Bayesian Networks in the Management of Oil Field Piracy Risk

Amal Bouejla, Xavier Chaze, Franck Guarnieri, Aldo Napoli

Bayesian Networks in the Management of Oil Field Piracy Risk

A. Bouejla [1], X. Chaze [1], F. Guarnieri [1], A. Napoli [1]
[1] *MINES ParisTech, Centre for Research on Risks and Crises, France*

Abstract

In recent years, pirate attacks against shipping and oil field installations have become more frequent and more serious. The SARGOS system provides an innovative solution that addresses the problem from the perspective of the entire processing chain; from the detection of a potential threat to the implementation of a response. The response to an attack must take into account multiple variables: the characteristics of the threat and the potential target, existing protection tools, environmental constraints, etc. The potential of Bayesian networks is used to manage this large number of parameters and identify appropriate counter-measures.

Keywords: Oil platforms, pirate attacks, Bayesian networks, SARGOS system

1 Introduction

Global oil production is spread over more than 10,000 offshore fields each of which requires on the one hand, equipment for the extraction, processing and temporary storage of crude oil and on the other hand, shipping capable of transporting petroleum between production and consumption sites.

These sites of energy production and the corresponding maritime transportation systems are subject to a high risk of piracy. Current monitoring systems have major weaknesses in terms of threat detection, and the procedures to be applied in the case of an attack are often particularly inefficient and inadequate. It is therefore essential that any system able to manage oil field security can offer suitable protection and provide effective crisis management.

This paper first describes the issues associated with acts of piracy against oil fields. In response to these threats a new system was designed that offers a method for the planning of counter-measures. The method, which is described in detail, includes notably the construction of a Bayesian network based on two principles: the use of the International Maritime Organization's (IMO) Piracy and Armed Robbery database, and the collection and formalisation of the

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

knowledge of experts in the domain. The paper finally describes how the method was tested using realistic and comprehensive scenarios of pirate attacks.

2 Piracy: an evolving risk and an economic and political challenge

Offshore activity is growing rapidly. The exploitation of offshore oil resources currently represents about a third of global oil production. This energy resource, despite its scarcity, is being explored in many areas, some of which are located in dangerous territorial waters (notably the Gulf of Guinea) that are becoming increasingly unstable. The lack of effective tools for infrastructure protection means that actors involved in the offshore oil and gas industry find themselves helpless. The attacks carried out against them generate significant additional costs, including for example, the payment of ransoms, higher insurance premiums and the installation of security equipment. These additional costs directly affect the international price of oil [1].

Moreover, oil fields form the interface between the maritime world and the petroleum industry. The many and various applicable rules that constitute the legal status of oil rigs create a complex situation, which may generate political conflicts between nations particularly as the nationality of the company operating the platform may not correspond to the physical location of the installation. This raises the question of how responsibility is divided between the different actors charged with protecting the area.

The importance of oil installations for the global economy and industry and the potential consequences of piracy create a strong incentive to better protect these assets. Although attacks against oil fields are infrequent and mostly low-profile, they are extremely disturbing due to the severe impact on the crew and infrastructure. One example is the attack on the Exxon Mobil platform [2] off the coast of Nigeria, which led to the kidnapping of nineteen employees and extensive damage to the facility caused by the explosive devices used by the pirates. This reflects the weakness of current anti-piracy tools.

Infrastructure managers, employees and safety officers do not want to continue to see their ships or other assets become the subject of substantial ransoms, nor crewmen injured, killed or kept in extreme conditions for days or even weeks [3]. At the same time, insurers are unwilling to continue to provide cover for such high risk activities indefinitely. Finally, nations do not want to continue to see the price of oil affected by such events.

Security on oil installations is currently assured by so-called classical tools (radio identification, radar, Automatic Identification Systems, etc.). These tools, despite their ability to detect threats, do not distinguish different types of threat (e.g. a fishing boat or dhow harbouring pirates and a drifting tanker) and their effectiveness depends on many parameters related to the environment and

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

technical and operational constraints. A new solution is therefore needed to improve infrastructure protection. Any new system should be capable of generating an alert and triggering internal and external responses when an intrusion is confirmed.

The Graduated Offshore Alert and Response System (*Système d'Alerte et de Réponse Graduée OffShore*; SARGOS) responds to this need to protect civilian infrastructure vulnerable to acts of piracy or terrorism carried out at sea. The project aims to design and develop a global alert and response system that takes into account the whole chain of events – from the detection of a potential threat to the implementation of the response. The system can be integrated into the infrastructure's operations and takes into account regulatory and legal constraints.

This French project is funded by the National Research Agency (*L'Agence Nationale de la Recherche*); it is recognised by regional organisations and Aerospace Valley (a cluster of French aerospace engineering companies and research centres). Activities include the development of an overall protection system; automatic threat detection and identification; risk assessment; and management of an appropriate response – it therefore draws upon skills from many disciplines[1].

The diagram of the SARGOS system shown in Figure 1 demonstrates the threat processing cycle. Current tools make it very difficult to arrive at a threat diagnosis and to determine how to manage the parameters and constraints related to an attack. The new approach proposed here aims to overcome these shortcomings through the development of automated response plans that are tailored to the nature of the detected intrusion.

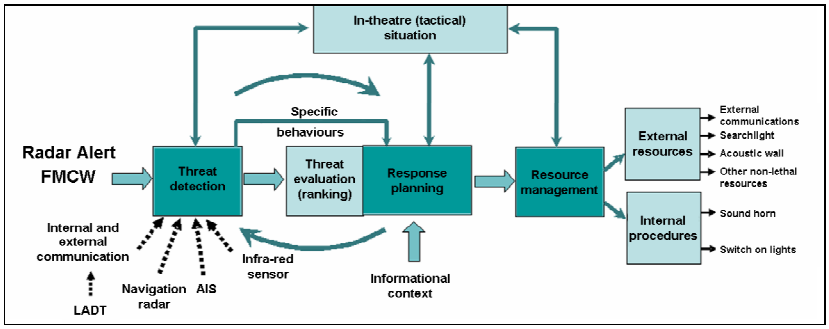

Figure 1: Functional diagram of the SARGOS system

[1] SARGOS project participants include private sector organisations such as DCNS (a French naval shipbuilder) 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).

3 The contribution of Bayesian networks to the creation of threat response action plans

A detailed investigation of the issues highlights significant constraints that the SARGOS system must take into account in order to fully reflect the complexity of a situation. On the one hand, the large number of variables to be included (representing the threat, the target, the environment, etc.) and the dependencies that may exist between them suggest the development of a decision support system based on graph theory. On the other hand, the uncertainty inherent in certain variables (threat identification, intervention options, etc.) emphasises the need for a system based on probability theory and probabilistic calculations. With these two approaches in mind, a process for the automatic preparation of response plans tailored to the nature of the detected intrusion, based on Bayesian networks was explored.

The response planning process aims to develop an appropriate, graduated and progressive response to a threat. The lack of knowledge and feedback related to attacks on oil platforms is addressed by the incorporation of database information and the knowledge and experience of experts in the maritime domain. This information and knowledge is then modelled with Bayesian networks; these tools are based on Thomas Bayes' theorem (1), which is one of the foundations of probability theory [4].

$$P(A/B) = \frac{P(B/A)\,P(A)}{P(B)} \qquad (1)$$

A Bayesian network is a system for the representation of knowledge and the calculation of conditional probabilities, which can be applied to many complex problems [5], [6] and [7].

BayesiaLab[2] software was used to build the Bayesian network. This powerful Bayesian network modelling tool provides an intuitive graphical interface.

The SARGOS Bayesian network was developed in two stages, which are described below, namely: the construction of an initial network from data contained in a specialist database and the creation of the final network enriched by expert domain knowledge.

3.1 Construction of a Bayesian network based on existing data

The first step exploited data contained in the Piracy and Armed Robbery database of the IMO. This is the only existing database to contain historic (dating back to 1994) data on pirate attacks in the maritime environment. On 15th July,

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

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

2011 the database contained records of 5,502 attacks and the data noted for each attack included: the name of the asset under attack, the number of attackers, the weapons used, the measures taken by the crew to protect themselves, the impact on the crew and the pirates, etc.

From this data, the BayesiaLab software was able to automatically generate a Bayesian network and propose interdependencies between the principal basic elements [8]. This analysis made it possible to establish the main protective measures taken by the majority of entities attacked. They included for example: initiate evasive manoeuvres, activate the Ship Security Alarm System (SSAS), contact the security vessel, secure the crew, turn on searchlights, etc.

These modes and conditional probabilities were then used to construct the expert network. Figure 2 shows the Bayesian network built from the information contained in the database. Some information, such as the longitude, latitude, name of the asset attacked, etc. is not included. This is due to the fact that this data was not specified for all attacks.

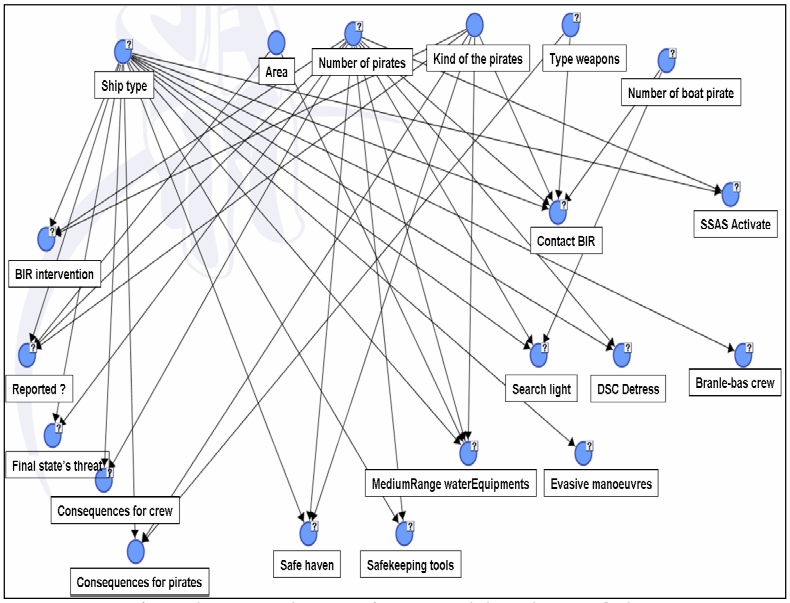

Figure 2: The Bayesian network based on IMO data

A classical statistical analysis of this data provided some initial findings that included the following observations: most ships that come under attack are bulk carriers or tankers; 48% of attacks take place in international waters (due to the absence of security patrols); and pirates prefer to attack in numbers (68% of attacks are organised by teams of more than five).

The network provides a very clear view of the tactics of pirates, the weapons they use, and above all the number of individuals involved. In addition, an examination of the network makes it possible to identify the principal tools and measures deployed by the crew of assets under attack in order to protect themselves, to assess the effectiveness of these tools and to define the probabilities of occurrence of certain types of attack.

3.2 Construction of a Bayesian network based on expert knowledge

The Bayesian network created from the modalities and conditional probabilities found in the IMO data provided a formal framework into which domain experts were able to integrate their knowledge in order to build the final SARGOS Bayesian network [9]. In this second step, experts from the maritime and oil domains analysed the data extracted from the Bayesian network created from IMO data. As the information contained in the IMO database related primarily to attacks on shipping, the contribution of knowledge from domain experts made it possible to extend the system to include oil fields: nodes and arcs were added to the model in order to make it as versatile as possible [10].

The basic architecture of the SARGOS response planning network was developed through the course of multiple brainstorming sessions during which various maritime security experts shared their experiences and discussed the modalities and probabilities of the network. The final architecture consisted of four modules and five sub-modules (Figure 3).

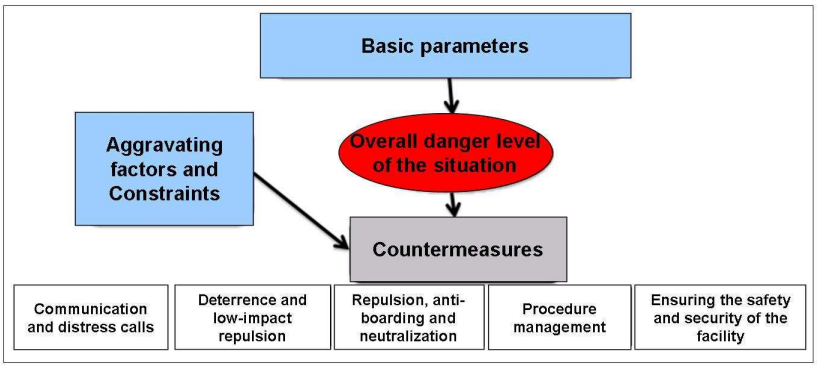

Figure 3: Structure of the SARGOS Bayesian network

In the Bayesian network, each module or sub-module consists of one or more nodes that receive input from and/or provide input to other nodes. Each node consists of a matrix of conditional probabilities that are calculated from an assessment of the interactions the node has with other nodes and the reality represented by the node itself.

The definition of the scope of each module is directly related to the composition of its constituent nodes. Module definitions include basic parameters, the overall danger level of the situation, aggravating factors and constraints, counter-measures and nodes related to communication and the request for assistance. These modules are described in detail below.

3.2.1 Basic parameters

Basic parameters are static or dynamic physical data that characterise the threat and the target. They are the direct result of, or are derived from the intermediate calculations of the alert report. They represent a minimum, but sufficiently detailed level of modelling required for a full understanding of the threat and the target when considering potential responses to an attack. Basic parameters include, for example, identification of the threat (suspicious or hostile), the distance between the threat and the target and the criticality of the target (divided into four categories: critical, major, significant or otherwise).

3.2.2 The overall danger level of the situation

The overall danger level of the situation is arrived from the basic parameters. The grading system runs from level 1 (least serious) to 4 (most serious). This level and the planning of counter-measures are constantly adapted to the situation.

3.2.3 Aggravating factors and constraints

Aggravating factors and constraints are elements that are both internal and external to 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 visibility and time of day. Constraints are represented by parameters which reflect the effectiveness of the response both technically and operationally. Technical constraints are directly related to the deployment of counter-measures – they include issues such as what equipment is available and the potential for remote control.

3.2.4 Communication and the request for assistance

Communication and the request for assistance are two key responses to a threat. Internal communication at the target can alert all relevant personnel (e.g., informing the crew master) while external communication makes it possible at various levels to warn the different actors involved in maritime security (request the intervention of the security vessel, activate the Ship Security Alarm System, etc.). These types of communication enable installations and shipping to prepare their response plan and to establish if external intervention is available.

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

3.2.5 Counter-measures

Counter-measures comprise all the defences mobilised by the target under attack in order to protect itself against an identified threat. They are the actual realisation of the response plan and constitute the set of means and actions intended to normalise, as quickly as possible, the situation. Counter-measures are divided into five sub-modules. These reflect the concept of a graduated response by proposing increasingly forceful measures depending on the nature of the detected threat. Measures range from deterrence and small-scale repulsion, through repulsion, anti-boarding measures and neutralisation, to procedure management and securing the facility. They are described in detail below.

Deterrence and small-scale repulsion measures are intended to inform the attacker that the target is aware of the attacker's intentions, can follow the attacker and that it is not in the attackers' interest to continue their actions. These measures include the ability of the target to repel an attack with low-impact devices such as searchlights, fire hoses or sonic cannons.

Repulsion, anti-boarding and neutralisation are high-impact measures whose main function is to at least mitigate an attack, if not neutralise the attackers (while remaining within the bounds of non-lethal self-defence). These devices also have the advantage of providing the crew with enough time to mobilise other defensive measures.

Procedure management is composed of two counter-measures. On the one hand, it involves the sounding of crew Action Stations and the reporting of crew to their pre-assigned post or station and, on the other hand, securing the target of the attack. Potential actions include: activate the Citadel, engage evasive manoeuvres (for mobile units and shipping), and declare the security post (a set of individual procedures undertaken by each crew member as necessary).

Like procedure management, the SARGOS system offers a way to secure the installation through the planning of actions related to the control of equipment on the installation in order to safely stop production and prevent access to sensitive areas [11], [12].

4 Discussion

Once the probability distribution of the various modalities has been established, an interesting exercise is to test the Bayesian network by simulating attack scenarios through the selection of certain criteria. An examination of these scenarios made it possible to finalise the network before integrating it into the SARGOS system.

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

4.1 Attack scenarios

The example below (Figure 4) shows how response planning is tailored to the danger level of the situation and can adapt to changes in parameters representing the threat and the target. Specifically, it shows the results of setting parameters to simulate an attack on a Floating Production, Storage and Offloading (FPSO) unit by an unknown vessel. This example shows that the danger level of the situation, at time T1, was 2 with a 64.68% probability of occurrence. In this case the counter-measures to be applied were: inform the crew master, request the intervention of the security vessel, broadcast a strong message by loudspeaker, turn on the searchlight and activate the security post.

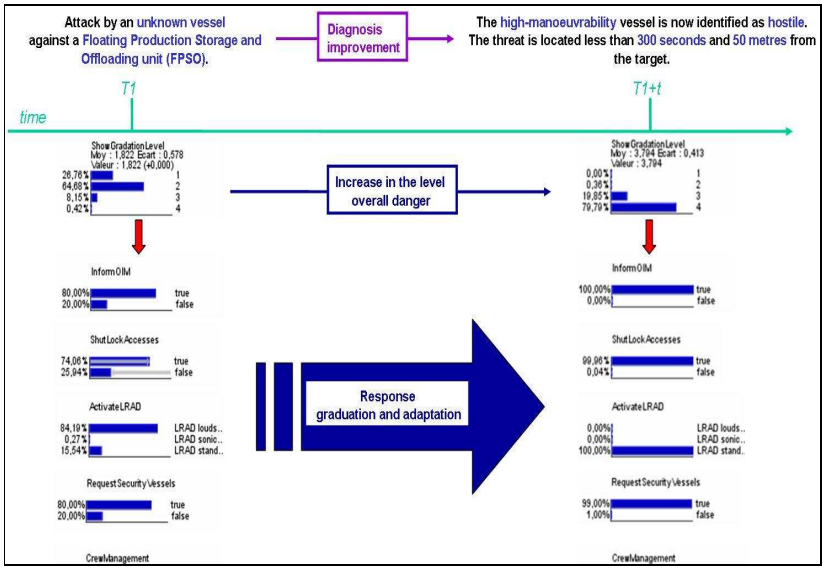

Figure 4: Evolution of response planning as more information about the situation becomes available

At time T1+t the attacker has been identified as hostile and equipped with a highly manoeuvrable boat. The parameters that impacted response planning were: the ranking between the threat and the target (i.e. the time required for the threat to cover the remaining distance to the target), the distance between the threat and the target and the response time of the security vessel. The danger level is now 4 with a 79.79% probability of occurrence. This higher level requires a more forceful response, reflected in the recommended measures: assemble the crew, secure the installation and block access to sensitive areas.

The creation of attack scenarios makes it possible to refine the probability of an attack and test the response of the Bayesian network by changing the parameters that represent the threat, the target, the environment, etc.

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

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 included an alert report as input and a planning report as output. The planning report contains all the counter-measures to be applied either by the crew or automatically by the system.

The alert report module provides an interface for the user to add attack parameters into the network, which remains invisible to the end user. The results of the intermediate calculations generated from the alert report are fed into the Bayesian network created from expert knowledge, via the BayesiaEngine module that provides an application programming interface (API) and a Java library.

The resulting set of counter-measures varies according to the situation. This creates a need to set an activation threshold in order to only activate those measures that provide the most relevant response at a particular time and in a particular situation. It was decided to set this threshold at 70% (i.e. the response planning report would only contain those counter-measures where one of its modalities had a probability greater than 70%). The figure was arrived at by domain experts as it reflects what actually happens in more than two-thirds of actual scenarios.

Once the counter-measures have been selected, they are added to the planning report in a specific order. The main factors determining this order of priority are: the action mode of the counter-measure, its ease of implementation, the degree of automation or the need for a large number of crew to activate it, the time required for it to become effective and its potential additional functions.

The SARGOS system can handle multiple threats contained in a single alert report. The first target to be treated is always the one with the lowest ranking (i.e. the threat will reach it first) as it is most exposed to the threat. The planning report is then divided into two parts: the first concerns communication and the request for assistance broadcast to the entire oil field, and the second concerns the specific target at risk. In both cases, the counter-measures to be activated are displayed in chronological order (Figure 5).

In the example shown in Figure 5 the global counter-measures are, in order: inform the crew master, request the intervention of the security vessel and broadcast information about the attack to other installations in the field. The specific measures are: assemble the crew, block access to the infrastructure, activate searchlights and activate the noise cannon (Long Range Acoustic Device; LRAD). The representation of the probability that a particular measure will be implemented can be seen in the counter-measure ‘Security Vessels’, where the proportion of the blue segment suggests a 60-70% probability that this method will be called upon.

Bouejla A., Chaze X., Guarnieri F. et Napoli A., 2012 :
« Bayesian Networks in the Management of Oil Field Piracy Risk »,
Conférence internationale Risk Analysis 2012 (8th International Conference on Risk Analysis and Hazard Mitigation), Ile de Brac, Croatie,
WIT Transactions on Ecology and the Environment (ISSN: 1746-448X, Digital ISSN 1743-3541), 2012

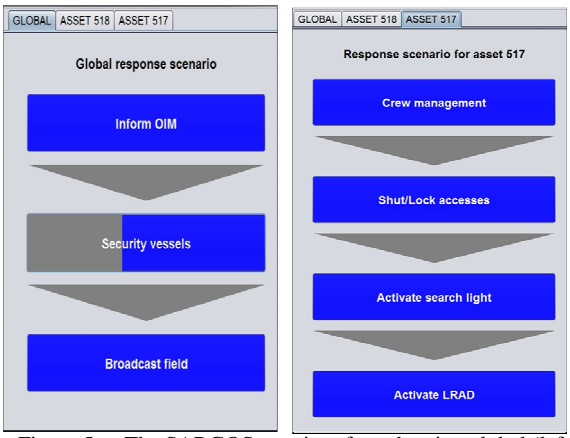

Figure 5: The SARGOS user interface showing global (left-hand side) and specific (right-hand side) countermeasures to be deployed

5 Conclusions

Response planning in the SARGOS system results in the preparation of a response planning report based on an intelligent assessment of the alert report. The response planning report includes all the information necessary for the physical implementation of measures to protect against a threat.

The use of a Bayesian network for response planning is a significant asset for the SARGOS system as the network is able to handle all possible combinations of threat characteristics and the target under attack (e.g. the environment, crew and facility management) and most importantly, it can adapt to changes in the danger level of the situation. The network is also able to integrate feedback from attacks that have already been managed, which means that the planning module can be continuously and iteratively improved.

Finally, in order to improve the modelling of knowledge embedded in the Bayesian network, an interesting approach would be to draw upon an appropriate ontology [13]. The use of a suitable ontology would make it possible to formalise knowledge upstream of the Bayesian network in order to consolidate the steps of threat detection and identification.

6 References

[1] One Earth Future. 2011. *The Economic Cost of Piracy*. Available from http://oneearthfuture.org/images/imagefiles/11%2001%20OBP-Brochure-A4.pdf (Accessed 15 May 2012)

[2] Giraud, M.A., Alhadef, B., Guarnieri, F., Napoli, A., Bottala-Gambetta, M., Chaumartin, D., Philips, M., Morel, M., Imbert, C., Itcia, E., Bonacci, D. and Michel, P. 2011. *SARGOS: Système d'Alerte et Réponse Graduée Off Shore [SARGOS: Graduated Offshore Alert and Response System]*. Paper presented at WISG, 25-26 January 2011, Troyes, France.

[3] Hudson, L. D., Ware, B.S., Mahoney, S.M. and Laskey, K.M. 2002. *An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners*. Available from http://digilib.gmu.edu:8080/jspui/bitstream/1920/268/1/Antiterrorism.pdf (Accessed 11 May 2012).

[4] L'Institut Supérieur d'Economie Maritime. 2010. *Piraterie: perturbation de l'économie maritime ? [Piracy: Disruption to the Maritime Economy?]*. Mer et Marine, October 2010. Available from http://www.meretmarine.com/article.cfm?id=114482 (Accessed 15 May 2012)

[5] Lee, C-J., and Lee, K.J. 2006. *Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal*. Reliability Engineering & System Safety, Vol. 91, No 5, May 2006, pp. 515-532.

[6] Martín, J.E., Rivas, T., Matías, J.M., Taboada, J., and Argüelles, A. 2009. *A Bayesian network analysis of workplace accidents caused by falls from a height*. Safety Science, Vol. 47, No 2, February 2009, pp. 206-214.

[7] Naïm, P., Wuillemin, P.H., Leray, P., Pourret, O. and Becker, A. 2007. *Réseaux bayésiens [Baysian Networks]*. 3rd ed. Eyrolles.

[8] SûretéGlobale.org. 2008. *Apport des réseaux bayésiens dans la prévention de la délinquance [The Contribution of Bayesian Networks to Crime Prevention]*. Available from http://www.sureteglobale.org/pdf/reseaux%20bayesiens.pdf (Accessed 15 May 2012)

[9] Chaze, X., Bouejla, A., Guarnieri, F. and Napoli, A. 2012. *The contribution of Bayesian networks to risk management in oil field piracy*. Paper presented at ITEMS2012, 15 April 2012, Busan, South Korea.

[10] Torti, L., and Wuillemin, P.H. 2009. *Modélisation de réseaux bayésiens de très grandes tailles [Large Scale Bayesian Network Modelling]*. Paper presented at MajecSTIC, 16-18 November 2009, Avignon, France.

[11] Dantu, R., and Kolan, P. 2005. *Risk management using behavior based bayesian networks*. Intelligence and Security Informatics, Vol. 3495, 2005, pp. 115-126.

[12] Kannan, P.R. 2007. *Bayesian networks: Application in safety instrumentation and risk reduction*. ISA Transactions, Vol. 46, No 2, April 2007, pp. 255-259.

[13] Vandecasteele, A., and Napoli, A. 2012. *Spatial Ontologies for Detecting Abnormal Maritime Behaviour*. Paper presented at OCEANS2012, 2012, Yeosu, South Korea.