SARGOS : Système d'Alerte et Réponse Graduée Off Shore

Marie-Annick Giraud, Benjamin Alhadef, Franck Guarnieri, Aldo Napoli, Michel Bottala-Gambetta, Denis Chaumartin, Michel Philips, Michel Morel, Christophe Imbert, Eric Itcia, et al.

▶ **To cite this version:**

Marie-Annick Giraud, Benjamin Alhadef, Franck Guarnieri, Aldo Napoli, Michel Bottala-Gambetta, et al.. SARGOS : Système d'Alerte et Réponse Graduée Off Shore. Conférence WISG - Workshop Interdisciplinaire sur la Sécurité Globale, Jan 2012, Troyes, France. 8 p. hal-00778616

HAL Id: hal-00778616

https://minesparis-psl.hal.science/hal-00778616

Submitted on 26 Jul 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

« SARGOS »
Système d'Alerte et Réponse Graduée Off Shore

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

Résumé – Les champs de production d'hydrocarbures deviennent de plus en plus une cible de choix pour la piraterie maritime voire la menace terroriste. Or si les plates-formes et navires associés forment un réseau industriellement abouti en ce qui concerne l'exploitation, ils sont démunis face aux actes de malveillance intentionnels : de ce point de vue, ce sont des cibles isolées et exposées.

Le projet SARGOS vise à répondre à l'émergence du besoin de sûreté des infrastructures offshore civiles vulnérables aux actions de malveillance, de piraterie ou de terrorisme menées à partir de la mer. Il propose le développement d'un système assurant de manière coordonnée la chaîne globale de protection : veille et surveillance automatisées ; détection d'intrusion ; évaluation de dangerosité ; plan de réaction gradué et piloté en temps réel pour rester constamment adapté au niveau de menace représenté par l'intrusion détectée.

Une des capacités clefs est l'élaboration d'une stratégie complète et mutualisée de défense, incluant la mise en sûreté des personnes, la diffusion de l'alarme, la coordination des moyens d'assistance extérieure et la mise en œuvre de moyens de dissuasion non létaux. Un enjeu fort est mis sur la prise en compte des modes de fonctionnement de l'infrastructure et des contraintes règlementaires et juridiques.

SARGOS apporte une réponse nouvelle et innovante dans ce domaine de la sûreté maritime pour lequel il n'existe pas aujourd'hui de système opérationnel.

Après un rappel de la problématique, cet article fait le point sur les différentes approches innovantes mises en œuvre dans le développement du projet.

Abstract – Offshore energy installations are becoming privileged targets for maritime piracy actions or even acts of terrorism. Offshore oil platforms and associated vessels constitute an accomplished industrial network with regards to exploitation but they are powerless when facing deliberate malevolent actions: they are isolated targets exposed to intrusions from the sea.

SARGOS project aims to satisfy the strong emerging need to improve the security of civilian offshore infrastructures, vulnerable to spiteful, piracy or terrorist actions led from the sea. The project proposes development of a new global system ensuring in a coordinate way the whole protection line: automated watch and surveillance, detection of intrusions, dangerousness assessment, graduated response plan driven in real time so as to stay continuously adapted to the level of threat associated with the detected intrusion.

A key capability is the development of a comprehensive and innovative defense strategy, which includes putting goods and persons under protection, alert broadcasting processes, coordination of external assistance and carrying out of non-lethal deterrent means. Another major aspect is to comply with the infrastructure operational ways of doing things and legal and regulations constraints.

SARGOS brings a new and innovative answer in the domain of maritime security for which there is currently no other operational system.

After a review of the issue, this article focuses on the innovative approaches developed to carry out the project.

1. Introduction

Les installations parapétrolières offshore sont des infrastructures énergétiques cruciales à l'échelle mondiale. A ce titre, elles constituent des cibles privilégiées pour des actions terroristes ou de piraterie en provenance de la mer.

Le renforcement de la sécurité maritime est devenu une priorité majeure des gouvernements après les événements de septembre 2001. Il s'est concrétisé notamment par la définition et la ratification du code international ISPS. Mais même dans ce contexte, la protection directe de chaque plate-forme à travers la mise en place de mesures de sécurité appropriées in situ relève toujours de la responsabilité industrielle.

Sur ces sites, le moyen de surveillance de base demeure le radar à impulsions de veille côtière ou de navigation, non adapté à la détection de la menace constituée par des esquifs ou des engins nautiques rapides et de faibles dimensions chargés d'explosifs (de type dinghy, vedette rapide ou « jet ski ») qui rechercheraient la collision ou l'abordage avec la plate-forme ou les navires en cours de chargement dans un terminal pétrolier ou gazier. En outre lors d'une intrusion avérée, il n'y a pas ou peu de règles formalisées pour réagir par des procédures de sauvegarde et par la mise en œuvre de moyens de dissuasion autonomes.

Il s'avère donc primordial d'augmenter le degré de protection de ces infrastructures en développant un nouveau système capable de générer une alarme et d'enclencher des réactions internes et externes en cas d'intrusion confirmée.

Le projet SARGOS répond à ce nouveau besoin de protection d'infrastructures civiles vulnérables aux actes de piraterie ou de terrorisme menées à partir de la mer.

L'objectif est de proposer un système global innovant permettant la surveillance et la protection d'infrastructures sensibles en mer, en prenant en charge toute la chaîne de traitement, depuis la détection de la menace jusqu'à la mise en œuvre de procédures de réaction adaptées au niveau de dangerosité de l'intrusion détectée.

2. Problématique

2.1 Enjeux

« La sécurité énergétique fait partie des challenges économiques et sécuritaires les plus sérieux, aussi bien aujourd'hui que dans le futur. La croissance des économies du monde et des sociétés va de pair avec l'importance de l'énergie et de pair avec les infrastructures qui produisent et fournissent cette énergie. Les infrastructures énergétiques critiques fournissent le carburant qui permet à l'économie globale d'avancer et à nos sociétés de fonctionner ».

C'est en ces termes que s'est ouverte l'allocution de l'OSCE (Organization for Security and Cooperation in Europe) lors de la réunion du comité Economique de l'OTAN du 22 septembre 2008 à Bruxelles.

Plusieurs catastrophes ont démontré la vulnérabilité que peuvent avoir de telles infrastructures et l'impérieuse nécessité d'une profonde rigueur dans le respect des procédures et la conception des systèmes. Pour ce qui concerne les infrastructures offshore, on doit citer entre autres « Piper Alpha » (6 juillet 1988) dans laquelle seuls 62 des 229 membres d'équipage ont survécu aux conséquences d'explosions aggravées par une suite d'erreurs humaines puis tout récemment « Macondo » (20 avril 2010) par la plateforme de forage Deepwater dans le Golfe du Mexique.

Fournissant déjà environ le tiers de l'approvisionnement mondial, l'activité parapétrolière offshore est en forte croissance à l'inverse de cette même activité en onshore. Les compagnies parapétrolières concentrent à présent la majorité de leurs efforts sur les activités d'exploration et de production offshore qui vont en s'accroissant : à moyen terme plus de la moitié du pétrole et du gaz seront extraits de l'offshore et particulièrement de l'offshore profond (jusqu'à 2000 mètres et prochainement 3000 mètres).

En 2010 il existe environ 3.300 puits forés en mer de par le monde et il s'est construit environ 420 plates-formes offshore, fixes et flottantes. Le marché du forage représentait environ 40 G$ et celui de l'ingénierie, des équipements et des constructions en mer environ 50 G$

Il faut bien reconnaître qu'alors même que ces infrastructures sont conçues pour affronter des environnements naturels extrêmes, elles ne sont pas suffisamment protégées face aux actes de malveillance intentionnels. Les plates-formes offshore forment un réseau industriellement abouti en ce qui concerne l'exploitation mais du point de vue de la sécurité, elles représentent des cibles isolées et exposées à des intrusions à partir de la mer.

La préservation de l'intégrité des installations pétrolières offshore est donc un enjeu majeur à l'échelle mondiale[1], et amène à s'interroger sur les conséquences qui peuvent découler de la conjonction de la piraterie et du terrorisme, aujourd'hui actifs même en haute mer, pour la sécurité d'approvisionnement énergétique.

2.2 Contexte

Face à la raréfaction de la ressource pesant sur les infrastructures énergétiques terrestres, les compagnies

[1] A titre d'exemple, on peut rappeler l'impact du cyclone Katrina sur le marché de l'énergie : alors que moins de 5% des plates-formes du golfe du Mexique sont détruites ou sérieusement endommagées, au lendemain de la catastrophe, les tensions sur les marchés pétroliers couplées à l'incertitude sur l'approvisionnement suscitée par l'absence de renseignements, font que le prix du baril enregistre un nouveau record et atteint la barre des 70 $, le prix du super augmente de 30%... Afin de restaurer la confiance dans le marché pétrolier, l'AIE est contrainte de mener une action collective et les pays membres sont invités à puiser dans leur réserves stratégiques 2 millions de barils par jour pendant 30 jours.

pétrolières avaient dans un premier temps effectué un repositionnement tactique sur des unités de production en offshore.

Lorsqu'en 1988 Jenkins établit, en se fondant sur le retour d'expérience, la première typologie des menaces qui pèsent sur les plateformes pétrolières, le risque de prise d'otage est estimé à particulièrement faible de part la nature des moyens qu'il conviendrait d'engager et la difficulté à accéder à une plateforme en pleine mer.

La piraterie a depuis 1988 pris une ampleur considérable. Kashubsky (2008) a ainsi conduit une étude très détaillée sur le Nigeria qui montre que l'hypothèse selon laquelle les installations offshore seraient protégées du fait même de leur éloignement ne tient plus. L'attaque en juin 2008 des infrastructures offshore de Shell à 120 km au large des côtes du Nigéria (champ pétrolifère « Bonga ») ou celle de la plateforme TOTAL du champ d'Amenam en mai 2009, démontrent que l'éloignement n'est plus un réel gage de sécurité.

Alors que les attaques de navires se multiplient (2008 et 2009 sont marqués par une augmentation sans précédent des détournements en mer), les exemples d'attaques d'infrastructures énergétiques offshore, s'ils restent pour le moment moins fréquents et moins médiatisés, n'en sont pas moins extrêmement inquiétants en ce sens qu'ils dévoilent une grande vulnérabilité. Ainsi, entre mi-2006 et mi-2008, Jenkins relève rien que sur le Nigéria une plus d'une vingtaine d'acte de piraterie. Depuis, on peut citer notamment :

- 19/06/2008 : Attaque du champ pétrolifère « Bonga » par des hommes armés dans des vedettes rapides. Plusieurs blessés. Fermeture du champ qui compte pour 10% de la production du Nigéria avec environ 225 000 barils par jour. Impact ressenti sur la montée des prix à l'échelle internationale.
- 31/10/2008 : Attaque du ravitailleur offshore Sagitta de l'armateur français Bourbon par des pirates lourdement armés au Cameroun - 10 personnes kidnappées.
- 07/01/2009 : Attaque d'une plate forme d'Exxon Mobil par des hommes armés dans un navire à fond-plat – Vol d'argent et d'objets de valeur.
- 23/01/2009 : Attaque d'un ravitailleur offshore par 10 hommes armés dans 2 vedettes rapides – Vol d'argent et d'objets de valeur.
- 26/05/2009 : attaque contre une installation de la compagnie française TOTAL sur le champ pétrolier d'Amenam au Nigéria.
- 22/09/2010 : 3 français employés de Bourbon sont pris en otage au large du Nigéria (champ pétrolier d'Addax).
- Novembre 2010 : Prise de 19 otages dans le delta du Niger parmi lesquels figurent deux Français, deux Américains, deux Indonésiens et un Canadien lors d'un raid sur un bateau et une plate-forme pétrolière de la société Afren ainsi que huit Nigérians enlevés lors d'une attaque sur une installation d'ExxonMobil
- 17/11/2010 : Des pirates embarqués sur une vedette rapide attaquent un bateau de la société française Perenco qui transportait des forces de sécurité camerounaises près d'une plate-forme pétrolière dans le golfe de Guinée (6 morts).
- 12/09/2011 : A moins de 12 kilomètres des côtes Togolaises, des pirates lourdement armés tentent en vain de s'emparer d'un navire commercial. Au même moment à 100 kilomètres de là, dans les eaux Béninoises, les 23 marins du *Mattheos*, moins chanceux, ont été pris en otage par un groupe de six individus.

Du Togo au Cameroun en passant par le Nigéria, l'on constate une hausse des attaques contre les pétroliers, les plates-formes offshores ou les navires commerciaux. Contrairement à la Somalie, ces groupes armés recherchent moins des otages que le pillage des marchandises.

2.3 Besoin

Les quelques exemples ci-dessus révèlent l'insuffisance des systèmes actuellement disponibles et mis en œuvre sur les infrastructures offshore pour les protéger contre des intrusions hostiles de type piraterie.

La sûreté des installations offshore est à ce jour assurée par les moyens « classiques » (vigie, identification radio, AIS, radar pour la surveillance de trafic et recours à des bateaux de surveillance généralement opérés par des sociétés sous-traitantes).

Les radars de surveillance du trafic sont destinés à détecter en priorité des mobiles coopératifs de taille importante ou moyenne. Ils ont des performances jugées insuffisantes face à de petites cibles marines de faible signature radar ou optronique, bien entendu non coopératives (absence de réflecteur radar ou d'AIS), évoluant dans une mer formée (fouillis de mer) et sont pénalisés par une zone aveugle à faible distance du porteur.

Les systèmes de type VTS permettent de sécuriser grandement la navigation commerciale en fournissant une image en temps réel des mouvements des navires dans une zone de surveillance donnée. S'ils sont largement opérationnels, d'une part leurs modes de détection usuels sont plus particulièrement adaptés à des bateaux « coopératifs » et d'autre part leur finalité de gestion du trafic maritime est très différente du concept de protection contre l'intrusion hostile par petite embarcation.

Le besoin opérationnel est donc de disposer en surcouche applicative de systèmes de type VTS d'un système d'aide à la réaction envers des menaces dédié à la protection des plates-formes offshore et s'intégrant au sein des systèmes existants tant ceux de management des infrastructures de production que ceux de gestion des différents moyens : **c'est ce que propose le système SARGOS.**

SARGOS utilise tous moyens de détection dont les informations VTS associées à d'autres informations spécifiques à la plateforme et à son environnement tant interne (topologie, personnel, opérations en cours, etc.) qu'externe (contexte politique, bateaux attendus, météo, événements locaux & internationaux, etc.).

En temps réel SARGOS apporte aux opérateurs une aide à la décision en informant des menaces et en lançant des procédures de réactions prédéfinies adaptées au contexte.

3. Le système SARGOS

Le système SARGOS vise à assurer la protection d'infrastructures sensibles en mer contre les menaces de surface en :

- détectant les menaces à l'aide d'un radar à onde continue modulée en fréquence (FMCW) et d'autres capteurs,(AIS, radar de navigation classique type Furuno) ;
- traitant la détection pour en évaluer sa dangerosité et définir la riposte appropriée ;
- mettant en œuvre un processus de riposte graduée et réversible ;

On notera que SARGOS fournit l'alerte à partir d'un cœur de système basé sur la technologie radar à onde continue innovante de RCF mais est apte à prendre en compte les données externes disponibles par ailleurs (pistes du radar de navigation, informations AIS, imagerie thermique, communications externes, etc.) en tant que de besoin pour mettre en place un processus planifié et gradué de réaction.

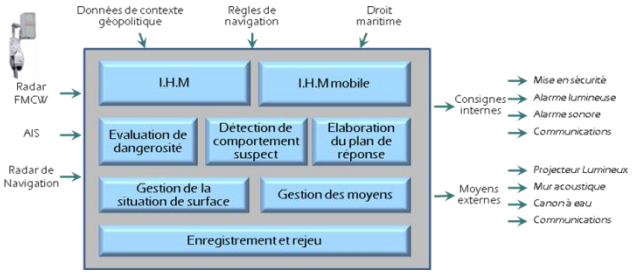

Figure 1 : Architecture globale SARGOS

Le système SARGOS est implanté sur un champ pétrolier et s'adapte à la configuration de celui-ci. Il est mis à la disposition du responsable sûreté du champ (généralement, l'Offshore, Installation Manager OIM). Il comprend les capteurs, le traitement et les mises en œuvre.

3.1 Détection

SARGOS s'adresse à la protection maritime rapprochée **envers de petites embarcations** caractérisée par des intrusions difficilement détectables par les moyens classiques et un faible temps de réaction.

La technologie FMCW a été retenue car elle apporte une réelle alternative aux technologies « RADAR pulsé » exploitées dans les radars de navigation, principalement dans sa capacité à détecter de petites cibles dans des conditions d'environnement particulières.

La surveillance des approches du champ pétrolier est donc réalisée en utilisant :

- les détections obtenues face aux petites embarcations, aux esquifs, aux engins flottants spécifiques (dinghy sur motorisé) et aux navires habituels, par le radar spécialisé du système SARGOS. Il s'agit d'un système radar dont l'émetteur émet une onde continue modulée en fréquence (FMCW), une technologie de formation de faisceau par le calcul étant par ailleurs mise en œuvre pour créer simultanément plusieurs faisceaux fins de réception sur l'ensemble de la zone de couverture du radar ce qui permet notamment de favoriser la détection de petites cibles par mer formée
- les informations recueillies par les capteurs associés au radar FMCW : radar de navigation classique type Furuno, tourelle IR, système AIS, moyens de communication.

Les mobiles détectés dans le périmètre du champ pétrolier protégé sont mis en piste pour élaborer les informations cinématiques.

3.2 Evaluation de la menace

SARGOS propose une approche novatrice pour la caractérisation d'une alerte en développant une logique d'analyse du comportement sur le franchissement graduel d'étapes dans un univers temps réel.

La connaissance de chaque objet « piste » est enrichie progressivement par un certain nombre d'attributs de classification (caractérisant la nature de l'objet) et d'identification (caractérisant la classe d'identité de ce même objet), attributs sur la base desquels le système évalue la dangerosité représentée par le mobile.

Un moteur de classification a été développé pour signer et classifier les différentes pistes. Il s'appuie sur l'implémentation d'un estimateur de Kalman pour la caractérisation cinématique des pistes et l'utilisation d'un classifieur bayésien pour déterminer la probabilité de la classe d'appartenance d'un navire.

Les informations fournies par le radar et les capteurs associés sont ainsi traitées pour déterminer la menace, selon les 3 étapes suivantes :

- l'évaluation de la dangerosité, basée sur une analyse croisée de la classe d'identité du mobile de surface détecté et de la position de l'intrusion détectée par rapport au périmètre de sûreté du champ pétrolier ;
- le calcul du rang de la menace, en utilisant les paramètres distance, vitesse et route du mobile détecté,
- l'analyse du comportement de la menace exploitant des règles expertes de caractérisation de comportement suspect.

Sur ces bases, le système décide de la nécessité de déclencher ou non, une alerte d'intrusion dangereuse.

3.3 Elaboration du plan de réaction

Lorsque le niveau de dangerosité atteint le seuil d'alerte, une alarme est générée et envoyée sur le poste opérateur et sur des terminaux mobiles (smartphones) pour alerter qu'une menace a été détectée. Le système oriente ses caméras vers la menace afin de pouvoir offrir des moyens d'identification visuelle.

L'alarme d'intrusion dangereuse déclenche en parallèle un processus d'analyse de la situation permettant l'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée, aux modes de fonctionnement de l'infrastructure et au contexte réglementaire et juridique du champ pétrolier.

Pour ce faire, une approche d'inférence bayésienne, alimentée par une base de données métier et de la connaissance experte du domaine maritime, a été mise en œuvre.

La planification des réactions possibles est déterminée en fonction du niveau de connaissance acquis en temps réel sur les différentes menaces détectées (critères de comportement, classes d'identité, et par comparaison de la situation connue en temps réel aux situations antérieurement rencontrées et mémorisées par le système) en tenant compte des éventuelles restrictions induites par la situation territoriale du champ pétrolier ou par le statut juridique de ce champ. Le réseau bayésien gère toutes les interactions possibles entre les caractéristiques de la menace, de la cible, de l'environnement pour déterminer dynamiquement et en temps réel le meilleur enchaînement de réponse pour faire face à la menace détectée. Ainsi le plan s'adapte à chaque instant à l'évolution du niveau de dangerosité de la situation.

Ce plan est présenté en support d'aide à la décision à l'opérateur qui en valide les différentes étapes, l'éventail des procédures proposées pouvant aller d'une simple activation d'alarme jusqu'à la mise en œuvre de moyens à capacité non létale.

3.4 Réactions et procédures de mise en œuvre associées.

Les moyens de réactions gérés par le système SARGOS s'articulent en :

- Un ensemble de contre-mesures d'ampleur croissante permettant de graduer la réponse pour s'adapter à la nature et l'évolution de la menace ;
- Un réseau de communication interne et externe permettant la diffusion de l'alerte, la coordination de la réponse et la demande d'assistance

Les réactions et procédures associées sont proposées pour activation par l'opérateur suivant une logique de priorisation permettant une réponse :

1. Adaptée
   La réponse est fonction de la nature de la menace ; elle s'accorde avec le type de mobile, le type de bien à protéger et les différents moyens et procédures de défense disponibles. SARGOS prend en compte les contres mesures et les différents moyens non létaux du marché mais gère également tout le système de procédures de mise en sûreté du site ou encore la coordination des navires de sûreté et d'intervention.
2. Graduée
   En fonction de la dangerosité de la menace, que ce soit en termes de moyens d'attaque ou de caractéristiques nautiques, la réponse peut aller en s'amplifiant afin d'accroître la riposte ou de mettre en sûreté au plus vite les personnes et les biens exposés.
3. Evolutive
   Le système suit en temps réel l'évolution de la menace dans le temps et l'espace afin de proposer à l'opérateur la réponse la plus pertinente en fonction de la situation actuelle.

Ainsi, SARGOS propose dynamiquement des plans de réponses priorisées comprenant par exemple :

- Communication aux navires de sûreté ;
- Application des Best Management Practices (BMP4) pour les navires menacés ;
- Blocage des accès ;
- Mise en protection des biens et des personnes ;
- Mise en œuvre d'effecteurs non létaux d'injonction et d'intimidation (diffusion sonore d'injonction, dispositif lumineux) ;
- des moyens de neutralisation (système acoustique paralysant ou autre) ;
- des moyens de communication externes (VHF, liaisons satellite) pour transmission d'alertes sur les menaces avérées et sur leur nature.

3.5 Poste opérateur

SARGOS s'adresse prioritairement à la surveillance et la protection d'infrastructures civiles : il ne doit pas requérir de personnel dédié dont le métier serait d'assurer la défense des biens et des personnes et il doit rester compatible d'une exploitation par un opérateur généraliste ayant comme principal objectif la production journalière et qui serait potentiellement stressé par la situation de crise à laquelle il serait confronté.

Le « Poste Opérateur » est le moyen de dialogue entre le système SARGOS et le gestionnaire du champ offshore. A ce titre, il assure la visualisation panoramique des pistes système de la situation de surface rapprochée et met à la disposition de l'opérateur des moyens d'aide à la décision ainsi que des moyens d'action (validation des réactions graduées proposées par le système et autorisation de déclenchement de la panoplie de ripostes préconisées).

Par une interface homme-machine tactile, le responsable de la sûreté est capable en quelques instants de mesurer la dangerosité de la situation et de lancer les procédures adéquates.

Concrètement, pour assurer une prise de connaissance complète et rapide de la situation, les informations SARGOS sont présentées sur 2 écrans adjacents :

- Le premier écran affiche la situation de surface donc permet visualiser les différents types de pistes avec un code forme / couleur précisant la classe du mobile et son caractère menaçant sur fond cartographique ECDIS recouvrant le champ pétrolier surveillé,
- Le second écran enrichit les informations maritimes en affichant la liste des navires détectés classés dans un tableau suivant leur dangerosité.

Le « Plan des Réactions » élaboré par les techniques de modélisation de la réaction est affiché en temps réel dans une fenêtre séparée que l'opérateur peut actionner à tout moment par simple pression tactile.

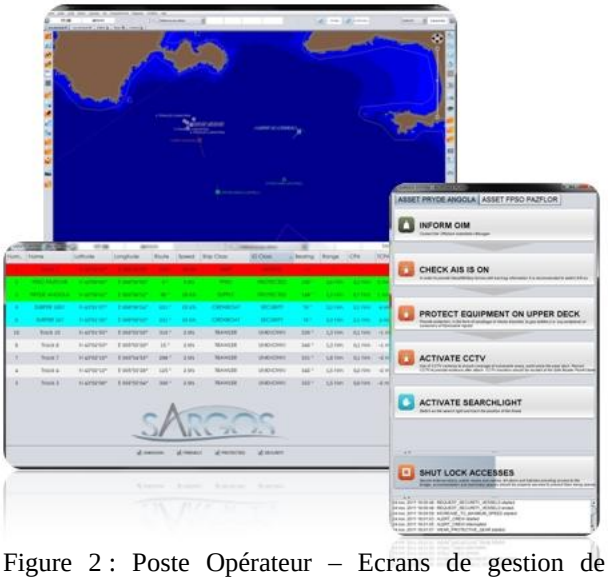

Figure 2 : Poste Opérateur – Ecrans de gestion de la situation de surface

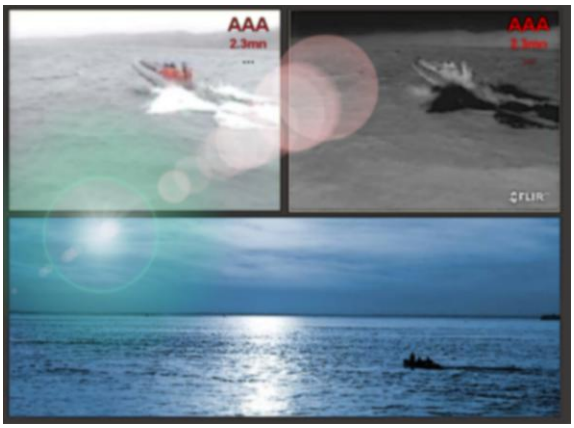

Figure 3: Poste Opérateur – Vue rapprochée

4. Démonstrateur

Toute la chaîne de traitement SARGOS a été implémentée dans une maquette logicielle opérationnelle couvrant toute la chaîne de protection, de la détection d'une menace potentielle jusqu'à la mise en œuvre des procédures de réaction adaptées. Cette maquette a permis de valider le fonctionnement des traitements effectués.

Une maquette matérielle est en cours de déploiement sur le site DGA de Saint-Mandrier (83).

Figure 4 : Site d'expérimentation

Le démonstrateur du système radar FMCW dédié à la détection et classification des petites embarcations actuellement déployé est constitué du senseur et d'une caméra montés sur un mat télescopique. Les pistes obtenues en sortie de traitement sont transférées via Ethernet vers le serveur SARGOS.

On dispose également d'un récepteur AIS et d'un radar de navigation LITTON qui sera relié au serveur SARGOS via un coffret de numérisation spécifique.

Ces 3 senseurs sont mis en œuvre et les pistes correspondantes fusionnées pour établir la tenue de situation de surface

Les moyens de poursuite optronique, d'alerte et de dissuasion utilisés par SARGOS ainsi que la gestion des communications internes et externes sont intégrés dans le sous-système SPPS (Système de Poursuite et de Protection SARGOS). Le SPPS comprend une tourelle infrarouge permettra la détection, localisation, identification de cibles désignées

Figure 5 : Système FMCW en place

Le démonstrateur SARGOS va être opéré durant plusieurs mois ce qui permettra d'optimiser les différents traitements implémentés et de réaliser les expérimentations probatoires en vraie grandeur à des fins d'évaluation et de validation des concepts développés au cours du projet.

5. Conclusion

La problématique de la protection des infrastructures civiles critiques vis-à-vis d'intrusions malveillantes nécessite de développer des stratégies assurant de manière coordonnée la chaîne globale de protection consistant en la surveillance automatique, la détection robuste, l'ajustement pertinent du plan d'action en réponse et la mise en œuvre graduée de la réaction.

Le projet SARGOS propose un **système global d'alerte et de réponse graduée**, pour répondre au fort besoin émergeant de sécurisation des infrastructures offshore civiles, vulnérables aux actes de malveillance, de piraterie ou de terrorisme menées à partir de la mer. Ce système traite :

- La détection automatique robuste et la classification de cibles marines de faibles dimensions par mer formée ;
- La détection de comportements suspects dans un périmètre de sécurité autour de la plate-forme ;
- La formalisation et la modélisation de réactions internes et externes graduées adaptées à la dangerosité de l'intrusion détectée et prenant en compte les règles de sécurité en vigueur sur la plate-forme, l'environnement géopolitique et les aspects juridiques ;
- Le déclenchement d'actions de réaction progressives et réversibles, selon un processus intelligent d'analyse de la situation, et pouvant aller d'une simple alerte interne jusqu'à la mise en œuvre de moyens à capacité non létale.

Cette approche système et transverse fait appel à des compétences pluridisciplinaires qui sont capitalisées dans un consortium de partenaires complémentaires regroupant une PME (SOFRESUD), des industriels (DCNS, RCF, CS-SI), et des laboratoires de recherche (ARMINES/CRC, TéSA, CDMT) avec le soutien d'organismes publics (DGA Techniques Navales).

Les travaux sont effectués sous l'égide d'un comité de pilotage comprenant des représentants des deux principales sociétés pétrolières et gazières françaises TOTAL et GDF SUEZ, de la DGA et de la Marine Nationale, réunis dans un comité des utilisateurs qui est sollicité pour communiquer l'expression de besoin, consolider les objectifs techniques, valider les scénarios de travail et évaluer la pertinence des résultats obtenus.

Remerciements

Le projet SARGOS a été sélectionné par l'Agence Nationale de la Recherche (ANR) pour être subventionné dans le cadre du programme 2010 sur les concepts systèmes et outils pour la sécurité globale (CSOSG).

Le projet SARGOS d'une durée de 30 mois a démarré en janvier 2010.

Références

[1] C. Imbert, J-P. Wasselin, E. Itcia, M-A. Giraud, M. Morel, H-P. Audubey *Système radar FMCW pour la detection et la classification de petites embarcations par mer formée*, 6ème Workshop Interdisciplinaire sur la Sécurité Globale (WISG12), Troyes, janvier 2012

[2] A. Bouejla, X. Chaze, A. Napoli, F. Guarnieri, T. Eude, B. Alhadef *Contribution des réseaux bayésiens à la gestion du risque de piraterie contre les champs pétroliers*, 6ème Workshop Interdisciplinaire sur la Sécurité Globale (WISG12), Troyes, janvier 2012

[3] M-A. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Bottala-Gambetta, D. Chaumartin, M. Philips, M. Morel, E. Itcia, D. Bonacci, P. Michel *SARGOS, Système d'Alerte et de Réponse Graduée OffShore* 5ème Workshop Interdisciplinaire sur la Sécurité Globale (WISG11), Troyes, janvier 2011

[4] 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* 4ème Workshop Interdisciplinaire sur la Sécurité Globale (WISG10), Troyes, janvier 2010

[5] 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

[6] 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

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

[8] 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

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

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

[11] 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.

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

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