The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields

Xavier Chaze, Amal Bouejla, Aldo Napoli, Franck Guarnieri, Thibaut Eude, Benjamin Alhadef

The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields

Xavier Chaze[1], Amal Bouejla[1], Aldo Napoli[1], Franck Guarnieri[1], Thibaut Eude[2], and 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, France
[2] SOFRESUD, 777 Avenue des Bruxelles, 83500 La Seyne sur Mer Cedex

Abstract. In recent years pirate attacks against shipping and oil fields have continued to increase in quantity and severity. For example, the attack against the Exxon Mobil oil rig in 2010 off the coast of Nigeria ended in the kidnap of 19 crew members and a reduction in daily oil production of 45,000 barrels, which resulted in an international rise in the price of oil. This example is a perfect illustration of current weaknesses in existing anti-piracy systems. The SARGOS project proposes an innovative system to address this problem. It takes into account the entire threat treatment process; from the detection of a potential threat to implementation of the response. The response to an attack must take into account all of the many parameters related to the threat, the potential target, the available protection resources, environmental constraints, etc. To manage these parameters, the power of Bayesian networks is harnessed to identify potential countermeasures and the means to manage them.

1 Introduction

World oil production is spread over more than 10,000 offshore fields, each of which requires tools and equipment to extract, process and temporarily store oil, and vessels that can transport the hydrocarbons between the point of production and the point of consumption.

Modern maritime piracy is currently the major threat to the security of these energy production installations and the maritime shipping of oil.

Monitoring methods, and above all protection measures are the major weaknesses in the detection of a threat on such installations. They tend to be ineffective and limited in the extent to which they can be tailored to a particular situation. Finding a system that can manage the safety of oil fields, and provide both suitable protection and effective crisis management is of primary importance.

The SARGOS project is a response to this need. It proposes a global system in the fight against acts of piracy committed against oil industry infrastructure.

H. Yu et al. (Eds.): DASFAA Workshops 2012, LNCS 7240, pp. 81–91, 2012.

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

This paper discusses the issues surrounding acts of oil field piracy. It describes in detail a method for the planning of countermeasures. Notably, it uses a Bayesian network to model the situation using two different inputs: the Piracy and Armed Robbery database of the International Maritime Organization (IMO) and the consolidated knowledge of experts in the domain. The results are tested using realistic and comprehensive pirate attack scenarios.

2 Problem Definition and Research Objectives

The infrastructure of the offshore oil industry is subject to a constantly rising risk of piracy. These acts have repercussions both on local operations and globally. This section describes the economic and political challenges related to these attacks. It highlights an increasingly insecure context, where the actors involved in the offshore oil industry are helpless to protect themselves, and the current tools do not effectively protect infrastructure. Finally, we outline the SARGOS project, illustrate its potential contribution to finding new ways of dealing with these issues and demonstrate their relevance.

2.1 Political and Economic Challenges

The offshore oil industry is growing rapidly. Offshore oil extraction currently accounts for about one-third of global oil production. Despite its scarcity, this source of energy is under active exploration in many parts of the world.

From an economic perspective, it is important to highlight that attacks on such infrastructure generate significant additional costs (ransom payments, insurance premiums, the installation of security equipment etc.). These additional costs directly affect the price of oil in the international market.

From the political perspective offshore oil fields are an interface between the activities of the oil industry and the maritime world. The legal status of oil rigs is complicated, although this is due more to the heterogeneity of applicable regulations than the absence of a body of law. This complexity can result in political conflicts between nations; it is often the case that the rig is located in one country, while the company operating the platform is located in another.

The importance of oil installations to the world economy and global industry, and the consequences that can arise from acts of piracy provides a strong incentive to better protect these assets.

2.2 Context and Operational Needs

Despite the fact that attacks against oil fields are infrequent and above all, receive little media coverage, they are of great cause for concern because of the serious consequences for both crew and infrastructure.

Infrastructure managers, employees and safety officers no longer want to see commercial assets become the subject of large ransoms. Nor do they want to

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

continue to see crewmen injured, traumatized, held under extreme conditions for long periods of time, or even killed. For their part, insurers do not want to continue to insure highly expensive risks for an indefinite period of time. Finally, nations want to see an end to the situation where the price of oil is affected by such events.

The recent attacks are a perfect illustration of the weakness of existing anti-piracy tools. Currently, the safety of oil installations is provided by so-called classical tools (radio identification, radar, Automatic Identification Systems, etc.). Despite their usefulness in helping to detect threats, they cannot distinguish between different types of hazard (fishing boats, jet skis, tankers, etc.). Moreover, their effectiveness depends on many and various parameters that are related to the environment as well as technical and operational constraints.

The proposed solution is therefore to increase the degree of infrastructure protection by developing a new system (SARGOS), which is capable of generating an alarm and can set in motion an internal and external response to a confirmed intrusion.

2.3 The Contribution of the SARGOS Project

The SARGOS project (*Système d'Alerte et de Réponse Graduée OffShore*/Graduated Offshore Response Alert System) aims to meet this new need to protect vulnerable civilian infrastructure, which is exposed to acts of piracy or terrorism carried out at sea. The project aims to design and develop a comprehensive system that takes into account the whole threat treatment process, from the detection of a potential threat to the implementation of the response. It can be integrated into the infrastructures operations and respects regulatory and legal constraints.

The project is funded by the French National Research Agency (*L'Agence Nationale de la Recherche*)[1] , and is approved by other regional bodies in France. The development of a comprehensive protection system requires multi-disciplinary technical skills; challenges include the automatic detection and identification of threats, assessment of potential risks, and management of an appropriate response. The functional outline of the SARGOS system (Figure 1) shows how the threat is processed.

In the context of the current discussion, there is insufficient emphasis on the preparation of the diagnosis and the way in which parameters and constraints related to attacks should be managed. In order to address these shortcomings, we propose a new approach that can automatically draw up response plans, tailored to the type of intrusion detected.

[1] The SARGOS project brings together many different private sector organisations (including the French naval shipbuilder, DCNS and SOFRESUD, a supplier of high-tech equipment to the defence industry) and public research centres (including ARMINES, a French contract research organisation and TéSA, Telecommunications for Space and Aeronautics).

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

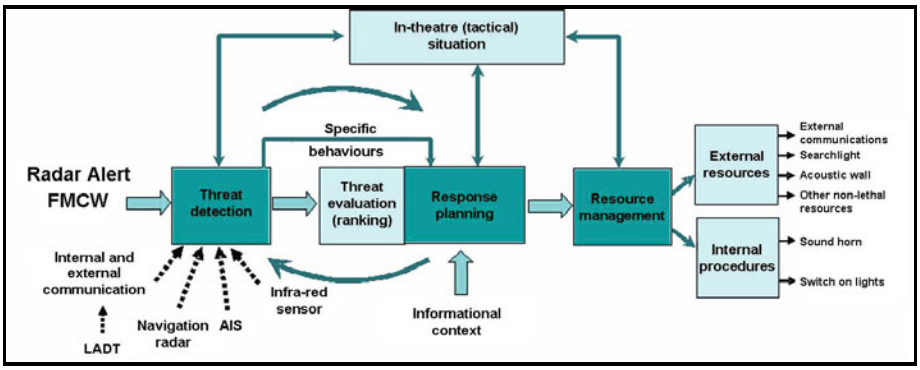

Fig. 1. Functional outline of the SARGOS system

3 Method

This paper will focus particularly on the contribution of a Bayesian inference approach, which uses input from an established database and the knowledge of experts in the maritime domain. The Bayesian network is used in the response planning process and the aim is to prepare a response that is appropriate, graduated and which can adapt as the threat evolves. Database information and the knowledge of oil industry experts are used together to address the lack of both *a priori* knowledge of the object in question and learning from experience in the applied domain.

The Bayesian network is used to model this information and knowledge; the tool is based on Thomas Bayes theorem (1), which forms the basis for probability theory.

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

A Bayesian network is a model that represents knowledge, and makes it possible to calculate conditional probabilities and provide solutions to various types of problems.

BayesiaLab software[2] was used to construct the Bayesian network. This tool for modelling Bayesian networks has many features and an intuitive graphical interface.

The SARGOS Bayesian network was developed in two stages, described below: first an initial network was constructed using data from an established, professional database, and then the final network was built using expert knowledge from the field.

[2] The BayesiaLab software has been developed by the French company Bayesia (`http://www.bayesia.com/`).

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

3.1 Construction of a Bayesian Network from Database Content

The first stage exploited data from the Piracy and Armed Robbery database of the International Maritime Organization (IMO). It is the only database in existence that holds records (dating from 1994) of pirate attacks in the maritime environment. On 15^{th} July, 2011 this database held 5,502 records and recorded the following information for each attack: the name of the asset targeted, the number of people involved, the type of weapon used, the measures taken by the crew to protect themselves, the impact on the crew and pirates, etc.

From this data the BayesiaLab software automatically generates a Bayesian network and suggests dependency relationships between the main elements found in the database. This study of the contents of the database made it possible to define the principle countermeasures adopted by the majority of entities attacked, namely: engage evasive manoeuvres, activate the Ship Security Alarm System (SSAS), contact the security vessel, move the crew to a safe location, and turn on the searchlight, etc.

These modalities and conditional probabilities were then used to construct the expert knowledge Bayesian network.

Figure 2 shows the Bayesian network created from the database content. Information such as longitude, latitude, name of the asset targeted, etc. was not used as data was not available for all attacks.

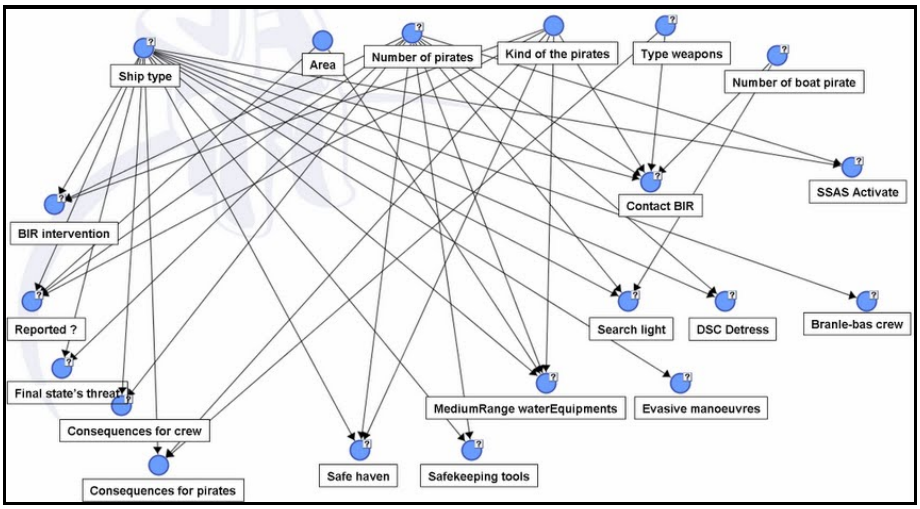

Fig. 2. The Bayesian network constructed from IMO data

In its initial form, the probability distribution of the nodes shows that most ships that come under attack are bulk carriers or tankers (this raw data does not reflect the application of constraints relating to particular attacks).

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

66.39 percent of attacks occur in international waters; this is due to the lack of security controls. Equally often, pirates profit from attacking in numbers: 60.39 percent of attacks are organized by pirate teams consisting of more than five people.

This network provides a very clear view of the pirates tactics, how they are armed, and above all the number of people involved.

The following example demonstrates how the network can be used to simulate a particular attack scenario. In the example, specific modalities are set for nodes that characterize an attack:

- The asset targeted: a tanker
- The location of the incident: international waters
- Type of attackers: thieves
- Type of weapons: armed personnel.

This makes it possible to identify the countermeasures used. The Bayesian network indicates that in this situation, the robbers fired shots at the potential target and that the crew, in order to protect themselves, tried to apply evasive manoeuvres and used high-pressure fire hoses on the attackers.

The Bayesian network created from the IMO data made it possible to make an initial assessment of the main tools and protection measures used by a crew under attack to protect themselves, to evaluate the effectiveness of these tools, and to determine the probability of certain types of attack.

Secondly, the use of this database made it possible to test the functionality of the BayesiaLab tool and establish the feasibility of creating a Bayesian network from existing data.

3.2 Construction of a Bayesian Network from Expert Knowledge

The first stage of the project was to construct a Bayesian network from the IMO data. In the second stage, expert knowledge from the marine community was used to construct the network. Civil and military experts in the maritime domain shared their experiences and opinions during successive brainstorming sessions to define the variables (Bayesian network nodes) and connections (links between nodes) of the system. As a result of this expert knowledge the initial conditional probabilities were set. These probabilities were then updated through an iterative process in which many scenarios were simulated in order to verify, and if necessary refine, the values which had been set for each node.

The principle is the following: when an object is detected by radar in the vicinity of an oil field, a set of variables is determined and calculated in order to identify and assess the potential danger. Such information includes, for example, the speed at which the object is moving, visibility, time of day, longitude and latitude of the object and the target etc.

This data is used to calculate the distance between the target and the moving object, and the time required for the intervention of the security vessel. This information is recorded in an alert report and each object detected is allocated

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

a unique identifier. The SARGOS system only generates this report when the threat is identified as suspicious or hostile.

The basic architecture of the SARGOS response planning network consists of five modules and four sub-modules. The definition and the scope of each of these five modules are directly related to the meaning of the nodes that constitute them. The modules are classified as: basic parameters, the overall danger level of the situation, aggravating factors and constraints, nodes related to communication and distress calls and countermeasures. These are described in detail below.

The Basic Parameters. These are static or dynamic physical data that characterize the threat and the target. They are the direct result of, or are derived from, the intermediate calculations of the alert report. They constitute the minimum data necessary to create a model that is still sufficiently detailed to permit a full understanding of the threat and the target, and the issues involved in responding to an attack. These parameters include, for example, the identity of the threat IdentityClass (suspicious or hostile), the distance between the threat and the target DTG Threat/Asset, the criticality of the target AssetAssessment. Four modalities are defined for this node: critical, major, significant and other.

The Overall Danger Level of the Situation. The overall danger level of the situation is derived from the basic parameters. The node ShowGradationLevel is the formalization of this module in the Bayesian network. The grading system uses levels 1-4 (1 being least serious, 4 being most serious). This level, and the planning of countermeasures, is constantly adapted to each situation.

Aggravating Factors and Constraints. Aggravating factors and constraints are both internal and external elements of the system.

Aggravating factors make it possible to take into account a potential deterioration in the situation and thus to anticipate potential planning options. They represent the environment, for example the visibility (Visibility) and the time of day (PeriodOfDay).

Constraints are represented by parameters that reflect the effectiveness of the response both technically and operationally. Technical constraints are directly related to the use of countermeasures and include factors such as their availability (ImmediateReadiness) or the potential for remote control (RemoteControlled).

Communication and Distress Calls. Communication and the distress call are two indispensable resources called upon in response to a threat. Internal communication at the target can be used to notify all relevant personnel (e.g. inform the Offshore Installation Manager, InformOIM), while external communication operates at various levels to alert the various actors involved in safety at sea (for example, to request the intervention of security vessels RequestSecurityVessels, or activate the Ship Safety Alarm System, RaiseSSAS). This communication makes it possible for oil field installations and shipping to prepare their response and to ask, where possible, for outside intervention.

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

Countermeasures. This refers to the set of defensive measures implemented when the target is attacked, in order to protect itself against an identified threat. They are the concrete expression of the response and provide a set of means and actions to normalize the situation as quickly as possible following an attack.

The countermeasures module is divided into four sub-modules which are the core of the concept of a graduated response as they off er increasingly forceful countermeasures depending on the nature of the detected threat: they include deterrence and low-impact repulsion measures; repulsion, anti-boarding and neutralization measures; management of procedures, and ensuring the safety and security of the facility. They are described in detail below.

Deterrence and Low-Impact Repulsion Measures. These inform attackers that the target is aware of their intentions, that the target is able to follow the attackers and the target has no interest in taking action. Low-impact repulsion is the ability of the target to repel the attack using relatively low impact means such as searchlights, high-pressure fire hoses or Long Range Acoustic Devices (ActivateLRAD).

Repulsion, Anti-boarding and Neutralization Measures. These are high-impact countermeasures, whose main function is at least to mitigate if not neutralize attackers. The node EngageRepellentEquipment encompasses a growing number of resources available on the maritime piracy market that make it possible to repel an attack at a distance, while respecting the principle of non-lethal self-defence. The main function of anti-boarding measures, as with repulsion equipment, is to prevent attackers from being able to board should they approach the facility or ship.

The role of SetCrowdControlMunition is to delay the progress of the attackers to the point of exhaustion, or even neutralize them and so allow maximum time for the crew to deploy other safety actions.

Procedure Management. This consists of the following countermeasures:

The CrewMangement node refers to the sounding of crew action-stations, and for the crew to immediately report to their pre-assigned post or station on the installation.

The AssetAssaultManagement node relates to the management of safety and security at the potential target. The modalities of this node are: withdrawal to a designated safe room, evasive manoeuvres (on mobile units and ships), and activating the security station (this consists of particular procedures to be followed by individual crew members when the alarm is raised).

Ensuring the Safety and Security of the Facility. As is the case with procedure management the SARGOS system includes action plans for the management of production equipment in order to safely shut it down, and deny access to sensitive areas.

Conditional Probabilities. In the Bayesian network, each module or sub-module consists of one or many nodes that all have an effect on each other.

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

Each node consists of a matrix of conditional probabilities that are calculated by taking into account the various influences between nodes and the actual situation represented by the node itself.

The probabilities of the base nodes are normalized, i.e. elements that would characterize a specific attack have not been added.

4 Discussion

When the probability distribution of the different modalities has been established, and the Bayesian network has been developed, various attack scenarios can be simulated. Once the initial conditions have been determined, the network translates them into a response report. Experiments with different potential scenarios enabled the network to be finalised before it was integrated into the SARGOS system.

4.1 Attack Scenario Case Studies

The following two examples demonstrate what happens when parameters are set to simulate an attack on a Floating Production, Storage and Offloading (FPSO) unit, which is considered to be a critical asset. Figure 3 describes the first scenario where an unknown vessel creates the threat.

The parameters that were set to reproduce the scenario on an FPSO are: the identity class of the threat, the ranking between the threat and the target (Ranking Threat/Asset, which corresponds to the time in seconds required for the threat to travel the remaining distance to the target), the distance between the threat and the target (DTG Threat/Asset, in meters), the security vessel response time (TTG SecurityVessels/Asset, in seconds), the time of day and the visibility. The simulation shows that the danger level of this situation is 2, with a percentage of 64.68. In this case the countermeasures to be applied are: inform the boatswain, request the intervention of a security vessel, send a clear, strong message using a long-range loudspeaker, activate the searchlight, activate the security station, and activate repulsion equipment. Planning is tailored to the danger level of the situation and evolves in response to changes in the parameters relating to the threat and the target. In the second scenario the attacker is now hostile, armed and equipped with a highly manoeuvrable boat. This high-threat scenario is described in Figure 4.

In this scenario, the danger level is 4, with a percentage of 79.79. Figure 5 illustrates the adapted response plan. This level of danger requires internal and external communications (BroadcastField and ActivateDistressCall) but more importantly, a more vigorous response demonstrated by the following countermeasures: assemble the crew (CrewManagement), activate the security station (AssetAssaultManagement), ensure the safety and security of the production facility (EngageESDS), block access to sensitive areas (ShutLockAccesses) and delay the progress of the attackers (SetCrowdControlMunition). Finally, a low-impact repulsion measure such as the Long Range Acoustic Device (ActivateLRAD) is put on stand-by.

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

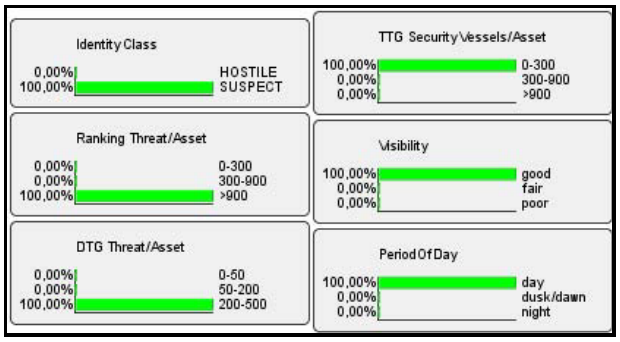

Fig. 3. Observations set for scenario1

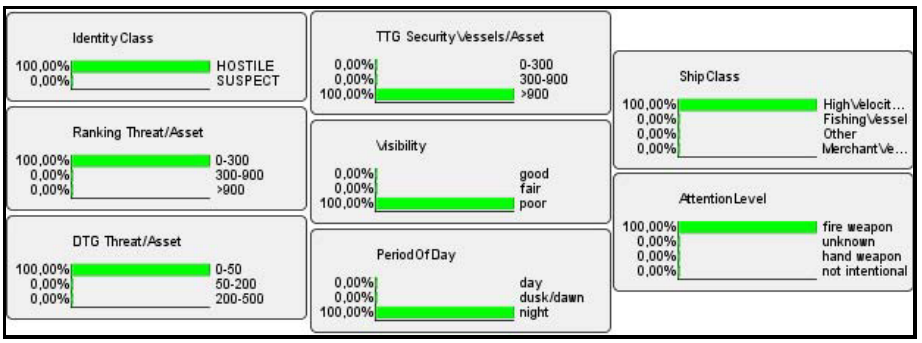

Fig. 4. Observations set for scenario2

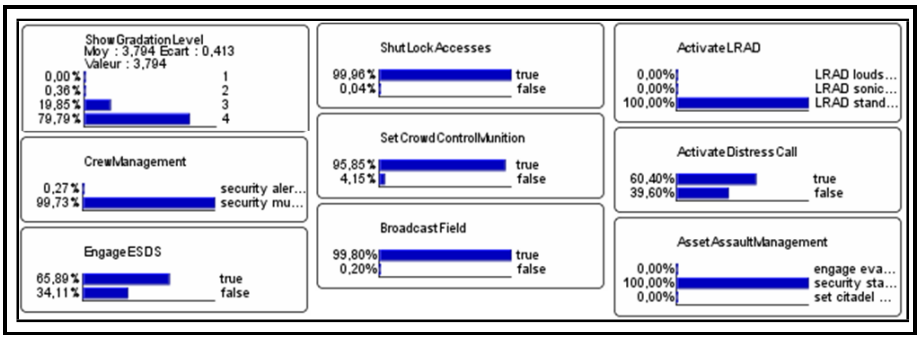

Fig. 5. Simulation of a high-threat scenario on an FPSO

Generating attack scenarios in this way helps to refine the probability distribution and tests the response of the Bayesian network to changes in parameters (the threat, the target, the environment, etc.).

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91

4.2 Integration of the Bayesian Network into the SARGOS System

In order to integrate the Bayesian network into the SARGOS system, a prototype was developed that took as input an alert report and generated as output a response plan. The response plan contains all the countermeasures to be applied either by the crew or automatically by the system. Once the countermeasures (whose probability exceeds the activation threshold) have been selected, they are displayed in the response plan in a specific order. The main factors that determine the order are: the action mode of the countermeasure, its ease of implementation, the extent to which it is automated (or the need for a large number of people to activate it), the time needed for it to become effective, and any potential additional functions.

5 Conclusion and Future Work

The SARGOS system responds to an alert report with a response plan, which is the result of an intelligent analysis of the alert report. This response plan brings together the information necessary for the physical installation to protect itself against a threat.

An initial constraint of the project is met, as all the countermeasures are non-lethal responses.

The use of a Bayesian network for the planning of the response is a major asset of the SARGOS system as this network can handle all possible combinations of threat characteristics, the target under attack, environment, crew management and facilities. Most importantly, it adapts to changes in the danger level of the situation.

Finally, the network is able to integrate feedback from attacks that has previously been used to administer and can therefore evolve. Consequently, the planning module can be modified and improved iteratively.

References

[GA1] Giraud, M.A., Alhadef, B., Guarnieri, F., Napoli, A., Bottala Gambetta, M., Chaumartin, D., Philips, M., Morel, M., Imbert, C., Itcia, E., Bonacci, D., Michel, P.: SARGOS: Securing Offshore Infrastructures Through a Global Alert and Graded Response. In: System Workshop MAST Europe, Juin 27-29 (2011)

[GA2] Giraud, M.A., Alhadef, B., Guarnieri, F., Napoli, A., Bottala Gambetta, M., Chaumartin, D., Philips, M., Morel, M., Imbert, C., Itcia, E., Bonacci, D., Michel, P.: SARGOS: Système d'Alerte et Réponse Graduèe Off Shore. In: Conference WISG, Janvier 25-26 (2011)

[GV1] Giraud, M.A., Van Gaver, A., Napoli, A., Scapel, C., Chaumartin, D., Morel, M., Itcia, E., Bonacci, D.: SARGOS: Système d'Alerte et Réponse Graduèe Off Shore. In: Conference WISG, Janvier 26-27 (2010)

[WB1] Ware, B.S., Beverina, A.F., Gong, L., Colder, B.: A Risk-Based Decision Support System for Antiterrorism. Digital Sandbox, 8 pages (Août 14, 2002)

[NW1] Naïm, P., Wuillemin, P.H., Leray, P., Pourret, O., Becker, A.: Les réseaux bayésiens 3, 424 pages (1999)

Chaze X., Bouejla A., Napoli A., Guarnieri F., Eude T. et Alhadef B., 2012 :
« The Contribution of Bayesian Networks to Manage Risks of Maritime Piracy against Oil Offshore Fields »,
Conférence internationale ITEMS 2012 (Information Technologies for the Maritime Sector), Busan, Corée du Sud,
DASFAA Workshops 2012, Lecture Notes in Computer Science Volume 7240, 2012, pp 81-91