided by various sensors, and estimates the dangerousness of each craft navigating near the platform. When the level of dangerousness reaches a threshold, the system leaves the "Automatic surveillance" phase to enter the "Alert" phase.

- Stage 2 : Alert

One of the system tracks reaches a level of dangerousness above the alert threshold: the operator assessment is required. An alarm is generated so as to warn the operator about the detected risk. The system video cameras are turned toward the threat in order to propose visu.al identification means

- Stage 3 : Processing

The system enters the "reactions processing"

The operator has been acquainted with the situation; he has confirmed and identified the threat. The system enters the reactions processing phase. The system proposes to the operator a reaction plan based on the threat nature and on the time required to carry on these reactions.

4. Operating Station

First and foremost, SARGOS addresses the issue of surveillance and protection of civilian infrastructures: the system shouldn't require dedicated staff devoted to people and goods protection; it has to remain compatible with exploitation by a non-specialized operator having for first objective the daily oil production and being potentially put under stress if confronted to a crisis situation.

To assure a fast and comprehensive apprehension of the situation, SARGOS information is displayed on two adjacent screens:

The first screen shows (cf. Figure 4):

- The tactical surface situation displayed on a map enriched with relevant maritime information, detected ships sorted regarding their dangerousness;
- A decision making support presenting the plan of reaction elaborated using reaction modeling approaches.

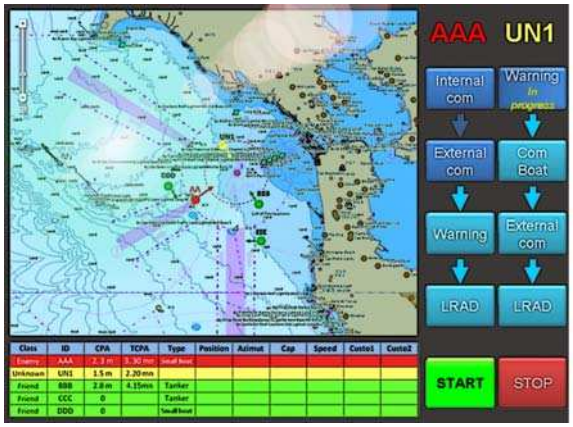

Figure 4 : Operating station "Surface situation management screen"

The second screen is reserved for video camera imaging in order to allow threat identification. It is divided into 3 areas:

- The banner is used to display either the current panoramic view of the scene, or an historical background allowing to show to the operator pictures captured before he arrived;
- A close view focused on the detected threat, so as to enable the operator to validate the class of craft and the threat identity class;
- A close IR view complementing the day vision to improve threat identification.

Figure 5: Operating station – Identification screen

5. Conclusion

The challenge of protecting critical civilian infrastructures against malevolent intrusions requires developing innovative strategies so as to ensure in a coordinate way the whole processing line: automatic surveillance, robust detection, continuous adjustment of the reaction plan and graded implementation of the relevant set of reactions.

SARGOS proposes a global alert and graded response system, and so answer the recent but strong need for securing civilian offshore infrastructures, vulnerable to malevolent acts, piracy or terrorism from the sea.

The system handles:

- Automatic and robust detection and classification of small size maritime targets in rough sea;
- Detection of suspicious behaviors in a security zone around the platform;
- Formalization and modeling of graded internal and external reactions, adapted to the dangerousness of the detected intrusion and taking into account security rules in force on the platform, geopolitical environment and legal aspects;
- Activation of progressive and reversible reactive actions, according to an intelligent situation analysis process. Reactions can go from a simple alert up to bringing non lethal reaction means into play

The project will materialize with the implementation of all the processing line in a single platform that will be used to carry out experimentations and to validate the overcoming of critical issues and the appropriateness of the proposed concept with regards to users' needs.

This transversal and systemic approach relies on multidisciplinary competences, capitalized into the consortium SARGOS. This consortium is composed of well fitted and complementary skills with a SME as coordinator (SOFRESUD), 3 industrial entities (DCNS, Rockwell Collins France and CS SI), and 3 research organisms (TéSA, ARMINES/CRC and CDMT) with the support of public bodies (DGA Techniques Navales).

Work is made under the aegis of a steering committee which includes representatives of two main French oil and gas companies TOTAL and GDF Suez, of the DGA and the French Navy, also gathered into a users committee which is sought to communicate the need, to strengthen the technical objectives, to validate the chosen scenarios and to assess the relevance of the obtained results.

Acknowledgment

SARGOS has been selected by the French National Research Agency (ANR) in the frame of their 2009 global safety program (CSOSG).

The authors would like to thank the French National Research Agency for their financial support.

References

[1] Honeywell. *Maritime Security: Meeting Threats to the Offshore oil and Gas Industry* – May 2008

[2] Thales Group *Security Solutions for the oil and Gas Industry*

[3] *Securing Oil & Gas Assets* Society of Petroleum Engineers, 20-22 Oct. 2008

[4] Jenkins B.M; (1988). *Potential threats of offshore platforms. Rand Corporation*, 1988

[5] Kashubsky M. (2008). *Offshore energy force majeure: Nigeria's local problem with global consequences*. Maritime studies, May-June 2008.

[6] A. Sanière, S. Serbutoviez, C. Silva *Les investissements en exploration-production et raffinage* IFP Energies Nouvelles, Oct. 2010

[7] MA. Giraud, A. van Gaver, A. Napoli, C. Scapel, D. Chaumartin, M. Morel, E. Itcia, D. Bonacci *SARGOS, Système d'Alerte et de Réponse Graduée OffShore* Workshop Interdisciplinaire sur la Sécurité Globale (WISG10), Troyes, janvier 2010

[8] P. Georgé, JP. Mano, MP. Gleizes, M. Morel, A. Bonnot, D. Carreras. *Emergent Maritime Multi-Sensor Surveillance Using an Adaptive Multi-Agent System (regular paper)* Cognitive systems with Interactive Sensors (COGIS 2009), Paris, 16/11/2009-18/11/2009, SEE/URISCA, (support électronique), novembre 2009

[9] F. Jangal, JP. Georgé, A. Bonnot, MA. Giraud, M. Morel, A. Napoli. *Toward a complete system for surveillance of the whole EEZ: SCANMARIS and associated projects.* Oceans'09, Biloxi, Mississippi, USA, 26/10/2009-29/10/2009

[10] A. Littaye, MA. Giraud, JP. Mano, A. Bonnot, A. Napoli, M. Botalla, F. Jangal, M. Morel. *SCANMARIS : détection des comportements anormaux des navires* Workshop Interdisciplinaire sur la Sécurité Globale (WISG09), Troyes, 27/01/2009-29/01/2009

[11] M. Morel, A. Napoli, A. Littaye, MP. Gleizes, P. Glize. *ScanMaris: an Adaptive and Integrative Approach for Wide Maritime Zone Surveillance*. Cognitive systems with Interactive Sensors (COGIS 2007), Stanford University California USA, 26/11/2007-27/11/2007, p. 1014, 2007

[12] A. Littaye, M. Morel, A. Bonnot, A. Napoli, JP. Georgé, MA. Giraud, F. Jangal, M. Botalla. *Trafic Maritime : détection des comportements anormaux é des navires.* Journées scientifiques et techniques du CETMEF Paris 8, 9 et 10 décembre 2008

[13] M. Morel, A. Littaye, C. Saurel, O. Poirel, A. Napoli, S. Valle, G. Proutière-Maulion. *TAMARIS, Traitement et Authentification des MenAces et RISques en mer* ; Workshop Interdisciplinaire sur la Sécurité Globale (WISG09), Troyes, 27/01/2009-29/01/2009.

[14] M. Morel, C. Saurel, O. Poirel, P. Salom, A. Napoli. *TAMARIS*. MAST 2009, Stockholm, Suède

[15] D. Chaumartin, J. Déon, C. Granet, M. Grimaldi, Y. Lacroix, G. Tedeschi. *Maritime Warning and Protection System* Actes colloque WISG'09 (Janv. 2009).

[16] D. Chaumartin *Maritime Warning and Protection System.* Journées scientifiques et techniques du CETMEF Paris 8, 9 et 10 décembre 2008.

[17] C. Andrieu, M. Davy, A. Doucet. *Efficient Particle Filtering for Jump Markov Systems. Application to Time-Varying Autoregressions*, IEEE Trans. On Signal Processing, Vol. 51, No. 7, pp 1762-1770, July 2003.