CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Archive Ouverte a LUniversite Lyon 2

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 2011 - Workshop Interdisciplinaire sur la Sécurité Globale, Jan 2011, Troyes, France. 8 p., 2011. <hal-00660225>

HAL Id: hal-00660225

https://hal-mines-paristech.archives-ouvertes.fr/hal-00660225

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 – Le projet SARGOS propose de répondre au fort besoin émergeant de sécurisation des infrastructures offshore civiles vulnérables aux actions de malveillance, de piraterie ou de terrorisme menées à partir de la mer. L'objectif du projet est de concevoir et développer un système global d'alerte et de réponse graduée, prenant en charge l'ensemble du processus de protection de l'infrastructure depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de procédures de réaction.

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. Un enjeu fort est mis sur la prise en compte des modes de fonctionnement de l'infrastructure et des contraintes règlementaires et juridiques. L'aspect novateur réside en premier lieu dans le caractère global de l'approche retenue au sein des systèmes existants, tant ceux de management des infrastructures de production que de ceux de type VTS (Vessel Traffic Services), et ensuite dans son articulation dans les trois niveaux suivants :

a) Le niveau d'une détection sûre d'un objet marin de faible dimension dans un périmètre de protection rapproché par mer agitée en utilisant des formes d'ondes radar continues innovantes couplées à de nouveaux algorithmes de traitement de signal ;
b) Le niveau d'élaboration d'un plan de réaction vis-à-vis de l'intrusion décelée, prenant en compte l'enrichissement progressif de la connaissance et de la nature de l'objet détecté par des attributs de caractérisation de celui-ci. Le processus d'acquisition de la connaissance employé permet le déclenchement au moment approprié de réponses graduées prenant en compte le contexte de la crise (règles de sécurité en vigueur sur la plate-forme, environnement géopolitique, aspects juridiques) ;
c) Le niveau de gestion de la panoplie des moyens de réaction, soit internes à la plate-forme offshore (application de procédures de ***sureté*** prédéfinies, mise en sécurité), soit externes pour riposter à la menace (injonction, intimidation, voire en dernière extrémité activation de moyens non létaux) et diffuser l'alerte vers les autorités locales.

Cet article présente plus spécifiquement les fonctionnalités et l'architecture du système SARGOS

Abstract – The SARGOS project aims to satisfy the strong emerging need to improve safety for the civilian offshore infrastructures, sensitive to the actions conducted by spite, piracy or terrorism on sea.

SARGOS brings a new and innovative answer in this field of maritime security. A special care is taken to comply with the infrastructures operational constraints and the contractual and legislative rules. The innovative part of the project is mainly the global approach used, based on three levels:

a) The level of a safe detection of a small size marine object, in a small range protection area, with rough sea, using innovative CW radar waveforms improved by new efficient signal processing algorithms
b) The level of construction of a response plan facing a detected intrusion, taking into account the progressive improvement of the knowledge and the kind of detected object defined by its characterisation attributes. The acquisition process allows appropriate responses taking into account the crisis situation. (Platform safety rules, geopolitical environment and legal aspects).
d) The managing level of the variety of non-lethal response means, either internal to the offshore platform (predefined security procedures, safety mode), or external to reply to the menace (injunction, intimidation or, as a last resort, activation of authorised means) and broadcast the alert to the local authorities.

This article presents more specifically the main functionalities and the design of SARGOS system.

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.

[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.

2.2 Contexte

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

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 (plates-formes offshore) 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 ;
- traitant la détection pour en évaluer sa dangerosité et définir la riposte appropriée ;
- mettant en œuvre un processus de riposte graduée et réversible ;

conformément au schéma bloc de principe de la Figure 1.

Figure 1 : Schéma fonctionnel

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.

3.1 Conception globale

Le système SARGOS est implanté sur une plate-forme offshore et adapté à la configuration de celle-ci. Il est mis à la disposition du responsable sûreté de la plate-forme. Il comprend les capteurs, le traitement et les mises en œuvre.

3.1.1 Les capteurs

Le capteur principal est un radar à onde continue modulée en fréquence (FMCW) concu spécifiquement pour détecter des petites cibles marines à des distances de l'ordre de huit kilomètres. L'analyse fine de l'écho radar permet de le classifier. Un degré de dangerosité en est déduit à partir de la collecte d'informations complémentaires.

On notera que le système est apte à prendre en compte des données externes fournies par des communications intérieures et extérieures, des radars de navigation, des systèmes de réception AIS et des capteurs de veille infrarouge.

3.1.2 Le traitement

Les informations fournies par le radar et les capteurs associés sont traitées pour définir le degré de dangerosité de la cible, déclencher une éventuelle alerte avec une priorité appropriée et définir les moyens de protection à mettre en œuvre, à partir d'une « planification des réactions ».

Le poste opérateur SARGOS permet de visualiser les pistes des menaces sur un fond cartographique du lieu de la plate-forme, et de réaliser l'administration générale du système.

3.1.3 La mise en œuvre

Le module de gestion des moyens de réaction commande et contrôle les alertes internes et externes, les moyens de sécurité et de sûreté passifs et les moyens de réaction non létaux d'intimidation comme des projecteurs lumineux, des canons sonores, etc.

3.1.4 Logique de fonctionnement

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.

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 logique de détection et de traitement d'une intrusion est présentée sur la Figure 2.

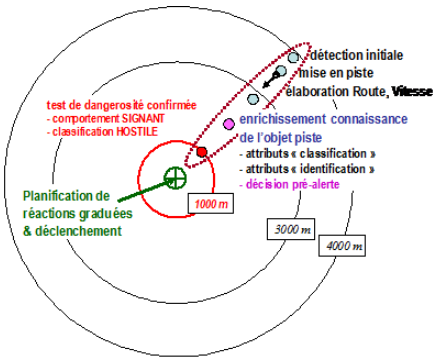


Figure 2**:** Logique de détection et traitement d'une intrusion

Les mobiles détectés dans un périmètre prédéfini autour de la plate-forme sont mis en piste pour élaborer les informations cinématiques. 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 on évalue la dangerosité représentée par le mobile.

3.2 Architecture fonctionnelle

Le système SARGOS est décomposé en plusieurs grandes blocs fonctionnels (cf. Figure 3).

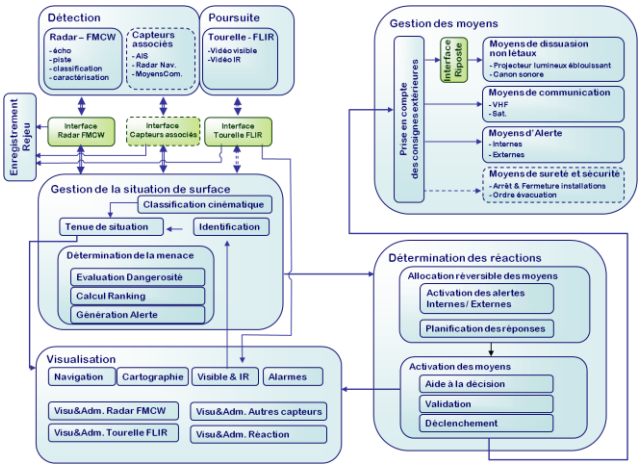


Figure 3: Architecture fonctionnelle du système

3.2.1 Détection

La surveillance des approches de la plate-forme offshore est 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 FMCW spécialisé du système SARGOS ;
- les informations recueillies par les capteurs associés au radar FMCW : radar de navigation classique, tourelle IR, système AIS, moyens de communication.

Le radar FMCW assure notamment la localisation de l'écho détecté, la mise en piste de la détection et le calcul de la cinématique de la piste, une classification des objets détectés, la transmission des différents attributs des objets mis en pistes aux abonnés privilégiés du radar (fonction technique du radar, poste opérateur) et l'échange de données avec la fonction « Gestion de la situation de surface ».

La gestion de la situation de surface assure l'acquisition et l'association des informations nécessaires à l'établissement de la tenue de surface rapprochée autour de la plate-forme, le traitement des informations permettant de déterminer la « classe d'identité » de l'écho détecté et la détermination de 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 défini autour de la plate-forme off-shore ;
- le calcul du rang de la menace, en utilisant les paramètres distance, vitesse et route du mobile détecté,
- l'analyse des paramètres de caractérisation de la menace, afin d'évaluer la nécessité de déclencher ou non, une alerte d'intrusion dangereuse.

3.2.2 Détermination des réactions

L'alerte d'intrusion dangereuse générée par la fonction « Gestion de la situation de surface » est transmise pour traitement, à la fonction « Détermination des réactions » qui réalise :

- des calculs de « planification de réactions » possibles en fonction du niveau de connaissance acquis sur les différentes menaces détectées (critères de comportement, classes d'identité, et 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 de la plate-forme offshore ou par le statut juridique de cette plate-forme ;
- une proposition d'activation des moyens de riposte, proposition soumise à la validation du servant du « Poste Opérateur ». Le rôle du servant est de se prononcer sur la pertinence ou la non-pertinence de l'envoi d'une consigne d'exécution de riposte vers le module « gestion des moyens » ;
- l'activation d'un processus de diffusion de l'alerte en interne à la plate-forme offshore ;
- l'activation d'un processus de diffusion de l'alerte vers l'extérieur par enclenchement d'une logique de génération de messages types pour informer les autorités à terre sur la nature de l'intrusion et le degré de nuisance décelé.

3.2.3 Gestion des moyens

A partir des consignes de ripostes reçues, il s'agit d'élaborer les séquences de mise en œuvre :

- Blocage des accès ;
- Mise en protection des biens et des personnes ;
- des 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.

3.2.4 Visualisation et Actions

Le « Poste Opérateur » est le moyen de dialogue entre le système SARGOS et le gestionnaire de la plate-forme offshore. A ce titre, il assure la visualisation panoramique des pistes système de la situation de surface rapprochée de la plate-forme offshore 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).

3.2.5 Enregistrement / Rejeu

Les fonctions opérationnelles du système SARGOS sont complétées par des capacités d'enregistrement et de rejeu système.

Le rejeu permet notamment en phase de mise au point l'analyse de la logique de fonctionnement via le déroulement de scénarios opérationnels de test du système.

L'enregistrement des détections et réactions a plusieurs finalités :

- permettre d'identifier les menaces réelles et les faux problèmes par analyse après coup,
- apport de la Preuve,
- transmission à d'autres entités à fins de prévention,
- évaluation de l'efficacité et de la pertinence de l'action déclenchée (interne ou externe) en fonction de la menace réelle

Ces données a posteriori de type « retour d'expérience » sont appréciables pour des assurances ou des financiers qui veulent quantifier le risque en ayant accès à des statistiques objectives.

3.3 Mise en œuvre du système

SARGOS propose un processus automatisé d'analyse de situation, de levée d'alerte et d'élaboration d'un plan de réponses progressives et réversibles pour la mise en œuvre des moyens de réaction. La mise en œuvre du système se décompose en trois phases :

- Phase 1 : Veille automatique

Dans un premier temps, le système SARGOS est autonome, il entretient la situation de surface avec les pistes des capteurs et évalue la dangerosité de chaque embarcation naviguant aux alentours de la plateforme. Lorsque le niveau de dangerosité atteint un seuil, le système quitte la phase de « veille automatique » pour passer en phase « Alerte ».

- Phase 2 : Alerte

Le niveau de dangerosité d'une des pistes système a dépassé le seuil d'alerte : l'appréciation d'un opérateur devient nécessaire. Une alarme est générée afin d'avertir l'opérateur qu'une menace a été détectée. Le système oriente ses caméras vers la menace afin de pouvoir offrir à l'opérateur des moyens d'identification visuelle.

- Phase 3 : Traitement

L'opérateur a pris connaissance de la situation, a confirmé la menace et l'a identifiée. Le système entre en phase de traitement des réactions. Le système propose à l'opérateur une planification des réactions en se basant sur la nature de la menace et les temps de mise en œuvre de ces réactions.

4. Poste opérateur

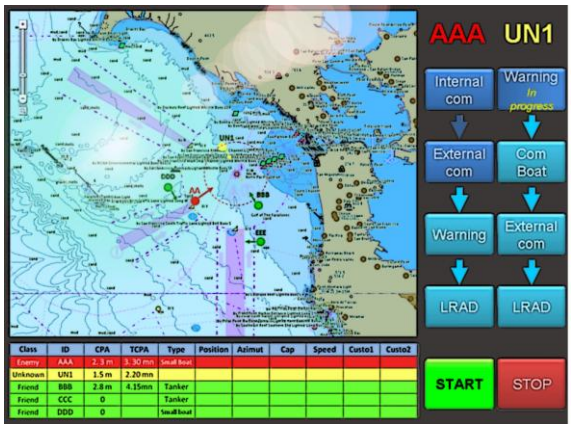
SARGOS s'adresse prioritairement à la surveillance et la protection d'infrastructures civiles : il ne doit pas requérir de personnel dédié dont le métier serait d'assurer la défense des biens et des personnes et il doit rester compatible d'une exploitation par un opérateur généraliste ayant comme principal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

Pour assurer une prise de connaissance complète et rapide de la situation, les informations SARGOS sont présentées à l'opérateur sur 2 écrans adjacents :

Le premier écran affiche (cf. Figure 4) :

- la situation de surface représentée sur une carte enrichie des informations maritimes, par la liste des navires détectés classés dans un tableau suivant leur dangerosité,
- une aide à la décision en présentant sous forme d'enchainement le « Plan des Réactions » élaboré par les techniques de modélisation de la réaction.

Figure 4 : Poste Opérateur – Ecran de gestion de la situation de surface



Le second écran est réservé à l'identification vidéo de la menace. Il est partagé en 3 zones :

- un bandeau qui affiche soit un plan large de la scène, soit un historique permettant de montrer à l'opérateur les images capturées par la caméra lorsqu'il n'était pas encore en poste devant la console ;
- une vue du plan rapproché de la menace qui permet à l'opérateur de valider la classe de l'embarcation et la classe d'identité de la menace ;
- une vue rapprochée en IR qui, en complément à la vision jour, peut permettre une meilleure identification.

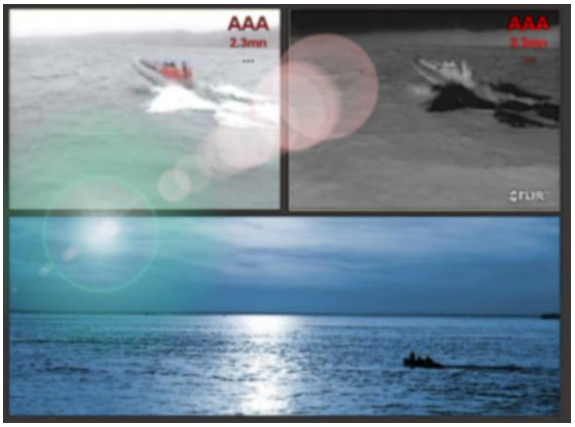


Figure 5: Poste Opérateur – Ecran d'identification

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] 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, Octobre 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.