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

Marie-Annick GIRAUD[1], Benjamin ALHADEF[1], Xavier CHAZE[2], Aldo NAPOLI[2], Anne-Cécile NAUDIN[3], Michel BOTTALA-GAMBETTA[3], Guillaume GRIMALDI[4], Denis CHAUMARTIN[4], Michel MOREL[5], Christophe IMBERT[6], Jean-Philippe WASSELIN[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, xavier.chaze@mines-paristech.fr, aldo.napoli@mines-paristech.fr, guillaume.grimaldi@c-s.fr ; denis.chaumartin@c-s.fr ; secretariat.cdmt@univ-cezanne.fr ; michel.morel@dcnsgroup.com ; cimbert@rockwellcollins.com; jwasseli@rockwellcollins.com, david.bonacci@tesa.prd.fr; patrice.michel@tesa.prd.fr

Résumé – Le projet SARGOS répond à l'émergence du besoin de sûreté des infrastructures offshore civiles vulnérables aux actes 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 pour apporter une réponse complète à la menace.
Un démonstrateur du système SARGOS illustrant toute la chaîne de protection a été déployé sur site pour des expérimentations en vraie grandeur selon des scénarios définis avec les opérationnels. Les essais ont permis de valider tous les points clefs : détection de petites embarcations – levée d'alertes pertinentes couplant analyse de comportement des embarcations et évaluation de dangerosité – Assistance intuitive à l'opérateur pour l'activation de procédures de réaction proposées en dynamique suivant une logique prédéfinie propre aux moyens disponibles.

Abstract – The project SARGOS aims to satisfy the strong emerging need to improve the security of civilian offshore infrastructures vulnerable to piracy and other hostile actions led from the sea. The project proposes to develop a new global system ensuring in a coordinate way the whole protection line: automated watch and surveillance, detection of intrusions, dangerousness assessment, and graduated response plan monitored in real time so as to stay continuously adapted to the level of threat associated with the detected intrusion. One of the key capabilities is the development of a comprehensive and pooled defence strategy, including putting goods and persons under protection, alert broadcasting processes, coordination of external assistance and carrying out of non-lethal deterrent means.
A demonstrator of the system SARGOS illustrating the whole chain of protection has been deployed on site for full-scale experimentations according to scenarios defined with operational people. The trials conducted have allowed to validate all the key points: detection of small boat – raising up of relevant alerts by associating vessel behavior analysis and dangerousness evaluation – intuitive support to the operator for activation of reaction procedures – dynamic elaboration of a graduated response plan according to a predefined logic suited to available resources.

1. Introduction

La production pétrolière mondiale est répartie sur plus de 10 000 champs offshore, impliquant chacun d'une part un ensemble d'infrastructures pour extraire, traiter et stocker provisoirement le pétrole et d'autre part des navires chargés d'effectuer le transport maritime d'hydrocarbures entre lieux de production et de consommation. La piraterie maritime moderne représente à l'heure actuelle le risque majeur pour la sécurisation de ces sites de production énergétique et du transport maritime pétrolier.

La protection directe de chaque champ à travers la mise en place de mesures de sécurité appropriées in situ relève de la responsabilité industrielle.

Le système SARGOS a été développé pour répondre à ce nouveau besoin de protection d'infrastructures civiles vulnérables aux actes malveillants menés à partir de la mer.

Il prend 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. Contexte et état de l'art

La sécurité énergétique fait partie des challenges économiques et sécuritaires actuels. Plusieurs catastrophes ont démontré la vulnérabilité que peuvent avoir les infrastructures qui produisent et fournissent l'énergie et l'impérieuse nécessité d'une profonde rigueur dans le respect des procédures et la conception des systèmes.

La production pétrolière offshore fournit actuellement environ un tiers de l'approvisionnement et cette proportion est nette augmentation du fait de l'exploitation de « réservoirs » situés à des profondeurs de plus en plus élevées : à moyen terme plus de la moitié du pétrole et du gaz seront extraits de l'offshore et particulièrement de l'offshore profond.

Compte tenus des enjeux économiques liés à la cherté des hydrocarbures, les champs de production offshore 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.

Les cas d'attaques d'infrastructures énergétiques offshore, s'ils restent pour le moment moins fréquents et moins médiatisés que ceux d'attaque de navires, n'en sont pas moins extrêmement inquiétants en ce sens qu'ils dévoilent une grande vulnérabilité [1-4].

Pour les neuf premiers mois de l'année 2012, si les statistiques du BMI font état d'une amélioration de la situation de la piraterie dans la corne de l'Afrique, celle du Golfe de Guinée reste largement inquiétante, avec 34 attaques recensées dont 21 devant le Nigéria impliquant souvent de la violence, des enlèvements ou des vols de cargaison, notamment de produits raffinés.

Ces actes 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. Approche scientifique et technique

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

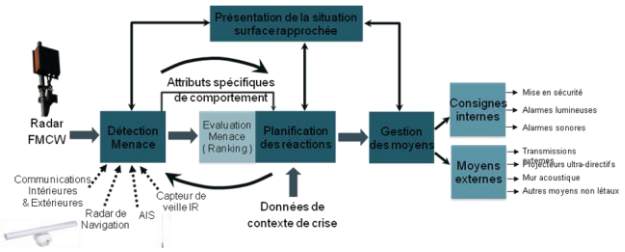

Figure 1 : Schéma fonctionnel

La démarche mise en œuvre, illustrée sur la Figure 1, s'articule autour d'une approche système et transverse s'appuyant sur plusieurs technologies clefs :

- La surveillance des approches du champ offshore est réalisée en utilisant notamment les détections obtenues face aux petites embarcations et aux navires habituels par un radar spécifique (technologie FMCW) mais aussi les informations recueillies par les capteurs associés disponibles par ailleurs (AIS, radar de navigation classique, etc.).
- Une analyse intelligente des différentes caractéristiques de l'objet détecté va permettre de le classifier et d'évaluer sa dangerosité. Lorsque le niveau de dangerosité atteint le seuil d'alerte, une alarme est générée et l'opérateur est alerté par un message sur un terminal mobile qu'une menace a été détectée ;

- L'alarme d'intrusion dangereuse déclenche un processus d'analyse de la situation permettant l'élaboration automatique à l'aide de réseaux bayésiens d'un plan de réactions graduées et réversibles, adapté à la nature de l'intrusion détectée, aux modes de fonctionnement de l'infrastructure et au contexte réglementaire et juridique du champ pétrolier ;
- Le 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

Sur la base d'un recueil de besoin auprès des opérationnels ayant permis de préciser les spécifications système, chacune des briques technologiques nécessaires a été développée. Ces briques ont été intégrées dans une maquette logicielle puis dans un démonstrateur déployé sur site pour des essais en vraie grandeur permettant d'évaluer les mérites des technologies développées.

3.1 Détection et tracking

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 (Frequency Modulated Continuous Wave – Onde Continue Modulée en Fréquence) a été retenue car elle apporte un réel complément aux technologies « pulsées » exploitées de manière standard dans les radars de navigation, principalement dans sa capacité à détecter de petites cibles dans des conditions d'environnement particulières. On notera que peuvent être également mises à profit les informations recueillies par les capteurs potentiellement associés en opérationnel au radar FMCW (radar de navigation classique, tourelle infrarouge, système AIS, moyens de communication, etc.).

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

3.1.1 Radar FMCW

Le système radar développé [6,7] associe technologies FMCW et Formation de Faisceau par le Calcul. La technologie radar FMCW permet d'atteindre des performances remarquables en terme de résolution distance et vitesse radiale. De plus, à distance donnée, elle requiert une puissance d'émission crête beaucoup plus faible que celle requise par la technologie des radars classiques « pulsés » pour obtenir un même rapport signal à bruit.

L'émetteur du système radar « illumine » la mer suivant un diagramme d'antenne large permettant d'assurer instantanément la couverture requise.

L'antenne de réception est une antenne réseau. La cartographie des cibles en réception est alors obtenue par le traitement des données reçues par l'antenne réseau. La formation de faisceau par le calcul permet de créer simultanément plusieurs faisceaux fins de réception sur l'ensemble de la zone de couverture du radar. Ce procédé permet d'obtenir à la fois :

- un temps d'observation long des cibles sur toute la zone de couverture du radar, ce qui favorise la détection de petites cibles ;
- un taux de rafraîchissement important ;
- une limitation de la désensibilisation due au masquage des vagues, en supprimant l'effet cumulé masquage/balayage séquentiel du champ de vision.

Enfin, aucun mouvement de l'antenne n'est requis, ce qui facilite son déploiement et augmente la fiabilité du système sur le long terme.

3.1.2 Traitement du fouillis de mer et tracking

Le signal radar reçu est loin d'être pur. Il est souvent entaché de bruit et d'échos parasites, ce qui rend son traitement plus délicat. Dans le cas du projet SARGOS, le principal bruit correspond au « fouillis de mer », l'étendue d'eau se comportant comme une surface dont la SER (Surface Equivalente Radar) dépend de l'état de la mer et en particulier de la force du vent, de l'angle de vue par rapport à la direction du vent et aussi de la longueur d'onde et de la polarisation. Lorsque la résolution distance devient inférieure à la dizaine de mètres, ce qui est le cas pour le radar FMCW expérimenté dans SARGOS, le fouillis de mer perd son aspect homogène. Par conséquent, sa distribution d'amplitude présente des pics importants, ce qui entraîne des fausses alarmes et rend la détection difficile (le fouillis de mer est alors généralement décrit par une distribution Weibull ou log-normale).

La nature temporelle impulsionnelle de ces pics liés au clutter fait du tracking un algorithme particulièrement bien adapté pour limiter considérablement le nombre de fausses alarmes liées à la présence du fouillis en ne confirmant que des tracks qu'il estime issus de vraies cibles (présentant un comportement continu dans le temps). Il s'agit alors, en s'appuyant sur les données acquises lors des campagnes de mesures préliminaires faites en début de projet, de mettre au point l'algorithme permettant l'initialisation du tracking, et le suivi de l'évolution du track pendant chaque cycle de mesure pour décider de le maintenir en tentative, le confirmer ou le fermer.

3.2 Levée d'alerte

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 est 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.

En parallèle, une méthode de classification avancée s'appuyant sur le traitement de l'image radar dans le plan Range-Doppler est étudiée.

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.

Lorsque le niveau de dangerosité atteint le seuil d'alerte, une alarme est générée et envoyée sur le poste opérateur 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.

3.3 Elaboration de la réaction

L'alarme d'intrusion dangereuse déclenche 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.

3.3.1 Planification par réseau bayésien

L'approche proposée est de développer un réseau bayésien exploitant les données de la base OMI sur les actes de piraterie pour déduire les réactions les plus utilisées, leurs efficiences et les distributions d'utilisation de ces réactions. Ces résultats sont intégrés dans un autre réseau bayésien élaboré à de la connaissance experte du domaine maritime

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 afin de 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 [8-10].

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.

3.3.2 Gestion des contre-mesures

Les moyens de réactions (contre-mesures) 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 :

- **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.
- **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.
- **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.

3.4 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.

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 et permet donc de 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.

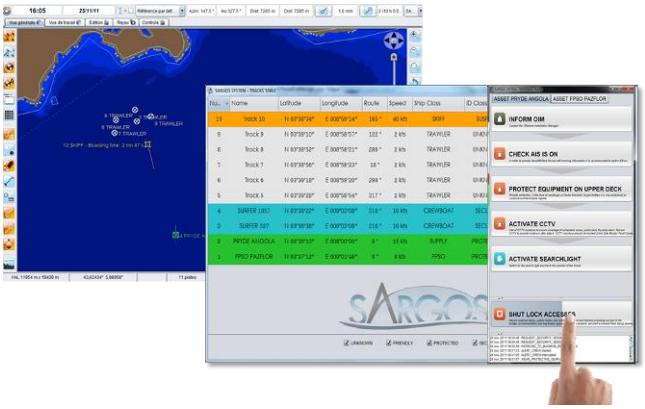

Figure 2 : Poste Opérateur – Ecrans de gestion de la situation de surface

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

4. Expérimentations

Dans un premier temps, les traitements SARGOS ont été implémentés 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 modules développés.

Une maquette matérielle a ensuite été spécifiée, intégrée et déployée sur le site DGA du SESDA (cf. **Erreur ! Source du renvoi introuvable.**) à Saint Mandrier (83) pour mener des campagnes d'essais en vraie grandeur, selon des scénarios d'attaque définis avec les opérationnels.

Le démonstrateur du système radar FMCW dédié à la détection et classification des petites embarcations 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 qui est 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 (cf.Figure 3)

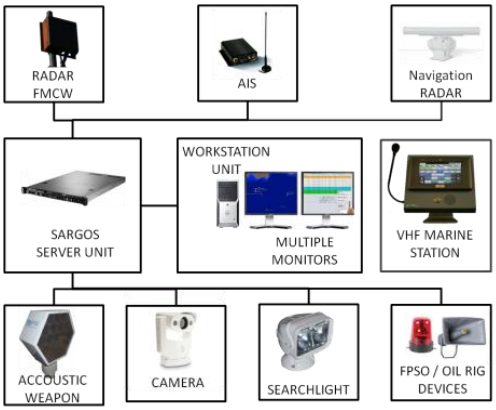

Figure 3 : Architecture matérielle du démonstrateur

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.

Le site d'expérimentation possède l'ensemble des spécificités permettant de réaliser des essais significatifs en vraie grandeur : ouvert sur la mer sur plus de 180°, il bénéficie de la présence régulière de petites cibles représentatives de la menace **Erreur ! Source du renvoi introuvable.**(cf. Figure 4).

Figure 4 : Site d'expérimentation

Le démonstrateur SARGOS a été opéré durant plusieurs mois ce qui a permis d'optimiser les différents traitements implémentés. Plusieurs campagnes d'expérimentation

dédiées ont aussi été réalisées avec le support des équipes DGA TN à des fins d'évaluation et de validation des concepts développés au cours du projet.

5. Résultats

5.1 Détection et tracking

Les nombreuses acquisitions de données faites sur des cibles d'opportunité et les campagnes d'expérimentation dédiées avec cibles collaboratives ont montré que le prototype radar FMCW développé présente des performances tout à fait satisfaisantes avec des distances typiques de détection de 5km pour un petit bateau de pêche (cf. Tableau 1)

Expérimentations SARGOS	**Portée(*)**
Zodiac (coopératif)	3.2 NM – 6 km (état de mer 4)
Cibles d'opportunités	**Distance de détection observée(**)**
Porte Conteneur	6 NM – 11 km (***)
Frégate	6 NM – 11 km (***)
Petite escorte de Frégate	5.4 NM – 10 km
Voilier	4.4 NM – 8.2 km
Yacht	3.8 NM – 7 km
Petit bateau de pêche	2.7 NM – 5 km
Bouée de pêcheur	1 NM – 1.8 km
Barque	0.6 NM – 1.1 km
Kayak	0.5 NM – 0.9 km

Tableau 1 : Performances observées du prototype FMCW

(*) Distance au-delà de laquelle la qualité de la détection ne permet plus le maintient de la piste

(**) Ne définit pas la portée maximum car les cibles d'opportunités ne sont pas coopératives

(***) Distance maximale instrumentée

5.2 Classification avancée

L'algorithme de segmentation GrowCut spécialement développé, couplé aux détections fournies par la chaîne de traitement du signal radar a permis l'extraction des "pixels" correspondant à une cible dans le plan Range-Doppler à partir des données réelles récoltées lors des différentes campagnes d'acquisition préliminaires réalisées en début de projet à Saint Mandrier.

L'ACP (Analyse en Composantes Principales) a permis d'optimiser les composantes du vecteurs forme (i.e. trouver les caractéristiques les plus signantes de ces cibles) et construire un premier dictionnaire (différent vecteurs forme d'objets déjà identifiés et rangés par classe) de façon semi-automatique. Ce dictionnaire peut ensuite être enrichi grâce à des mesures certaines (en mode apprentissage) et utilisé en situation opérationnelle pour la classification de tout objet (présent dans le dictionnaire) détecté par le radar en minimisant la distance entre le vecteur forme mesuré et les vecteurs forme présents dans le dictionnaire. Ceci donne à l'algorithme une capacité d'apprentissage limitée uniquement par la taille du dictionnaire.

Les résultats sur les données issues des campagnes de mesure ont mis en évidence une dimension optimale de 5 pour le vecteur forme et un taux de réussite d'affectation à la bonne classe de 81% pour la classe "zodiac" (dinghy) et 76% pour la classe "speed" (vedette rapide).

5.3 Plan de réaction

Le prototype bayésien a été testé par procédé itératif pour affiner les probabilités conditionnelles des nœuds en jouant différents scénarios d'attaque avant de l'intégrer dans le système SARGOS. Le plan émis est issu du traitement intelligent du dernier rapport d'alerte reçu. Seules les contre-mesures dont les modalités ont une probabilité supérieure à 70% sont retenues pour contribuer à la réaction. L'ordre de priorisation proposé dépend de plusieurs facteurs dont notamment le mode d'action, la facilité de mise en œuvre, le temps nécessaire à une bonne efficacité. Ainsi, l'utilisation d'un réseau bayésien pour la planification de la réaction face à une menace permet bien de gérer les interactions possibles entre les caractéristiques de la menace et de la cible attaquée, l'environnement, la gestion des personnes et installations. De plus il s'adapte en temps réel à l'évolution du niveau de dangerosité tout en tenant compte de l'incertitude liée aux données en entrée du système.

5.4 Contre-mesures

Les procédures de prise en charge d'une intrusion aussi bien sur le plan interne que sur le plan externe ont été définies. Elles se déclinent en 5 grandes catégories (sûreté, communication/assistance, dissuasion, anti-invasion, anti intrusion) et regroupent actuellement une trentaine de réactions unitaires. Le système est ouvert pour permettre l'ajout de nouvelles contre-mesures.

L'asservissement de la caméra jour/nuit sur la piste désignée comme menaçante apporte une réelle valeur ajoutée pour l'identification précise de la menace.

5.5 Concept SARGOS

Plusieurs campagnes d'essais en vraie grandeur mettant en œuvre le démonstrateur et deux embarcations de type semi rigide affrétées spécifiquement ont été organisées pour valider le concept SARGOS.

Plusieurs scénarios représentatifs définis avec les opérationnels ont été déroulés, l'objectif étant d'évaluer :

- La bonne gestion des intrusions non malveillantes ;
- La réactivité du système face à une attaque directe contre une infrastructure fixe en mer et ses capacités à bien coordonner la réaction avec en particulier l'intervention d'un navire de sécurité

– La réactivité du système face à une attaque d'un bateau travaillant au profit du champ (type Supply)

Ces essais ont permis de confirmer les capacités clefs proposées par SARGOS :

– Les détections fournies par le radar FMCW et les autres moyens disponibles (radar de navigation, AIS) permettent d'établir une situation de surface ;
– Le moteur de classification permet de signer et classifier les pistes ; les comportements suspects sont correctement détectés et génèrent des alertes opérateur à bon escient ;
– La gestion de la situation au travers du poste opérateur constitué de 2 écrans est efficace :
  ▪ La symbologie spécifique utilisée pour la situation de surface permet d'apprécier instantanément la situation ;
  ▪ L'écran tactile permet une activation simple et intuitive des contre-mesures du plan de réaction proposé dès qu'une piste est déclarée suspecte.
– Le plan de réactions proposé est dynamique et adaptatif fonction de la menace et des capacités/équipements des installations à protéger. Les messages clefs sont générés automatiquement ;

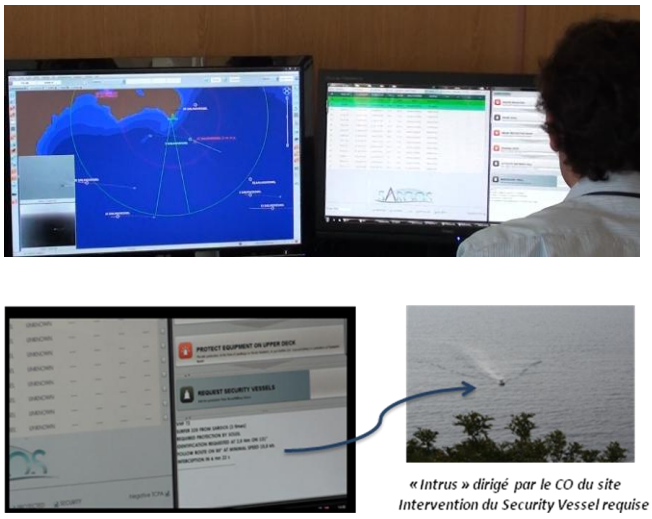

Figure 5 : Mise en œuvre de la maquette SARGOS lors des essais en vraie grandeur

6. Discussion

Au niveau système, les objectifs initiaux du projet ont été atteints : SARGOS propose un système efficace d'alerte et de réponse graduée prenant en charge toute la chaîne de protection d'un champ offshore et adapté à un environnement opérationnel civil.

Certains des résultats obtenus dans le cadre du projet SARGOS peuvent d'ores et déjà trouver des voies de valorisation :

– La technologie radar FMCW a démontré des caractéristiques tout à fait intéressantes pour la protection de zones côtières ou offshore sensibles envers la menace asymétrique ;
– Les briques décisionnelles développées en surcouche de la tenue de situation sont pour la plupart directement exploitables (moyennant une phase d'industrialisation) dans un système opérationnel ;
– De manière générale, l'approche mise en œuvre peut être avantageusement déclinée pour traiter des problématiques voisines : sécurité maritime (anti-collision), protection de navires marchands envers la menace asymétrique, management des mouvements des mobiles dans un champ éolien offshore, etc.

Quelques points durs demeurent avant d'envisager une exploitation opérationnelle :

– Concernant le tracking, le temps nécessaire à l'algorithme pour faire les calculs d'estimation de tous les tracks dépend fortement du nombre de détections à traiter. Ainsi, si pour une raison ou une autre (état de mer, densité de trafic, ...) le nombre de détections venait à trop augmenter, il y aurait des conséquences sur la capacité temps réel de l'algorithme (dans ce cas il peut être intéressant de limiter le nombre de détection en sortie de CFAR). Notons aussi que pour des raisons de temps de calcul, l'utilisation de l'association PDA (beaucoup moins coûteuse) est choisie par défaut par rapport au JPDA (permettant de traiter les croisements simultanés de pistes mais bien plus lourde).
– Concernant la classification avancée, il était initialement privilégié d'explorer les possibilités de modélisation conjointe par réseau de neurones mais cette approche est rapidement apparue peu adaptée au contexte et lui a été préférée une caractérisation du mobile détecté par un « vecteur de forme » permettant de déterminer l'empreinte de ce mobile.
  Même si les performances évaluées sur les campagnes de mesures réelles SARGOS sont élevées, la principale limitation est la nécessité de réaliser un apprentissage de chaque classe d'objet à classifier (nécessitant donc de nombreuses campagnes d'essais à réaliser par tous types d'état de mer). D'autre part, d'un point de vue purement opérationnel, la connaissance du type d'embarcation se dirigeant vers le site à protéger n'est pas forcément pertinente pour évaluer sa dangerosité (par exemple, on peut citer des cas de terroristes s'emparant d'une embarcation connue avant de l'utiliser pour aborder le site).
– De la même façon, la planification des réactions par inférence bayésienne résultant d'un processus d'apprentissage, il faudra pouvoir intégrer des retours d'expériences relatifs au traitement des attaques pour la faire évoluer, ce qui peut être pénalisant si l'on veut intégrer de nouvelles contre-mesures dans le

processus. Une parade possible tant qu'on ne dispose pas de suffisamment de données est de coupler réseau bayésien et moteur de règles.

7. 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.

En réponse, le projet SARGOS a adopté une approche système et transverse faisant 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 ont été 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.

Le projet SARGOS a permis de développer un système global d'alerte et de réponse graduée traitant :

- 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.

Le système a été déployé sur le site d'expérimentation DGA TN de Saint Mandrier (83), et testé en vraie grandeur en déroulant des scénarios opérationnels lors de campagnes d'essais.

Ces essais ont permis de valider la sûreté, la rapidité et la pertinence de la réaction SARGOS face à une intrusion menaçante.

Remerciements

Le projet SARGOS a été sélectionné par l'Agence Nationale de la Recherche (ANR) pour être subventionné dans le cadre de l'édition 2009 du programme CSOSG (Concepts Systèmes et Outils pour la Sécurité Globale)

Références

[1] MA. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Botalla-Gambetta, D. Chaumartin, M. Philips, M. Morel, C. Imbert, E. Itcia, D. Bonacci, P. Michel. *SARGOS : Système d'Alerte et de Réponse Graduée Off Shore*. Workshop WISG 2012, Université de Technologie de Troyes, 24-25/01/2012

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

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

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

[5] MA. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Botalla-Gambetta, D. Chaumartin, M. Philips, M. Morel, C. Imbert, E. Itcia, D. Bonacci, P. Michel. *SARGOS : Securing Offshore Infrastructures Through aGlobal Alert and Graded Response System*. Workshop MAST Europe 2011, Marseille, 27-29/06/2011

[6] C. Imbert, JP Wasselin, E. Itcia, MA. Giraud, M. Morel, HP Audubey. *Système radar FMCW pour la détection et la classification de petites embarcations par mer formée*. Workshop WISG 2012, Université de Technologie de Troyes, 24-25/01/2012

[7] JP Wasselin, S. Mazuel, E. Itcia, A. Huizing, A. Theil. *FMCW Radar System for Detection and Classification of Small Vessels in High Sea State Conditions.* Conférence EuMC 2012, Amsterdam, 28/10 - 02/11/2012

[8] A. Bouejla, X. Chaze A. Napoli and F. Guarnieri, T. Eude, B. Alhadef. *Contribution des réseaux bayésiens à la gestion du risque de piraterie contre les champs pétroliers,* Workshop WISG 2012, Université de Technologie de Troyes, 24-25/01/2012

[9] X. Chaze, A. Bouejla, A. Napoli and F. Guarnieri. *Integration of a Bayesian network for response planning in a maritime piracy risk management system.* 7th IEEE International Conference on System Of Systems Engineering SOSE 2012, Gênes, Italie, 16-19 juillet 2012.

[10] A. Bouejla, X. Chaze, F. Guarnieri and A. Napoli, *Coupling Quantitative and Qualitative Knowledge into a Bayesian Network to Manage Risks of Maritime Piracy against Offshore Oil Fields*, in International Journal of Information Technology and Management IJITM 2012 - Special issue : An Interdisciplinary Approach to Crisis Response and Management

[11] M. Botalla-Gambetta et AC. NAUDIN. *Sûreté maritime: le cadre juridique relatif aux installations offshore* » Revue de droit commercial, maritime, aérien et des transports. Presses universitaires d'Aix-Marseille

[12] 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

[13] 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

[14] 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

[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.