A Bayesian network to manage risks of maritime piracy against offshore oil fields

Amal Bouejala, Xavier Chaze, Franck Guarnieri, Aldo Napoli

A Bayesian Network to Manage Risks of Maritime Piracy against Offshore Oil Fields

Amal Bouejla[1], Xavier Chaze[2], Franck Guarnieri[3] and Aldo Napoli[4]

MINES ParisTech, CRC

Crisis and Risk Research Centre

1 rue Claude Daunesse

06904 Sophia Antipolis

Abstract

In recent years, pirate attacks against shipping and oil field installations have become more frequent and more serious. This article proposes an innovative solution to the problem of offshore piracy 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, offshore oil fields, pirate attacks, Bayesian networks, quantitative and qualitative knowledge.

Introduction

Currently there are over seven thousand oil platforms scattered throughout the world, each of which requires on the one hand, equipment for the extraction, processing and temporary storage of petroleum, and on the other hand shipping capable of transporting crude oil between production and consumption sites.

Modern piracy is currently the major threat to the security of these energy production sites and maritime crude oil transport. In 2011, 552 attacks on ships and platforms were registered with the International Maritime Bureau[5] compared to 487 reports in 2010. At production sites, monitoring methods are a major weakness in the detection of a threat, and the procedures to be applied in the event of an attack are often inefficient and

[1] amal.bouejla@mines-paristech.fr
[2] xavier.chaze@mines-paristech.fr
[3] franck.guarnieri@mines-paristech.fr
[4] aldo.napoli@mines-paristech.fr
[5] International Chamber of Commerce International Maritime Bureau's Piracy Reporting Centre (http://www.icc-ccs.org)

inappropriate. It is therefore essential to have a system that ensures the security of oil fields and offers them appropriate protection and effective crisis management.

The SARGOS[6] system, funded by the National French Research Agency[7] (*L'Agence Nationale de la Recherche*) and recognised by regional organisations addresses this need by offering a global protection system in the fight against oil infrastructure piracy.

This article is organised into three parts. It first addresses the issue of acts of piracy against oil fields. Next the method used for the planning of counter-measures is described in detail. This includes notably, the construction of Bayesian networks from two datasets: the "Piracy and Armed Robbery" database of the International Maritime Organization (IMO) and the collection and formalisation of the knowledge of domain experts. Finally, the article describes how the model was tested using realistic and comprehensive pirate attack scenarios and the results are discussed.

Piracy against Oil Installations: a Serious Threat and Limited Defences

Offshore oil infrastructure is subject to a constantly increasing risk of piracy. The consequences of these actions have repercussions as much at a local level (on operations) as globally (on distribution). This section highlights both the economic and the political implications of pirate attacks and describes an increasingly insecure context where actors in the offshore oil and gas industry, without effective tools to protect themselves, find themselves helpless. Finally, it presents the SARGOS system and describes the contribution that this new system is expected to make to dealing with the problem of maritime piracy.

Economic and political issues

Offshore oil exploration is expanding rapidly. The exploitation of offshore oil resources currently represents about a third of global petroleum 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. In the offshore waters of politically unstable countries, attacks on oil field infrastructure generate significant additional costs – caused by, for example the payment of ransoms, increased insurance premiums and the installation of security equipment. The annual cost of piracy is estimated at 7-12 billion United States dollars (BMI, 2011). These additional costs directly affect the international price of oil.

Moreover, oil fields form the interface between the maritime world and the oil and gas industry. The heterogeneity of applicable regulation (rather than the absence of law) makes the status of installations a legal headache. Moreover, this complexity can lead to political conflicts between nations; when the nationality of the company operating the platform does not correspond to physical location of the installation, the problem arises of who has responsibility for the protection of the area (Schroeder et al., 2004).

---

[6] The Offshore Warning and Graduated Response System (*Système d'Alerte et de Réponse Graduée OffShore*).

[7] The SARGOS project includes participants from 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).

The importance of oil installations in the global economy and industry and the potential political consequences of piracy therefore require that such assets are better protected.

Violent attacks

Although attacks against oil fields are infrequent and mostly low-profile, they are extremely disturbing because of the severe impact on the crew and infrastructure.

The following examples demonstrate the point:

- On 22nd September, 2010 the tug Bourbon Alexandre located in the Addax oil field off the Nigerian coast was attacked by four speedboats; three French sailors were taken hostage. This was the fourth attack against the Bourbon Company since 2009.
- The attack on the Exxon Mobil platform off the coast of Nigeria, led to the kidnapping of nineteen of its employees and significant damage to the oil facility caused by explosive devices used by the pirates.
- Finally, on 17th November, 2010 pirates aboard a speedboat attacked a ship owned by the French company Perenco that was carrying Cameroonian security forces near an oil platform in the Gulf of Guinea. The attack killed six people.

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. At the same time insurers are unwilling to continue to provide cover for such high risks indefinitely. Finally, nations do not want to continue to see the price of oil affected by such events.

Emerging operational requirements

The attacks described above are a perfect illustration of the weakness of current anti-piracy tools. At the present time, there is no comprehensive system capable of managing the entire threat processing chain. Current systems treat the detection of a threat and the response to it as independent operations. Among the available detection tools, radar-based (pulse) systems[8] can spot large or medium-sized cooperative mobile objects but perform poorly in the detection of small craft (e.g. fishing boats and motor boats) in a rough sea; moreover the analysis of a large domain is relatively slow. There are also optronics surveillance systems[9] that, despite their ability to detect small targets at long-range, are handicapped by the problem of solar reflection from the sea and are very sensitive to weather conditions. As for the tools used to counter an attack, they are often inadequate or incorrectly used (e.g. water jets, Ship Security Alert System).

In terms of the threat response, the targets in danger can currently send alert messages to other units in the area but this diffusion is restricted to a very small geographic area. Moreover, even if a security vessel is alerted to a threat, it cannot be assumed that it will be able to intervene, particularly if it is not close to the location of the attack.

---

[8] In these systems, a radar antenna emits microwave pulses towards the target. These signals are reflected back, and then intercepted by the radar receiver, which collects an electrical signal called the echo.

[9] These electronic and electrical systems generally consist of an optical sensor, an image processing system and a data storage, or display device.

Therefore, the aim of the SARGOS system is to offer a new method that is able to both detect threats and plan a response. The response implements a graduated series of non-lethal counter-measures (sonic cannons, barring infrastructure access, etc.) that can be applied in order to eliminate the danger.

The contribution of the SARGOS system

The SARGOS system addresses the need to protect civilian infrastructure that is vulnerable to acts of piracy or terrorism at sea. It is a global system that takes into account the whole threat processing chain, from the detection of a potential danger to the implementation of the response. It can be integrated into the operations of the installation and takes into account regulatory and legal frameworks at both national and international level. The creation of the system, which involved the development of an overall protection method, automatic threat detection and identification, risk assessment and management of an appropriate response, required professional skills from many domains.

The functional diagram of the SARGOS system (Figure 1) describes the threat processing cycle. The overall system operates as follows: when the detection module instruments (Frequency Modulated Continuous Wave radar, infrared cameras, etc.) identify a vessel in an area near to the oil field, the system evaluates the threat and the potential danger and generates an alert report containing comprehensive data describing the scenario. This information includes details such as visibility, time of day, the speed, longitude and latitude of the detected vessel and its potential target, etc. The distance between the two entities and the theoretical response time of the security vessel is also calculated from this data. If the threat is identified as suspicious or hostile, the system generates an alert report every second. The alert report is used in the planning stage where external and internal means to respond to the attack are mobilised. This paper particularly addresses this aspect of response planning and the management of internal and external resources available on the installation (such as searchlights or sonar alarms).

Figure 1: from the information detected by the FMCW radar, the system identifies the threat and then calculates the ranking and generates an alert report containing all the information necessary to assess the situation in order to use internal and external resources to manage the threat. The ranking is calculated in corresponding to the time required (in seconds) to the threat to go the distance to CPA asset considered taking into account the assumption that at any time the threat may change course and coming in on the target constant radial. The terms are: [ranking <300 s], [300 <ranking <900 s] or [s 900 <ranking <1800 s].

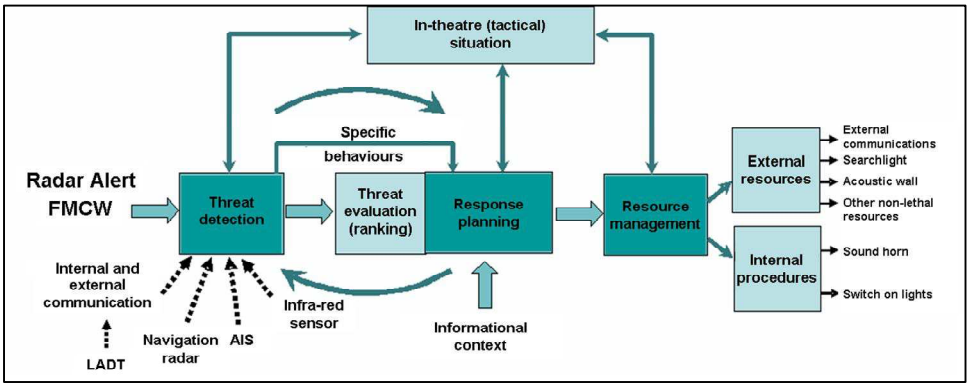

Figure 1. *Functional diagram of the SARGOS system*

Elements of threat analysis and principles for resource management

There are significant obstacles inherent in addressing the problem of maritime piracy. An initial difficulty concerns how to manage the large number of parameters necessary to describe an attack. These parameters, which form the inputs and outputs of the system, characterise the asset in danger (type, criticality, vulnerability, on-board safety tools, etc.), the threat (the type of ship used by the attackers, its speed, their weapons, etc.) and the environment (the time of day, visibility, sea state, etc.). A second problem lies in the fact that these parameters may interact with each other. For example, whether it is relevant to request the intervention of the security vessel will depend not only on the time required for it to reach the asset under attack but also how well armed the attackers are and how fast they are moving. Therefore, the management of the multiple interrelations between system variables presents another major challenge. These first two constraints suggest that the system be based on graph theory, which would make it possible to translate and exploit, using a graph, the large number of variables, their interdependencies and interrelationships, etc.

However, an additional concern is uncertainty in the information describing the threat. The SARGOS system generates an alert report that contains on the one hand, data issuing from various detection instruments (type of ship detected, number of crew, potential weapons, etc.) and on the other hand, mathematical calculations based on dynamic variables (the distance between the target and its attackers, time available before the attackers are able to board the asset, etc.). Despite the improving performance of radars, this data is known to be unreliable. This situation is only made worse as the distance between the target and the threat increases, or if the sea state deteriorates, etc. This uncertainty is a constraint that emphasises the need to use a system based on probability theory and probabilistic calculations.

With these constraints in mind, a solution based on Bayesian networks was explored (Leray and al., 2008). A Bayesian network is a system for the representation of knowledge and the calculation of conditional probabilities (Naim and al., 2007). The tool is based on Thomas Bayes' theorem, which is one of the foundations of probability theory (Nielsen and al., 2009). Widely used in medical and industrial diagnosis (Lee, 2006), Bayesian networks make it possible to capitalise on, and exploit knowledge and are particularly suitable when uncertainty must be taken into account (Hudson, 2002), (Martín, 2009).

The aim was to automate the preparation of response plans that are tailored to the nature of the detected intrusion and can provide an appropriate, graduated and progressive response to a threat. Information concerning attacks on shipping and petroleum installations was gathered from a specialist database, and experts in the maritime domain who offered their knowledge and expertise. The data from each of these two sources was modelled with Bayesian networks. The network was built using

BayesiaLab[10] software; this powerful network modelling tool provides an intuitive graphical interface.

Recently, Bayesian networks are used in risk assessment because the model can perform forward or predictive analyses as well as backward or diagnostic analyses. Some methodologies have been proposed to structure Bayesian networks and perform risk assessment.

Several authors have already used Bayesian networks in order to solve problems in offshore. Among these authors, (Baoping and al., 2012) who modeled a Bayesian network for the quantitative evaluation of the preventive operation underwater eruption wells. The choice of using Bayesian networks has been done because they are models to perform predictive analytics and diagnostics systems. Another application described in the article of (Eleye-Datubo and al., 2008) is the use of a Bayesian network to provide an intuitive and vital representation that mimics the real world. The integration of the human element in a model based on probabilistic risk requires integrated appropriate technical and essential contributions of the linguistic nature. For this reason, the author proposed a Fuzzy Bayesian network as fuzzy logic is an excellent tool for such integration and Bayesian networks can make a probabilistic framework and cross the boundaries of possibility theory. The implementation of this method was demonstrated in a study of human performance at sea.

Khakzad and al. (2013) looked at preventing the risk of blowouts during drilling operations. The authors demonstrate the application of both the "bow-tie" and Bayesian network methods. In the first method, fault trees and an event tree are developed for potential accident scenarios. In the second method, individual Bayesian networks are created for accident scenarios and an object-oriented Bayesian network is constructed by connecting the individual networks. The dynamic Bayesian network method is a better approach than the "bow-tie" model because it can take into account common cause failures and conditional dependencies along with performing probability updates and sequential learning based on accident precursors.

Ren et al. (2007) also addressed the contribution of Bayesian networks when taking into account human factors. The authors designed and developed a methodology based on the "Swiss cheese" model developed by James Reason (Reason, 1990). Reason's model provides a generic framework for risk assessment linked to human factors. Five levels are used to characterize latent failures within the causal chain of events: root causes, trigger events, incidents, accidents and consequences. The detailed characterization of each level made it possible to build the Bayesian network. A range of events was specified, and the prior and conditional probabilities of the model were assigned based on the inherent characteristics of each event.

Trucco and al. (2008) presented an approach to integrate human and organizational factors into risk analysis. This approach has been developed and applied to a case study in the maritime industry, but it can be also be utilized in others sectors. A Bayesian Belief Network has been developed to model the maritime transport system, by taking into account its different actors ship-owner, shipyard, port and regulator and their mutual influences.

Vinnem and al. (2012) addressed the issue of hydrocarbon releases at sea during the exploitation or maintenance phases of a platform. A generic model, based on risk

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

influencing human factors was developed and adapted to specific failure scenarios. The authors describe a full Bayesian network model and two implementations are outlined. The probability of human error, importance measurement of consequences and common causes and interactions are analysed. The authors demonstrate that the model is able to reflect human and organizational factors and safety culture.

These references highlight the wealth of work that has been carried out into both the assessment of technical risks and human and organizational factors in order to prevent the threats that face platforms at sea.

Coupling of quantitative and qualitative knowledge for the construction of a Bayesian network for response planning

The creation of the Bayesian network used for response planning relied on the coupling of quantitative information from the IMO's "Piracy and Armed Robbery" database and qualitative knowledge offered by experts in the maritime domain. Development was divided into two stages. The first step was to construct a Bayesian network from database records of attacks against shipping and oil installations across the globe, while the second step was to exploit the knowledge of experts in order to refine the results and to add counter-measures.

Construction of a Bayesian network from quantitative data

This first step involved the extraction of data from the IMO's "Piracy and Armed Robbery" database. This is the only database currently in existence that contains historic data (dating from 1994) of pirate attacks at sea. On 15th July, 2011 the database contained records of 5,502 attacks and provided detailed information on 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.

In the table below are listed some examples of recent attacks and armed robberies.

Date	Ship name	Ship type	Incident details
2012-12-23	ASSO VENTUNO	Supply ship	Pirates armed with guns attacked and boarded the offshore supply ship underway and kidnapped four crew members. The ship sailed to a safe port after the incident. The other crew members did not sustain any injuries.
2012-12-29	SANKO MERCURY	Bulk carrier	Robbers boarded the anchored ship while waiting to commence loading operations. They broke into the forward bosun store, stole the ship's stores and property and escaped unnoticed. The incident occurred between 29.12.2012, 2300 LT and 30.12.2012, 0400 LT and was reported to the local agent and the port authorities.
2012-12-29	NORD DISCOVERY	Bulk carrier	Duty crew onboard the anchored bulk carrier found that the lock of the forward store had been broken. After checking, he saw the ship's stores lying on the

			deck and the robbers escaping in their two boats empty-handed.

Table 1. *Examples of recent attacks and armed robberies*

To classify this information, we applied a method of textmining to the database using the software RapidMiner[11].

The BayesiaLab software made it possible to automatically generate a bayesian network and describe the interdependencies between the principal basic elements. Among the unsupervised learning methods available (data segmentation algorithms or characterisation of the target node for examples), an algorithm for finding associations was chosen as it offered the most appropriate modelling.

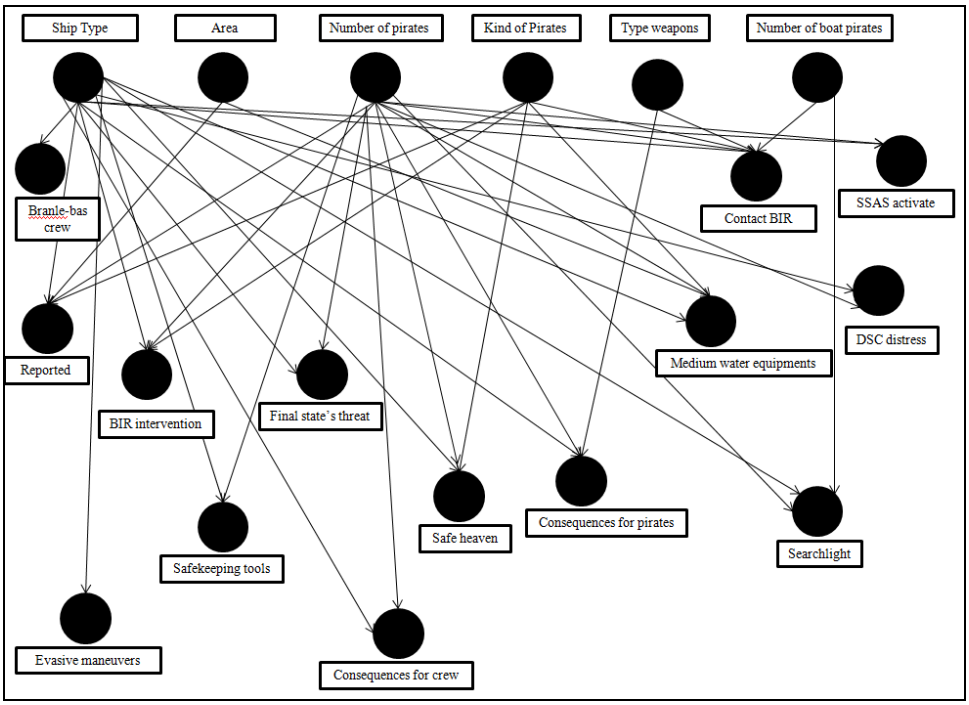

Figure 2. *The Bayesian network based on IMO data*

The Bayesian network constructed from data related to attacks held in the International Maritime Organization's database lacks many values related to the modalities of the different nodes because of a lack of detail in the description of pirate attacks. BayesiaLab makes it possible to impute missing values by adding a state to the variable. Moreover, the k-means algorithm applied to the data made it possible to

[11] RapidMiner is unquestionably the world-leading open-source system for data mining. It is available as a stand-alone application for data analysis and as a data mining engine for the integration into own products

estimate the independence relations between database variables and thus to obtain the best "cause and effect" structure. For each attack scenario, the network performs a statistical calculation by applying the parameters given as input to simulations of similar cases. The large amount of missing data in the database therefore does not impact any of the parameters for the simulation of attack scenarios.

Figure 2 shows the Bayesian network constructed from the information contained in the IMO 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. The network contained around twenty nodes that described the type of vessel under attack, the location of the attack, the type of weapons used by the pirates, their numbers, etc. The interrelationships between these variables were also identified through a machine learning process.

A classical statistical analysis of this data provided some initial findings, which included the observation that most ships coming 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 pirates). The network therefore provides a very clear view of the tactics of pirates, the weapons they use, and above all the number of individuals involved.

In the example below, specific modalities were set for nodes that characterise the threat in order to identify the counter-measures used by the crew of the asset under attack. Figure 3 illustrates the following assumptions:

- The asset under attack: a tanker
- The location of the accident: international waters
- The type of attackers: thieves
- Type of weapons: armed personnel

The Bayesian network indicates that in this case (as in most cases) the assailants fired shots at the potential target and that the crew, to protect themselves from the threat, tried to apply evasive manoeuvres and aimed water hoses at the attackers.

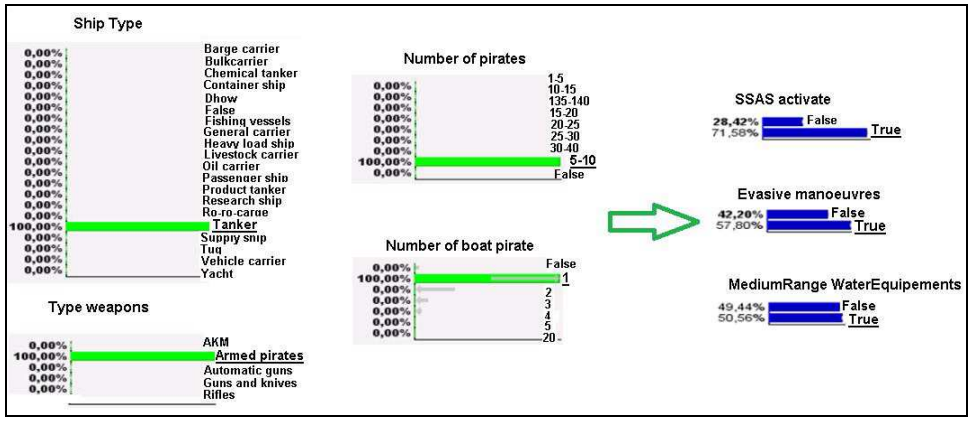

Figure 3. *Hypothetical attack against a tanker*

The network created from the IMO database therefore helped to define the principal steps taken by the crew of attacked entities in order to protect themselves, namely: initiate evasive manoeuvres, activate the Ship Security Alarm System (SSAS), contact the security vessel, secure the crew, turn on searchlights, etc. It also made it possible to assess the effectiveness of these tools and to define the probability of occurrence of certain types of attacks.

It is necessary to carry out an initial analysis of the IMO database to establish the challenges posed by these threats to the crew, the platform, the economy and national security. It makes it possible, in a second step, to identify the frequency of attacks, risk zones, types of ships used to carry out attacks, etc. and to list the most commonly used and effective counter-measures.

Coupling the Bayesian network based on IMO data with the qualitative knowledge of marine experts

The Bayesian network created from the modalities and conditional probabilities found in the IMO database provided an initial formal framework. Domain experts were then able to enrich this initial network by integrating their knowledge and expertise in order to create the final SARGOS network (Hudson, 2002).

The second step of the approach was for experts in the maritime and petroleum industries to analyse the information provided by the Bayesian network that had been constructed from the IMO data. As the information contained in the IMO database related primarily to attacks on shipping, experts were able to contribute their knowledge of attacks on oil fields in order to extend the results: nodes and arcs were added to the model in order to make it as versatile as possible. Consequently, the Bayesian network was able to model both main target categories (shipping and fixed installations). While the inputs to the network (type of vessel used by the attackers, its movements, etc.) are identical regardless of the nature of the target, the counter-measures recommended by the Bayesian network are tailored to the type of target under attack (for example, evasive manoeuvres are not proposed when a fixed installation is the subject of the attack).

The design of this enhanced Bayesian network, adapted to the constraints and conditions associated with fixed installations came about as a result of many brainstorming sessions during which various maritime security experts shared their experiences and discussed the modalities and probabilities of the network.

The combination of information from the IMO database and the knowledge and experience of experts in marine and offshore safety made it possible to create the SARGOS response planning network, which consisted of four modules and five sub-modules (Figure 4).

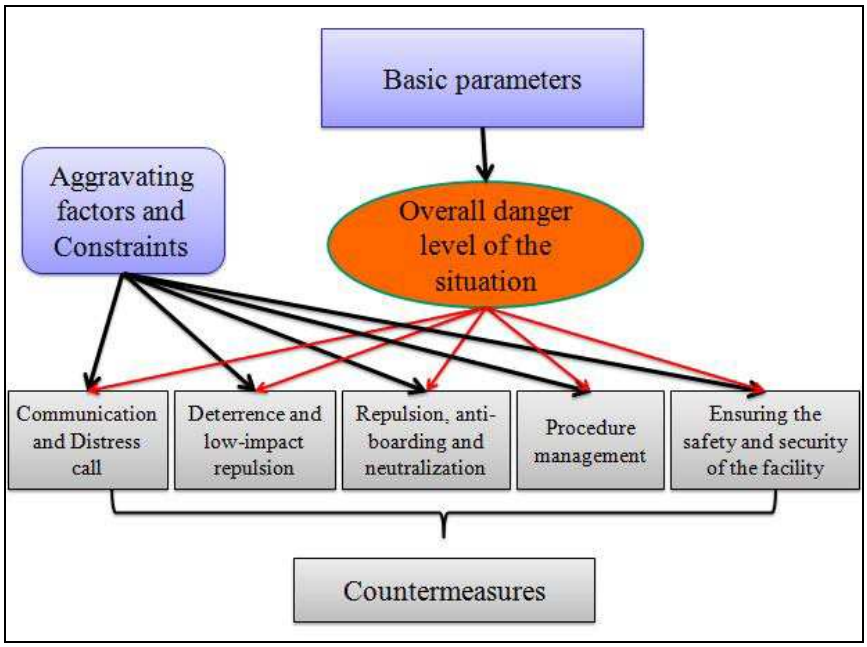

Figure 4. *Structure of the SARGOS Bayesian Network*

In the SARGOS Bayesian network, each module or sub-module consists of one or more nodes that receive input from and/or output to other nodes. Each node is a matrix of conditional probabilities that are calculated from an assessment of the interactions between nodes and the reality represented by the node itself. For example, the probability distribution of the node to activate searchlights ('ActivateSearchlight') is the direct result of interactions with other nodes that describe visibility, time of day and technical constraints such as availability and remote control. The probabilities of the basic nodes are initially standardised as no specific attack characteristics are set.

The definition of the scope of each module is directly related to the composition of its constituent nodes. The module classification included: 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.

Basic parameters

The basic parameters module comprises static or dynamic physical data that characterise the threat and the target. These data are the direct result of, or are derived from the intermediate calculations of the alert report. Basic parameters represent the minimum, but sufficiently detailed level of modelling required for a full understanding of the threat and the target when assessing potential responses to an attack. They include, for example, threat identification (the node 'IdentityClass' which has two values: suspicious or hostile), the distance between the threat and the target (the node 'DTGThreat/Asset'), and the criticality of the target (the node 'AssetAssessment' that takes four values: critical, major, significant or otherwise).

In the Bayesian network, we take into account the longitude and latitude of the pirate ship for the calculation of the kinematics of the vessel to determine the distance between

the graft vessel and the platform. These two variables are passed in the alert report but not included in the network nodes.

The overall level of danger of the situation

The overall danger level of the situation is arrived from the basic parameters. The node 'ShowGradationLevel' is used to formalise this module in the Bayesian network. 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.

Aggravating factors and constraints

The aggravating factors and constraints module consists of 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. The nodes in this module represent the environment, for example visibility (the node 'Visibility') and time of day ('PeriodOfDay'). Constraints are represented by parameters which reflect the effectiveness of the response both technically and operationally. Technical constraints are directly related to the use of counter-measures, and include nodes that represent their availability ('ImmediateReadiness') or the potential for remote control ('RemoteControlled').

Counter-measures

Counter-measures include all defences that are mobilised by a target under attack in order to protect itself against an identified threat. They are the concrete 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, which reflect the concept of a graduated response through increasingly forceful measures that correspond to the nature of the detected threat. Measures range from communication and a request for assistance, through deterrence and small-scale repulsion, repulsion, anti-boarding measures and neutralisation, to procedure management and securing the facility. They are described in detail below.

Communication and the request for assistance are two key responses to a threat. Internal communication can be used to alert all relevant personnel on the target (e.g., the node 'InformOIM' which represents informing the crew master), while external communication makes it possible at various levels to alert the different actors involved in maritime security – for example to request the intervention of the security vessel (represented by the node 'RequestSecurityVessel') or to activate the Ship Security Alarm System (represented by the node 'RaiseSSAS') etc. Both of these types of communication enable fixed installations and shipping to prepare their response plan and to establish if external intervention is available.

From the position of the ship security (BIR), the system calculates the time required for the intervention on the location of the threat. If the estimated response time is greater than 300 seconds, the ship security may be required, in which case a request must be sent.

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. These measures include the ability of the target to repel an attack with low-impact devices such as searchlights, fire hoses or sonic cannons (Long Range Acoustic Devices), represented by the node 'ActivateLRAD'.

Repulsion, anti-boarding and neutralisation are high-impact counter-measures whose main function is at least to mitigate an attack, if not neutralise the attackers. The node 'EngageRepellentEquipment' represents a growing number of tools available on the anti-piracy market that are designed for the repulsion of an assault at long-range (while remaining within the bounds of legitimate, non-lethal defence). Like repulsion equipment, the main function of anti-boarding tools is to prevent attackers from gaining access to the facility or vessel. The function of the 'SetCrowdControlMunition' node is to delay the progress of the attackers in order to exhaust or even neutralise them and thereby provide the crew with maximum time to mobilise other safety measures.

Procedure management is composed of two counter-measures. On the one hand, the node 'CrewManagement' represents the sounding of crew Action Stations and the reporting of crew to their pre-assigned post or station. On the other hand, the 'AssetAssaultManagement' node represents activities related to securing the target of the attack. The modalities of this node are: activate the Citadel, engage evasive manoeuvres (for mobile units and shipping), and declare the security post (a set of individual procedures to be applied by each crew member as necessary). Like procedure management, the SARGOS system offers a way to secure the installation through the planning of actions designed to safely stop production and prevent access to sensitive areas.

Demonstration of the contribution of the Bayesian network and discussion

Once the probability distribution of the various modalities has been established, an interesting exercise is to test the Bayesian network by using it to simulate different 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.

The integrated data that provides the input to the network is interpreted from images captured by cameras and various sensors. The uncertainty of this information increases with the distance between the target to be protected and the pirate ship. In its current form, the Bayesian network cannot handle the temporal evolution of the attack and there is no connection between response reports generated for the same attack. This issue is addressed in other research based on dynamic Bayesian networks (Dabrowski and al, 2013).

Attack scenarios

The example below (Figure 5) shows the results of setting parameters to simulate an attack on a Floating Production, Storage and Offloading (FPSO) unit by an unknown vessel. In this example the danger level of the situation is 2 with a 64.68% probability of occurrence and the counter-measures to be applied are: inform the crew master; request the intervention of the security vessel; broadcast a strong, clear message by loudspeaker; activate the searchlight; activate the security post; and engage repulsion equipment. Figure 5 shows that the planning of the response corresponds to the danger level of the situation and is able to adapt to changes in parameters representing the threat and the target. Setting parameters to represent the threat, the target, the environment, etc. creates

different attack scenarios that make it possible to refine the probability of an attack and test the response of the Bayesian network.

In this case it is necessary to inform the master of the crew of the FPSO, request the intervention of ship safety and security since the probability of their action is equal to 80% (close to the ship attacked infrastructure). Several counter-measures can be activated as the speakers, bright lights and water jets. Following the evolution of the situation a few moments later and the increased level of danger that follows, it should then alert the crew to use the security station.

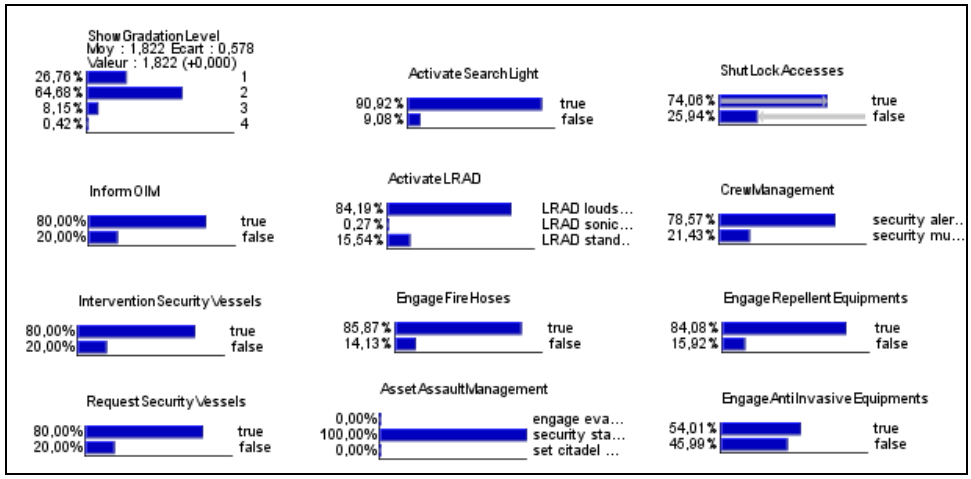

Figure 5. *Result of response planning using the scenario of an attack from an unknown vessel*

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 (which listed all the counter-measures to be applied either by the crew or automatically by the system) as output. The BayesiaEngine software provides a module that makes it possible to select and set attack parameters. This module consists of an application programming interface (API) and a Java library. Intermediate calculations are carried out on the basis of these parameters and the results are fed into the enhanced Bayesian network created from expert knowledge.

The resulting list of counter-measures varies according to the attack scenario. Consequently, a threshold must be set in order to only activate those measures that provide the most relevant response at a particular time, and in a particular situation. This threshold was set at 70%. In other words, only those counter-measures where one of the modalities had a probability greater than 70% were selected for further processing. This threshold was arrived at by domain experts as it reflects actual events in more than two-thirds of real-life cases. Following an extensive period of testing, the selected counter-measures were found to correspond to realistic and reliable responses.

Once the counter-measures had been selected, they were added to the planning report in a specific order. The main factors determining this order of priority were: the action mode of the counter-measure, its ease of implementation, the degree of automation or the

need for a large number of crew members 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. Consequently, priorities must be established. In the system, the first threat to be treated is always the one where time available to react is the shortest for the target that is most exposed.

The system detected several potential threats heading towards the oil field and has classed them into 'Enemy', 'Unknown' or 'Friend'. An alert is only generated following a classification of Enemy or Unknown. Once a threat has been detected and analysed, the response planning report is prepared. It is divided into two parts: the first concerns communication and a general request for assistance directed at the entire oil field; the second concerns the specific asset at risk. The response planning report also displays the counter-measures to be activated in chronological order (Figure 6).

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.

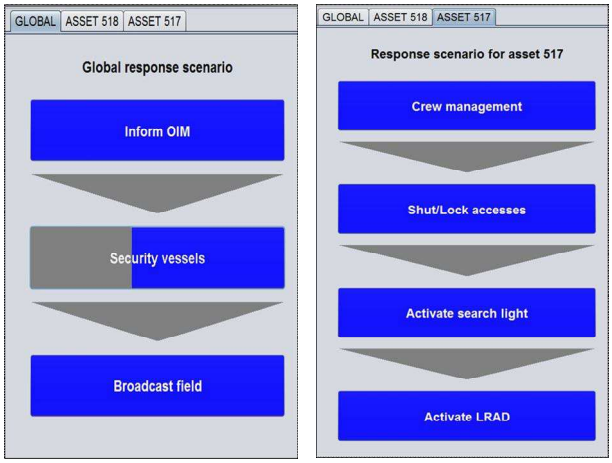

Figure 6. *The user interface of the SARGOS system showing global counter-measures on the left (in order: inform the crew master, request the intervention of the security vessel and inform other installations in the field) and specific counter-measures on the right (assemble crew, block access to infrastructure, activate searchlights and activate the sonar cannon).*

Conclusion

Acts of maritime piracy against oil field infrastructure present a complex problem. The effectiveness of current measures designed to protect infrastructure is significantly affected by the vast terrain and environmental constraints. Moreover, it is difficult to assess a potential threat given the constantly changing nature of a dangerous situation and the huge number of parameters that must be managed.

The implementation of a Bayesian network therefore offers a significant advantage for the SARGOS system as this type of network is able to handle all possible combinations of parameters. These include not only the characteristics of the threat and the target under attack, but also the environment and variables related to crew and facility management. Most importantly, the system is able to adapt in real-time to changes in the danger level of the situation. The SARGOS system offers a response planning solution that manifests in the preparation of a planning report created from an intelligent assessment of successive alert reports, and which can react to an evolving situation.

The activation threshold of counter-measures has been determined by experts. Most counter-measures are against-enabled manually by the crew. Some of them are not systematically exploited if their activation requires setting a crew danger. The Bayesian network was developed specifically for the protection of static targets (platforms) and is therefore not suitable for ensuring the safety of ships.

The network can be continuously improved through the integration of feedback from attacks that have already been managed. It is therefore possible to continue to enhance and tailor the planning module iteratively.

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

The use of dynamic Bayesian networks is a way to explore. These networks have been an interesting development as a generalization of models hidden Markov models or Kalman filters for applications such as speech recognition, state estimation of a dynamic system, etc. A dynamic Bayesian network is a factored representation of a Bayesian network whose nodes are indexed by time on a discrete scale. The Bayesian network is represented by nodes and indexed by generic no time and two types of links: links classical Bayesian networks and so-called temporal relationships that define the conditional probability tables of the nodes according to their parents located to lower time indices. The application of a dynamic Bayesian network would integrate the notion of time on decisions to be taken in case of attack and its influence on the evolution of the threat.

References

Baoping C, Yonghong L, Zengkai L, Xiaojie T, Yanzhen Z and Renjie J. 2012. *Application of BayesianNetworks in Quantitative Risk Assessment of Subsea Blowout Preventer Operations,* Society for Risk Analysis, 2012, p 1-20.

BMI. 2011. *Study: Piracy Costs World Up to $12 Billion Annually,* Bureau International Maritime, 14 juillet 2011. http://www.voanews.com/english/news/africa/Study-Piracy-Costs-World-up-to-12-Billion-Annually-113609239.html.

Dabrowski J.J., Pieter de Villiers J., Maritime piracy situation modelling with dynamic Bayesian networks, Information fusion, 2013.

Eleye-Datubo A.G, Wall A and Wang J. 2008. *Marine and offshore Safety Assessment by Incorporative Risk Modelling in a Fuzzy-Bayesian Network of an Induced Mass Assignment Paradigm,* Society for Risk Analysis, 2008, p 95-112.

Hudson, Linwood D, Bryan S Ware, Suzanne M Mahoney, and Kathryn Blackmond Laskey. 2002. *An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners,* August 2002, 8p.

Khakzad N, Khan F, Amyotte P. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science; 57 (2013): 108-117.

Lee, Chang-Ju, and Kun Jai Lee. 2006. *Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal,* Reliability Engineering and System Safety, volume 91, n°5, May 2006, p 515-532.

Leray, P., Meganck, S., Maes, S., and Manderick, B. (2008). Causal graphical models with latent variables : learning and inference. In Holmes, D. E. and Jain, L., editors, Innovations in Bayesian Networks: Theory and Applications, Studies in Computational Intelligence, vol.156/2008, pp.219-249. Germany, Springer.

Martín, J.E., T. Rivas, J.M. Matías, J. Taboada, and A. Argüelles. 2009. *A Bayesian network analysis of workplace accidents caused by falls from a height,* Safety Science, volume 47, n°2, février 2009, p 206-214.

Naïm, P., Wuillemin, P.-H., Leray, P., Pourret, O., and Becker, A. (2007). Réseaux bayésiens. Eyrolles, Paris, 3 edition.

Nielsen T.D., Finn V.J. 2009. Bayesian networks and decision graphs, Springer, 2009, 463p.

Reason J. 1990. *Human Error,* Cambridge University Press, 1990, 320p.

Ren J, Jenkinson I, Wang J, Xu DL, Yang JB. A methodology to model causal relationships on offshore safety assessment focusing on human and organizational factors. Journal of Safety Research 39 (2008) 87-100.

Schroeder, D.M., and Love, M.S. 2004. *Ecological and political issues surrounding decommissioning of offshore oil facilities in the Southern California Bight,* Ocean and Coastel Management, volume 47, 2004, p 21-48.

Trucco P, Cagno E., Ruggeri F and Grande O. 2008. *A Bayesian Belief Network modelling of organisational factors in risk analysis : A case study in maritime transportation,* Reliability Engineering and System Safety, 2008, p 823-834.

Vinnem JE , Bye R, Gran BA, Kongsvik T, Nyheim OM, Okstad EH, Seljelid J, Vatn J. Risk modeling of maintenance work on major process equipment on offshore petroleum installations. Journal of Loss Prevention in the Process Industries 25 (2012), 274-292.