# Contribution des réseaux bayésiens à la gestion du risque de piraterie contre les champs pétroliers

Amal BOUEJLA[1], Xavier CHAZE[1], Aldo NAPOLI[1], Franck GUARNIERI[1], Thibaut EUDE[2], Benjamin ALHADEF[2]

[1] Mines ParisTech, CRC - Centre de recherche sur les Risques et les Crises, BP 207 1 rue Claude Daunesse,, 06904 Sophia Antipolis Cedex

amal.bouejla@mines-paristech.fr

xavier.chaze@mines-paristech.fr

aldo.napoli@mines-paristech.fr

franck.guarnieri@mines-paristech.fr

[2]SOFRESUD, 777 Avenue des Bruxelles, 83500 La Seyne sur Mer Cedex

thibaut.eude@groupegeos.com

benjamin.alhadef@sofresud.com

**Résumé** – Ces dernières années, les attaques de pirates contre des navires ou des champs pétroliers n'ont cessé de se multiplier et de s'aggraver. Pour exemple, l'attaque contre la plate-forme pétrolière Exxon Mobil en 2010 au large du Nigeria s'est soldée par l'enlèvement de dix neuf membres d'équipage et la réduction de 45.000 barils de sa production pétrolière quotidienne ce qui a engendré une montée des prix à l'échelle internationale.
Cet exemple est une parfaite illustration de la faiblesse actuelle des dispositifs d'anti-piraterie existants.
Pour faire face à ce problème, le projet SARGOS propose un système innovant prenant en compte toute la chaine de traitement depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction.
Pour réagir contre une attaque, il faut considérer de nombreux paramètres relatifs à la menace, la cible potentielle, les dispositifs de protection mis en place, les contraintes liées à l'environnement, etc.
Pour gérer ces paramètres, les potentialités des réseaux bayésiens sont exploitées afin de définir les contre-mesures possibles ainsi que leur mode de gestion.

**Abstract** – In recent years, pirates attacks against ships or oil platforms have continued to multiply and get worse. For example, the attack against Exxon Mobil oil rig in 2010 off the coast of Nigeria has caused the removal of nineteen of the crew and the reduction of 45.000 barrels of daily oil production which resulted the rise in prices internationally.
This example is a perfect illustration of current weaknesses of the existing anti-piracy systems.
To address this problem, the SARGOS project proposes an innovative system taking account the whole processing chain from detection of a potential threat to the implementation of the reaction.
To react against an attack, we should consider many parameters of the threat, the potential target, the existing protection tools, the environment constraints , etc.
To manage these parameters, the potentials of Bayesian Networks are used to identify feasible counterattacks and their management.

## 1. Introduction

La production mondiale pétrolière est répartie sur plus de 10.000 champs offshore, impliquant chacun d'une part un ensemble d'équipements 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.

Sur ces sites les moyens de surveillance présentent des faiblesses majeures au niveau de la détection d'une menace et surtout la procédure à appliquer pour se protéger sera-t-elle efficace et adaptée à chaque situation ? Il s'avère donc primordial de trouver un système qui gère la sécurité des champs pétroliers et propose une protection adaptée ainsi qu'une gestion efficace en cas de crise.

Le projet SARGOS répond à ce besoin de protection en proposant un système global de lutte contre les actes de piraterie envers les infrastructures pétrolières.

Au cours de cet article, la problématique liée aux actes de piraterie contre les champs pétroliers sera présentée. La méthode utilisée pour la planification des contre-mesures sera ensuite décrite précisément, avec notamment, la construction d'un réseau bayésien selon deux principes : l'utilisation de la base de données « piraterie et vol à mains armées » de l'Organisation Maritime Internationale (OMI) et le recueil et la formalisation de connaissances d'experts

Bouejla A., Chaze X., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« Contribution des réseaux bayésiens à la gestion du risque de piraterie contre les champs pétroliers »,
WISG 2012 (Workshop Interdisciplinaire sur la Sécurité Globale), Troyes, France, 24-25 janvier 2012

du domaine. Les résultats seront enfin testés sur des scénarios complets et réalistes d'attaques de pirates.

# 2. Définition du problème et objet de la recherche

Les infrastructures pétrolières offshore sont soumises à des risques de piraterie en constante augmentation. Ces actes ont de nombreuses répercussions tant au niveau local, de l'exploitation, que global. Les enjeux économiques mais aussi politiques liés à ces attaques seront ainsi précisés et viendront introduire un contexte en insécurité croissante où les acteurs de l'offshore pétrolier se trouvent démunis, les dispositifs actuels ne permettant pas de protéger efficacement ces infrastructures. Enfin, la présentation du projet SARGOS illustrera les nouveaux apports attendus pour faire face à cette problématique et ainsi légitimer leurs pertinences.

## 2.1 Enjeux

L'activité pétrolière offshore est en forte croissance. L'exploitation en mer des ressources pétrolières représente actuellement environ le tiers de la production mondiale de pétrole. Cette ressource énergétique, malgré sa raréfaction présente de nombreuses zones en voie d'exploration.

Il faut bien reconnaître que les attaques menées contre ces infrastructures engendrent des coûts supplémentaires élevés pour le versement des rançons, le paiement des primes d'assurances, l'installation d'équipements de sûreté, etc. Ces surcoûts influencent directement le prix du pétrole à l'échelle internationale.

De plus, les champs pétroliers constituent l'interface entre le monde maritime et le monde de l'industrie pétrolière. C'est en fait plus l'hétérogénéité des règles applicables que l'absence de droit qui font du statut juridique des plates-formes pétrolières un puzzle compliqué. Cette complexité peut générer en plus des conflits politiques entre les états : la société exploitant la plate-forme appartenant à un état différent de celui de son emplacement.

L'importance des installations pétrolières sur l'économie et l'industrie mondiale et les conséquences qui peuvent découler de la piraterie amènent à augmenter le degré de protection de ces biens.

## 2.2 Contexte

Malgré le fait que les attaques contre les champs pétroliers sont peu fréquentes et surtout peu médiatisées, elles sont extrêmement inquiétantes de par la gravité des conséquences sur l'équipage et l'infrastructure.

Citons à titre d'exemples les trois attaques suivantes :

- Le 22 septembre 2010, le remorqueur Bourbon Alexandre se trouvant sur le champ pétrolier d'Addax au large du Nigeria, a été attaqué par quatre embarcations rapides qui ont pris en otage trois marins français. Il s'agissait de la quatrième attaque contre Bourbon depuis 2009.
- L'attaque de la plate-forme Exxon Mobil, au large des côtes du Nigeria, a engendré l'enlèvement de dix neuf de ses employés et des dégâts importants sur l'installation pétrolière causés par les engins explosifs utilisés par les rebelles.
- Enfin le 17 novembre 2010, des pirates embarqués sur une vedette rapide ont attaqué 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. Cette attaque a fait six morts.

Les responsables des infrastructures, les employés et les agents de sûreté ne souhaitent plus voir leurs biens détournés faire l'objet de fortes rançons, ni voir des hommes d'équipages blessés, traumatisés voire tués, ou retenus dans des conditions extrêmes durant des jours, des semaines, voire des mois. Les assureurs, quant à eux, ne veulent pas assurer indéfiniment des risques d'une valeur trop importante. Enfin les états ne veulent plus voir le cours du pétrole impacté par de tels événements.

## 2.3 Besoins opérationnels

Ces exemples d'attaques sont de parfaites illustrations de la faiblesse des dispositifs anti-piraterie mis en place actuellement. La sécurité des installations pétrolières est à ce jour assurée par des dispositifs dits classiques (identification radio, radar, Système d'Identification Automatique, etc.). Ces derniers malgré leurs points forts pour l'aide à la détection, ne traitent pas des différents types de menaces (bateau de pêche, jet ski, tanker, etc.) et leurs efficacités dépendent de nombreux paramètres liés à l'environnement ainsi qu'aux contraintes techniques et opérationnelles.

La solution consiste donc à augmenter le degré de protection des infrastructures en développant un nouveau système appelé SARGOS capable de générer une alarme et d'enclencher des réactions internes et externes en cas d'intrusion confirmée.

## 2.4 Les apports du projet SARGOS

Le projet Système d'Alerte et de Réponse Graduée OffShore (SARGOS) répond à ce nouveau besoin de protection d'infrastructures civiles vulnérables aux actes de piraterie ou de terrorisme menés à partir de la mer. En effet, ce projet vise à concevoir et développer un système global prenant en compte toute la chaîne de traitement depuis la détection d'une menace potentielle jusqu'à la mise en œuvre de la réaction, en s'intégrant dans les modes de fonctionnement de l'infrastructure et en prenant en compte les contraintes réglementaires et juridiques.

Ce projet financé par l'ANR[1], labellisé par le pôle mer PACA et par le pôle Aerospace Valley, fait appel à des compétences pluri-disciplinaires (développement d'un système de protection global : détection et identification

[1] L'Agence Nationale de la Recherche finance le projet SARGOS qui regroupe de nombreuses entreprises (DCNS, SOFRESUD, etc.) et centres de recherche (ARMINES, TESA, etc.).

automatiques de menaces, estimation des risques potentiels et gestion d'une réponse adaptée).

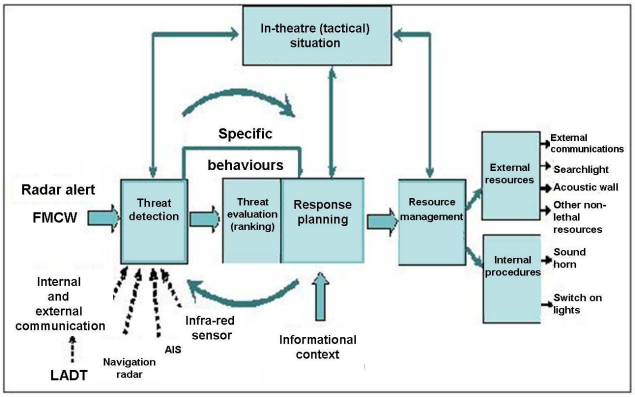


Fig. 1 : schéma fonctionnel du système SARGOS

Le schéma fonctionnel du système SARGOS (figure 1) montre le cycle de traitement de la menace. Dans la problématique qui nous intéresse, on observe un vrai déficit en matière de construction de diagnostic et dans la façon dont il faut gérer les paramètres et contraintes liées aux attaques. Pour lever cette insuffisance, nous proposons une démarche nouvelle d'élaboration automatique de plans de réaction adaptés à la nature de l'intrusion détectée.

# 3. Méthode

Il sera en particulier étudié l'apport dans le contexte de l'approche de l'inférence bayésienne alimentée par une base de données métiers existante et les connaissances d'experts du domaine maritime. Le réseau bayésien est utilisé dans le processus de planification de la réponse qui a pour but de mettre au point une réponse adaptée, graduée et évolutive face à une menace. Les informations contenues dans la base de données et le raisonnement des experts en entités pétrolières sont mis en commun pour combler les manques de connaissances a priori de l'objet considéré et de retour d'expérience dans le domaine applicatif.

Ces informations et connaissances sont ensuite modélisées par des réseaux bayésiens, outils fondés sur le théorème de Thomas Bayes (1), résultat de base en théorie des probabilités.

$$\left(\frac{P(B/A) * P(A)}{P(B)}\right) = P(A/B) \qquad (1)$$

Un réseau bayésien est un système représentant la connaissance et permettant de calculer des probabilités conditionnelles apportant des solutions à différentes sortes de problématiques. Pour construire le réseau bayésien le logiciel BayesiaLab[2] a été utilisé. Cet outil de modélisation des réseaux bayésiens présente de multiples fonctionnalités et une interface graphique intuitive.

Deux étapes, décrites ci-après, ont été nécessaires à l'élaboration du réseau bayésien SARGOS : la construction d'un premier réseau à partir d'une base de données métier existante et la construction du réseau final à partir de connaissances d'experts du domaine.

## 3.1 Construction d'un réseau bayésien à base de données existantes

Dans la première étape, a été exploité la base de données « Piraterie et vol à mains armées » de l'Organisation Maritime Internationale (OMI). C'est la seule base de données existante contenant un historique (depuis 1994) des attaques de piraterie en milieu maritime.

Au 15 juillet 2011, la base contenait 5 502 enregistrements et proposait pour chaque attaque recensée : le nom du bien attaqué, le nombre de personnes participant à l'attaque, le type d'armement utilisé, les mesures prises par l'équipage afin de se protéger, les conséquences sur l'équipages et sur les pirates, etc.

Le logiciel BayesiaLab permet alors de générer automatiquement un réseau bayésien et de proposer les relations de dépendances entre les principaux éléments de la base.

L'étude de la base de données a ainsi permis de définir les principales mesures prises par la plupart des entités attaquées :

- Enclencher des manœuvres évasives
- Activer SSAS (Ship Security Alarm System)
- Contacter le navire de sûreté
- Mettre l'équipage en sécurité
- Activer les projecteurs
- etc.

Ces modalités et probabilités conditionnelles ont été ensuite utilisées pour construire le réseau d'experts.

La figure 2 présente le réseau bayésien construit à partir de la base de données. Certaines informations comme la longitude, la latitude, le nom du bien attaqué, etc. ont été éliminées. Ce choix est dû au fait que ces champs ne sont pas mentionnés pour toutes les attaques.

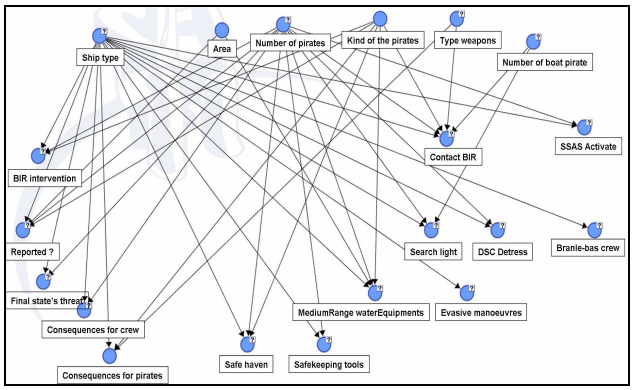


Fig. 2 : réseau bayésien basé sur les données OMI

[2] Le logiciel BayesiaLab est développé par la société française Bayesia (http://www.bayesia.com/)

La distribution des probabilités des nœuds (voir figure 3) montre dans un premier temps et avant d'appliquer des contraintes sur une attaque particulière que la plupart des navires attaqués sont des vraquiers ou des navires-citernes.

48,39% des attaques se déroulent dans les eaux internationales, ceci est dû à l'absence de contrôles de sécurité. Les pirates profitent aussi souvent de leurs nombres : 60,49% des attaques sont organisées par des équipes de pirates composées de plus de 5 personnes.

Grâce à ce réseau, une vision très claire sur la tactique des pirates, la nature de l'armement et surtout le nombre des personnes impliquées est désormais possible.

Dans l'exemple ci-dessous, des modalités spécifiques pour les nœuds caractérisant la menace ont été fixées afin d'identifier les contre-mesures utilisées par l'équipage de la cible attaquée. La figure 4 illustre ainsi les hypothèses choisies :

- Le bien attaqué : un tanker
- La position de l'accident : eaux internationales
- Type des attaquants : des voleurs
- Type d'armement : des personnes armées

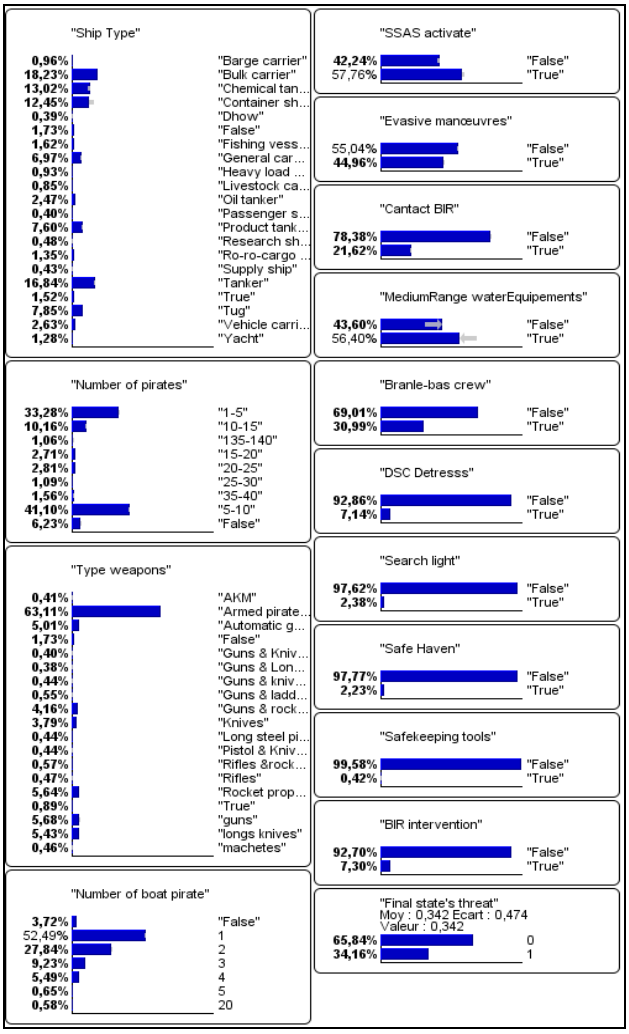


Fig. 3 : distribution des probabilités du réseau bayésien basé sur les données OMI

Le réseau bayésien indique dans ce cas, que les voleurs ont tiré des coups de feu sur la cible potentielle et que l'équipage, pour se protéger de ce danger, a essayé d'appliquer des manœuvres évasives et de projeter des jets d'eau sur les attaquants.

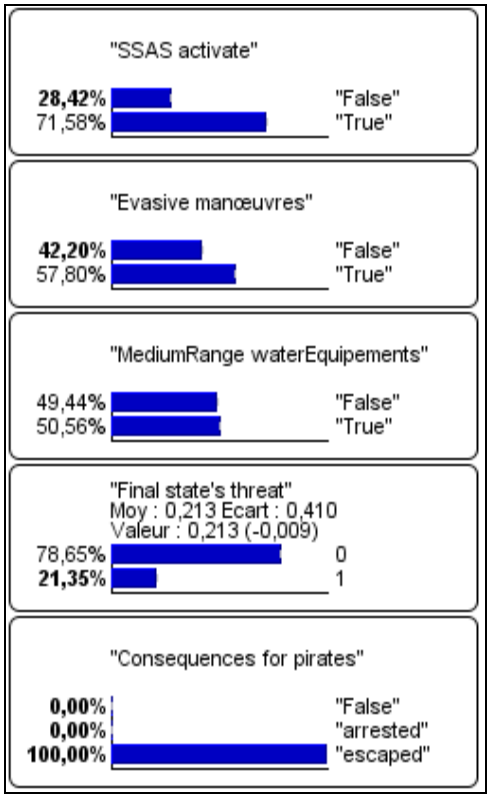


Fig. 4 : cas d'une attaque contre un tanker

Grâce au réseau construit à partir de la base de données « Piraterie et vol à mains armées », il a donc été possible dans un premier temps de déterminer les principaux outils et mesures utilisés par l'équipage des entités attaquées pour se protéger, d'évaluer l'efficacité de ces outils et de définir les probabilités de certaines occurrences d'attaques.

Dans un second temps, l'exploitation de cette base de données a permis de tester les différentes fonctionnalités de l'outil BayesiaLab et la faisabilité de la création d'un réseau bayésien à partir de données existantes.

## 3.2 Construction d'un réseau bayésien à base de connaissances expertes

En plus des informations extraites du réseau bayésien appliqué aux données OMI la seconde étape de la démarche méthodologique a consisté à exploiter les connaissances des experts du milieu maritime pour construire un réseau bayésien à destination du système SARGOS.

Le principe est le suivant : lors de la détection d'une piste radar qui circule dans une zone proche du champ pétrolier, un ensemble de variables est déterminé et calculé afin de l'identifier et d'évaluer sa potentielle dangerosité.

Parmi ces informations, citons par exemple la vitesse de la piste, la visibilité, la période de la journée, la longitude et la latitude de la piste et de la cible, etc.

A partir de ces données, la distance entre la cible et la piste attaquante ainsi que le temps théorique d'intervention du navire de sûreté sont calculés.

Ces informations sont enregistrées dans un rapport d'alerte avec un identifiant unique pour chaque piste détectée. Le système SARGOS ne génère ce rapport que lorsque la menace est identifiée comme suspecte ou hostile.

L'architecture fondamentale du réseau de la planification de la réaction SARGOS est constituée de cinq modules et quatre sous-modules.

Les modules en entrée du réseau et les contraintes opérationnelles sont présentés dans la figure ci-dessous (figure 5) :

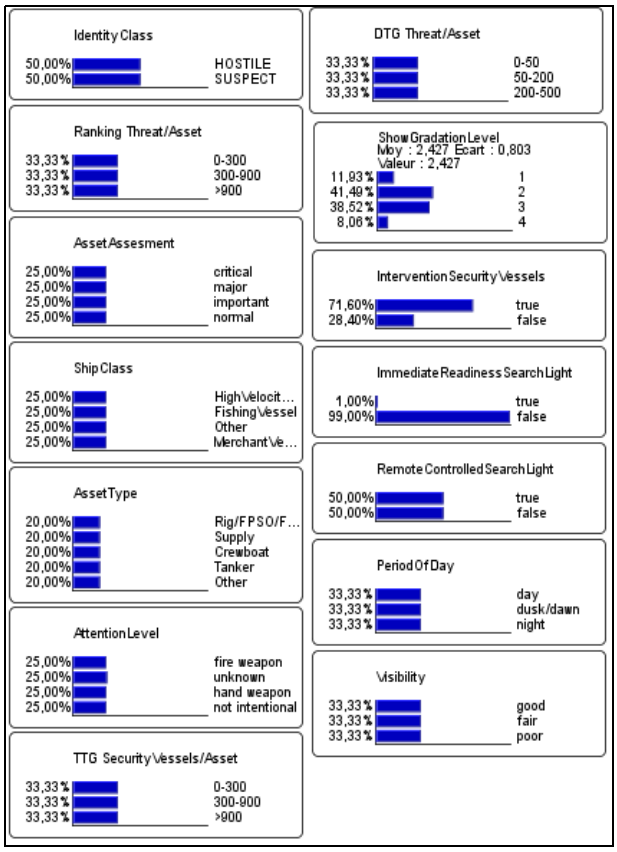


Fig. 5 : exemples des modules du réseau bayésien

La définition du périmètre de chacun de ces modules est directement liée à la signification des nœuds qui le constituent. Cette classification regroupe les paramètres fondamentaux, le niveau global de danger de la situation, les facteurs aggravants et les contraintes, les nœuds relatifs à la communication et la demande d'assistance et les contre-mesures, détaillés ci-après.

### 3.2.1 Les paramètres fondamentaux

Ce sont des données physiques statiques ou dynamiques qui caractérisent la menace et la cible. Elles sont directement issues, ou déduites de calculs intermédiaires, du rapport d'alerte. Elles constituent une forme de modélisation minimale nécessaire mais suffisamment pertinente pour permettre une pleine appréhension du couple menace / cible dans la problématique de réponse face à l'agression. Parmi ces paramètres, citons par exemple l'identité de la menace « Identity Class » suspecte ou hostile, la distance entre la menace et la cible « DTG Threat / Asset », la criticité de la cible « Asset Assesment », etc. Dans le nœud « Asset Assesment », sont définies quatre modalités : critique, majeur, important ou autre.

### 3.2.2 Le niveau global de danger de la situation

Il est élaboré à partir des paramètres fondamentaux pour définir la dangerosité globale de la situation. Le nœud « Show Gradation Level » est la formalisation de ce module dans le réseau bayésien. Le système de gradation fonctionne par niveaux de 1 pour le moindre à 4 pour le pire. Ce niveau et la planification des contre-mesures sont en permanence adaptés à chaque situation.

### 3.2.3 Les facteurs aggravants et les contraintes

Les facteurs aggravants et les contraintes sont des éléments internes et externes au système.

Les facteurs aggravants permettent de prendre en compte le potentiel de détérioration de la situation et donc d'anticiper sur l'éventuelle orientation à donner à la planification. Ils représentent l'environnement : la visibilité « Visibility » et la période de la journée « PeriodOfDay ».

Les contraintes sont représentées par des paramètres qui traduisent l'efficacité de la réponse tant sur le plan technique qu'opérationnel. Les contraintes techniques sont directement liées à l'utilisation des contre-mesures comme la disponibilité « ImmediateReadiness » ou le contrôle à distance « RemoteControlled ».

### 3.2.4 La communication et la demande d'assistance

La communication et la demande d'assistance sont deux types de réponse indispensables en cas de menace. La communication interne à la cible permet d'avertir tous les personnels concernés (exemple "informer le maître de l'équipage « Inform OIM ») alors que la communication externe permet à différentes échelles d'avertir les différents acteurs concernés par la sûreté de la vie en mer (demander l'intervention du navire de sûreté « Request Security Vessels », Mettre en œuvre le Système d'Alerte de Sûreté Silencieux « Raise SSAS », etc.). Cette communication permettra aux installations et navires du champ pétrolier d'anticiper sur leur plan de réponse et de demander si possible une intervention extérieure.

### 3.2.5 Les contre-mesures

Ce sont l'ensemble des moyens de défense mis en œuvre lorsque la cible est attaquée pour se protéger d'une menace identifiée. Elles sont la concrétisation du plan de réponse et constituent un ensemble de moyens et d'actions pour normaliser au plus vite la situation de la cible attaquée.

Ces contre-mesures sont partagées en quatre sous-modules (figure 6) :

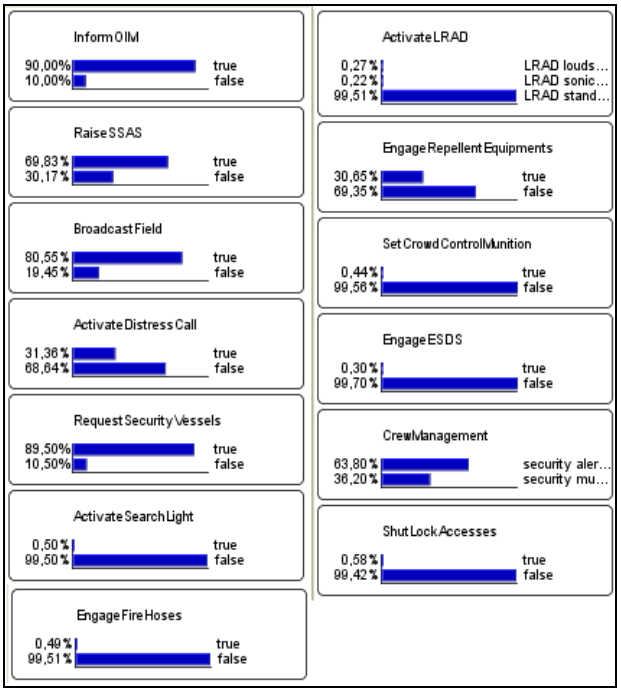


Fig. 6 : les contre-mesures du plan de réponse

Les quatre sous-modules ainsi définis traduisent la notion même de gradation de la réponse en proposant des contre-mesures d'ampleur croissante selon la nature de la menace détectée : la dissuasion et la répulsion de faible ampleur, la répulsion, l'anti-abordage et la neutralisation, la gestion des procédures, la mise en sécurité et en sûreté de l'installation, détaillés ci-après.

- **La dissuasion et la répulsion de faible ampleur**

Il s'agit de faire savoir aux attaquants que la cible connait ses intentions, qu'elle est capable de les suivre et qu'ils n'ont aucun intérêt à passer à l'action. La répulsion de faible ampleur est la capacité de la cible à pouvoir repousser l'attaque en utilisant des moyens à effets faibles tels que le projecteur lumineux de recherche, les lances à incendie ou les canons sonores « Activate LRAD » (Long-Rang Acoustic Device).

- **Répulsion, anti-abordage et neutralisation**

Ce sont les contre-mesures actives avec impact fort et dont la fonction principale est au moins l'atténuation si ce n'est la neutralisation des attaquants. Dans le nœud « Engage Reppellent Equipement », sont regroupés les matériels de plus en plus nombreux sur le marché de la piraterie maritime qui assurent la répulsion à distance d'un assaut tout en restant dans le cadre de la légitime défense non létale. De même que pour les équipements de répulsion, les équipements anti-invasions ont pour fonction principale d'empêcher les attaquants de monter à bord lorsqu'ils se trouvent à proximité de l'installation ou du navire.

Le rôle du « Set Crowd Control Munition » est de retarder la progression des attaquants pour les fatiguer voire les neutraliser et ainsi laisser un maximum de temps à l'équipage pour mieux gérer les autres actions de sûreté.

- **La gestion des procédures**

Cette planification est composée des contre-mesures suivantes :

Le nœud « Crew Mangement » propose pour chaque cas de sonner le branle-bas équipage de l'infrastructure puis de les réunir aux points de rassemblement définis en cas d'alerte de sûreté.

Le nœud « Asset Assault Management » permet dans chaque cas une gestion de la cible potentielle en termes de mise en sécurité et sûreté. Les modalités de ce nœud sont : activer le mode citadelle, effectuer des manœuvres évasives pour les cas des unités mobiles et navires, et déclarer le poste de sûreté qui est un ensemble de procédures individuelles que devra appliquer chaque membre de l'équipage le cas échéant.

- **La mise en sécurité et en sûreté de l'installation**

Comme pour la gestion des procédures, SARGOS propose, au sein de la planification, des actions qui concernent le contrôle de l'outil de production afin de le stopper en toute sécurité ou l'interdiction d'accéder aux locaux sensibles.

### 3.2.6 Les probabilités conditionnelles

Dans le réseau bayésien, chaque module ou sous-module est composé d'un ou plusieurs nœuds qui reçoivent et/ou émettent des influences vers d'autres nœuds. Chaque nœud est composé d'une matrice de probabilités conditionnelles calculées en tenant compte des différentes influences avec les autres nœuds et de la réalité afférente que lui même représente.

Les probabilités des nœuds fondamentaux sont ici normalisées puisque aucun élément caractérisant une attaque précise n'a été inséré.

# 4. Discussion des résultats

La distribution des probabilités des différentes modalités étant réalisée, il devient intéressant de tester le réseau bayésien ainsi élaboré en jouant différents scénarios d'attaque qui seront traduits au sein du réseau en fixant des observations de manière certaine. L'étude de ces scénarios permet ainsi de finaliser le réseau avant de l'intégrer au système SARGOS.

## 4.1 Étude de scénarios d'attaques

L'exemple ci-dessous (figure 7) présente les résultats liés à l'insertion des paramètres d'une attaque d'une unité flottante de production, de stockage et de déchargement (Floating Production, Storage and Offloading [unit], FPSO) par un navire inconnu.

Cet exemple montre que le niveau de dangerosité de la situation est 2 avec un pourcentage de 64,68%. Dans ce cas les contre-mesures à appliquer sont :

- informer le maître de l'équipage

- demander l'intervention du navire de sûreté
- émettre un message fort et clair à longue portée via le haut parleur
- activer le projecteur lumineux
- engager le poste de sûreté
- activer les équipements de répulsion

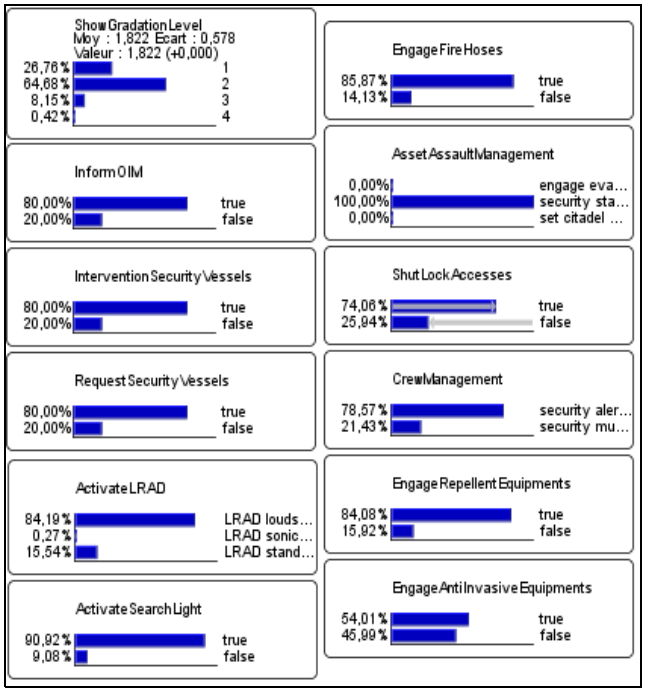


Fig. 7 : résultat de la planification des réactions suite à l'insertion d'une attaque élaborée par une piste inconnue

La planification est adaptée au niveau de dangerosité de la situation et change suivant l'évolution des paramètres de la menace et de la cible. Ceci est traduit dans le second scénario envisagé où la menace est désormais extrême.

Les éléments qui ont influencé la planification dans la figure 8 sont : le ranking entre la menace et la cible qui correspond au temps nécessaire à la menace pour parcourir la distance restante jusqu'à la cible, la distance entre la menace et la cible et le temps d'intervention du navire de sûreté. L'identité de l'attaquant est hostile et utilise un bateau de haute manœuvrabilité.

Le niveau de danger est 4 avec un pourcentage de 79,79%. Cette valeur permet d'augmenter le degré de réaction, traduit notamment par les actions suivantes :

- regrouper l'équipage
- mettre en sécurité et sûreté les installations de production
- verrouiller l'accès aux zones sensibles

La génération des exemples d'attaques, permet d'affiner les probabilités et de tester la réaction du réseau bayésien en changeant les paramètres relatifs à la menace, la cible, l'environnement, etc.

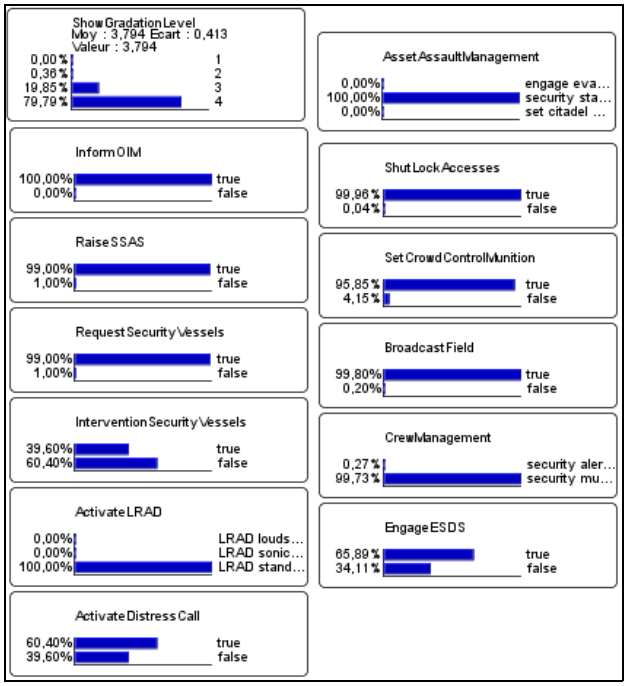


Fig. 8 : Cas d'une menace extrême contre un FPSO

## 4.2 Intégration du réseau bayésien au système SARGOS

Afin d'intégrer l'utilisation du réseau bayésien dans le système SARGOS, un prototype intégrant en entrée un rapport d'alerte et générant en sortie un rapport de planification « Response Plan » a été développé.

Le plan de planification contient l'ensemble des contre-mesures à appliquer par l'équipage ou automatiquement par le système.

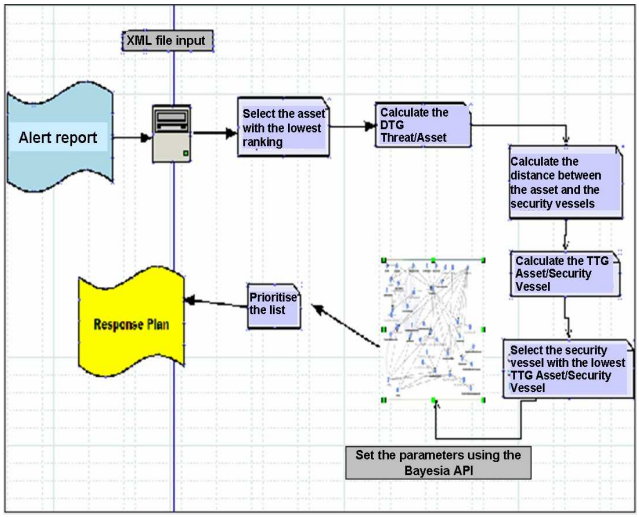


Fig. 9 : Schéma fonctionnel du prototype d'intégration du réseau bayésien dans le système SARGOS

La figure ci-dessus montre les calculs intermédiaires réalisés utiles pour alimenter le réseau bayésien d'experts via le module BayesiaEngine qui offre une interface

d'application (API) et une librairie Java. Via ce module, les paramètres concernant une attaque sont insérés dans le réseau qui est invisible pour l'utilisateur final.

Les résultats des contre-mesures varient en fonction des situations d'où la nécessité de fixer un seuil d'activation pour n'intégrer que les contre-mesures dont la réponse est la plus pertinente à cet instant donné dans la situation présente. Il a été décidé que seules les contre-mesures, intégrées au rapport de planification, dont une des modalités obtient une probabilité strictement supérieure à 70% soient pris en compte dans l'élaboration de la réponse. Ce seuil a été choisi par les experts car il correspond à une réalité supérieure à deux cas sur trois qui se réalisent. Après de nombreux essais et ajustements, les résultats en sortie du réseau correspondaient ainsi à des réponses fiables et réalistes.

Une fois que les contre-mesures dont la valeur de la probabilité en sortie du réseau bayésien dépasse le seuil d'activation, sont sélectionnées, elles sont inscrites dans le rapport de planification suivant un ordre d'affichage précis.

Les principaux facteurs qui jouent sur cet ordre de priorisation sont :

- le mode d'action de la contre-mesure
- la facilité de mise en œuvre de la contre-mesure
- l'automatisation poussée ou la nécessité d'un grand nombre de personnes pour l'activer
- le temps nécessaire pour que la contre-mesure soit effectivement efficace
- les éventuelles fonctions additionnelles d'une contre-mesure

Le système SARGOS peut traiter plusieurs menaces au sein d'un seul rapport d'alerte. La première cible à traiter est donc toujours celle qui présente le ranking le plus faible, car elle est la plus exposée à la menace. Le rapport de planification est partagé en deux parties. La première partie est la communication et la demande d'assistance qui concernent l'ensemble du champ pétrolier avec l'affichage du niveau de dangerosité de la menace. La deuxième partie concerne les cibles spécifiquement mises en danger. Pour chaque cible, SARGOS affiche les contre-mesures à déclencher.

# 5. Conclusion et perspectives

La planification de la réponse de SARGOS passe par l'émission d'un rapport de planification issu du traitement intelligent du rapport d'alerte. Ce rapport rassemble les informations nécessaires à l'établissement d'une réponse "physique" pour se protéger contre une menace.

La contrainte initiale du projet est respectée puisque toutes les contre-mesures sont des réactions non létales.

L'utilisation d'un réseau bayésien pour la planification de la réaction est un atout majeur du système SARGOS puisque le réseau gère toutes les interactions possibles entre les caractéristiques de la menace et de la cible attaquée, l'environnement, la gestion de l'équipage et des installations et surtout, il s'adapte à l'évolution du niveau de danger de la situation.

Enfin l'évolutivité du réseau est possible par l'intégration des retours d'expériences relatifs aux traitements des attaques qu'il est amené à gérer. Le module de planification est ainsi adapté et amélioré de manière itérative.

# Références


[1] M.A. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Bottala Gambetta, D. Chaumartin, M. Philips, M. Morel, C. Imbert, E. Itcia, D. Bonacci et P. Michel. *SARGOS : Securing Offshore Infrastructures Through a Global Alert and Graded Response.* System Workshop MAST Europe 2011, 27-29 juin 2011, Marseille.

[2] M.A. Giraud, B. Alhadef, F. Guarnieri, A. Napoli, M. Bottala Gambetta, D. Chaumartin, M. Philips, M. Morel, C. Imbert, E. Itcia, D. Bonacci et P. Michel. *SARGOS : Système d'Alerte et Réponse Graduée Off Shore.* Conférence WISG, 25-26 janvier 2011, Troyes.

[3] M.A. Giraud, A. Van Gaver, A. Napoli, C. Scapel, D. Chaumartin, M. Morel, E. Itcia et D. Bonacci. *SARGOS : Système d'Alerte et Réponse Graduée Off Shore.* Conférence WISG, 26-27 janvier 2010, Troyes.

[4] B.S. Ware, A.F. Beverina, L. Gong et B. Colder. *A Risk-Based Decision Support System for Antiterrorism*. Digital Sandbox, 14 Août 2002.

[5] Naîm, P., Wuillemin, P.H., Leray, P., Pourret, O. et Becker, A. *Les réseaux bayésiens 3,* 1999.