AN INNOVATIVE METHODOLOGY FOR MARITIME SECURITY RISK MANAGEMENT TO DESIGN COST-EFFECTIVE DEFENCE SYSTEMS

Francesca MATARESE[1], José FONSECA[2], Patrizia MONTEFUSCO[3]

[1]SESM Scarl, Giugliano in Campania - Napoli, Italy, fmatarese@sesm.it

[2]University of Coimbra/Polytechnic Institute of Guarda, Portugal, josefonseca@ipg.pt

[3]SESM Scarl, Giugliano in Campania - Napoli, Italy, pmontefusco@sesm.it

ABSTRACT

After 9/11 terrorist attacks, critical assets protection has become a priority all over the world. The focus moved from "safety" to "security": from the prevention and mitigation of casual and unexpected events to the mitigation of deliberate acts. Regarding the protection of particular critical assets as vessels and ports or aircrafts and airports, respectively International Maritime Organisation (IMO) and International Civil Aviation Organization (ICAO) developed two different methodologies for security management, both taking into account that "total security" would be attainable only with an infinite cost. IMO, through the International Ship and Port Facility Security (ISPS) Code (ref. to IMO, 2002), has stated that countermeasures have to be identified and implemented in a scalable way, according to the "security level". Nevertheless, "security level" is the result of intelligence information, whose trustworthiness is in inverse relation to malicious people's capability to act by surprise, which undoubtedly increases the success of their actions. Therefore, security risk assessment and consequent countermeasures should set aside intelligence information and base their cost-effectiveness on other considerations. This paper aims at proposing an innovative methodology for security risk management that allows the identification of cost-effective countermeasures, based on the evaluation of the impact of each potential incident, independently from the "security level". To meet this objective we will benefit of past experiences in airport security, where different strategies are suggested by ICAO.

1. INTRODUCTION

The attack of September 11 in 2011 and it is subsequent series that targeted the Madrid commuter trains in 2004 and the London public transport system in 2005 foster an increasing concern about the security of critical infrastructures such as ports and its surrounding facilities. Indeed, ports cover a pivotal role in the supply chain in Europe with about 90% of EU's external trade and 40% of internal trade transported by sea, corresponding to 3.5 billion tonnes of freight loaded and unloaded in EU ports each year (ref. to EC, 2006). This complex sea based trade system is vulnerable to several attacks like piracy, terrorism, illegal drug trafficking, human and weapons smuggling (ref. to Bakir, 2007). Port security has been addressed with several directives and regulations, among them the International Ship and Port Facility Security (ISPS) Code, the (EC) No 725/2004 and the ISO20858:2007. They mainly recommend security measures and activities related to risk assessment in a prescriptive way. Presently, the ISPS Code, one of the main references for threat and risk assessment in the maritime domain, offers little help in identifying and prioritising threats according to time and budget constraints (ref. to Farrow and Shapiro, 2009).

Despite the global nature of different sectors as Air Traffic Management (ATM) and Vessel Traffic Management (VTM), risk assessment is interpreted and implemented differently in the European states, thus resulting in a variety, sometimes conflicting, set of security measures (ref. to Pallis and Vaggelas, 2007).

Maritime and more specifically port security is concerned with securing the assets (including services), to prevent threats and limit their effects on the overall maritime system. This effect limitation could be achieved by preventing the creation of the vulnerability, removing the vulnerability from the system and/or increasing the tolerance in case of component failures due to attacks (ref. to Avizienis et al, 2004).

The increasing complexity of systems that support navigation and surveillance in ports, due to the pervasiveness of emerging technologies and growing number of vessels entering European ports, create the conditions for the rise of unpredicted threats that may potentially turn into dramatic events. This is also driven by the on-going update of legacy systems with new technologies and their connection to innovative systems, which creates a new environment with new threat vectors, for which these systems were not prepared when they were designed. Thereby, given that VTM systems (VTMSs) play a critical role in supporting the maritime safety, the security risk assessment of VTMS should be a major concern and a top priority (ref. to Helmick, 2008).

This paper proposes a generic methodology for security risk management based on the evaluation of the impact of each potential incident to the VTMS. It benefit of past experiences using ICAO strategies in airport security and allows the identification of cost-effective countermeasures independently from the "security level". It consists in a cascade of five stages: assets identification, threat analysis, vulnerability assessment, risk analysis and countermeasure identification/risk treatment. The security risk assessment methodology proposed in this paper can be seen as generic, as it is not bound to any technological or implementation constraints, so it can be applied to most VTMSs. In fact it is based on an abstract model defining assets, threats and vulnerabilities related to any VTMS.

It addresses the following objectives:

- To be adopted either by state-of-the-art systems as well as legacy systems allowing the assessment of the new risks that their interconnection may (and will) introduce.
- To be based on existing and well established safety standards already in use by the industry, including the ICAO, IMO, CC, the ISO 270xx, etc. and extend them to cover the VTMS security scenario. For example, although widely adopted, the CC does not provide the procedures that should be used to assess the security of the system, whereas the risk assessment methodology that we present addresses this aspect.

2. SECURITY ASSESSMENT METHODOLOGY

The proposed methodology is based on what is currently being done by the industry and it comprises five main stages that should be revisited during the development and periodically, after the deployment of the VTMS. The methodology is the synthesis of ICAO/IMO security guidelines (ref. to IMO (2002) and ICAO (2002)) and of Microsoft Threat Modelling (ref. to Swiderski, 2004) for the software related threats:

1. **Assets identification**. The system is formally decomposed using Use Cases or Data Flow Diagrams (DFD) to obtain the list of assets and their interconnections. The technique used is complemented with information about trust (or privilege) boundaries between entities.
2. **Threat analysis**. This stage involves determining the possible threats to each asset identified in the previous stage. The following groups of security attributes are used to obtain and classify the threats: the widely accepted set consisting of Confidentiality, Integrity and Availability, or a more detailed view consisting of Authentication, Integrity, Non-repudiation, Confidentiality, Availability and Authorization. It is also in this stage where the Fault Tree model of the threats of each asset is built.
3. **Vulnerability assessment**. Vulnerabilities, which are closely related to the threats, also drive the respective countermeasures, which will be implemented in the last stage, according to the risk analysis outcome.
4. **Risk analysis**. This allows prioritizing the threat mitigation by directing the resources to the most critical threats first. Risk is a measure of the threat impacts to the system vs.

the probability of that threat to occur. Several schemes to obtain the likelihood of the occurrence of the threat may be used.

5. **Countermeasure identification/risk treatment**. This provides mitigation procedures that need to be executed in order to eliminate threats or limit their effects to an acceptable residual level. They are closely related to the specific threat they apply to and to the target vulnerabilities. The set of countermeasures/security controls are the most important output from this security assessment methodology as they can be seen as the recommendations or the security requirements for the system under assessment.

2.1 Assets identification

An asset is something of value to the Organisation. In general, technological assets combine logical and physical assets and can be grouped into the following categories (ref. to Whitman and Mattord, 2012):

- **Information.** Documented (paper or electronic) data or intellectual property used to meet the mission of an Organisation. It is often the most valuable asset of the Organisation.0
- **Software.** Software applications and services (such as operating systems, database applications, networking software, office applications, custom applications, etc.) that process, store, or transmit information.
- **Hardware.** Physical devices needed for the proper functioning of the Organisation (such as workstations, servers, etc.). This asset normally focus solely on the replacement costs for physical devices.
- **People.** The people in an Organisation that possess unique skills, knowledge, and experience and that are difficult to replace.
- **Procedures.** Documents with instructions detailing how to accomplish a specific task. They should be available in a need-to-know basis.

2.2 Threat analysis

A VTMS consists of a set of hardware, software and communication assets, operated by several users with different operation statuses. Threat assessment and risk management together form the basis of a viable and cost effective security response to threats that could target VTMS. One of the most difficult tasks for security professionals is devising an effective security plan that correlates to the threat. Accurately identifying the threat or threats must be the first step in the process. Our challenge is to perform a quantitative analytical approach will be used to perform threat assessment.

In devising a threat assessment methodology to evaluate the threats affecting the VTMS, it is preferable to use a systematic and quantifiable approach. Therefore, the threat assessment proposed uses a quantitative analytical approach. The structure of this methodology employs three core principles of security: *identify*, *implement* and *sustain* (ref. to ICAO, 2002).

In undertaking the task of assessing the threats, there are several sources of empirical evidence and statistical data available in the fields of intelligence and security from which to form an analysis of past trends of acts of unlawful interference. In order to provide decision-makers with a current and credible threat assessment, however, multiple sources of information should be explored. Threat and vulnerability criteria have to be determined before conducting the assessment by deciding on *focal points/hot spots*. Focal points can be defined as those factors or criteria that are estimated to have the most weight or value in a given process.

This methodology utilises two facets of analysis that together form a credible means of assessing the threat and determining a security response through application of risk management measures.

First, it must be understood that a *deliberate* act of unlawful interference must, by definition, be premeditated and carried out with *purpose* by the perpetrators. This means that someone has a reason to conduct an unlawful act and thus proceeds to plan and execute the act. Therefore, before assessing how an act of unlawful interference may be carried out against a target, the

analyst should first consider the reasons why an unlawful act would be committed and the probability of its being committed.

The next step would be to create a working tool to assist in the assessment process: the *Vulnerability Matrix*. The Vulnerability Matrix forms the final analysis for a follow-on risk management process. It covers security threat categories, which can be adapted to assess the threat directed at a potential target or to evaluate the security posture of a part of the system.

Security professionals have long recognized that implementing increased preventive measures commensurate with a higher level of threat has an associated expense that may become a heavy financial burden on the resources of an Organisation. It is therefore considered more effective to deploy defences where and when they are most needed rather than applying them universally. This concept is called risk management.

Standards consist of a minimum set of security control measures that are expected to be applied equally at international level regardless of the threat environment impacting on operations. While these arrangements were established to ensure minimum uniform baselines, no specific standards exist to address variable threat conditions. Whenever an Organisation introduces additional security measures to meet a higher threat level, it may find that implementation is difficult to sustain, especially when the extra measures have not been tailored to the specific threat. Therefore, once an Organisation has properly assessed the nature and level of threat within its own territory, it can then apply appropriate enhanced measures. Organisations can profit of a risk management approach whereby enhanced measures are implemented either to prevent an unlawful act from being committed or, at a minimum, to discover the vulnerabilities that can be exploited or to mitigate any consequences resulting from an unlawful act.

2.3 Vulnerability assessment

A vulnerability assessment is a systematic, point-in-time examination of an Organisation's technology base, policies, and procedures. It includes a complete analysis of the security of an internal environment and its vulnerability to internal and external attacks.

Technology-driven assessments generally:

- Use standards for specific IT security activities (such as hardening specific types of platforms).
- Assess the entire computing infrastructure.
- Use (sometimes proprietary) software tools to analyse the infrastructure and all of its components.
- Provide a detailed analysis showing the detected technological vulnerabilities and possibly recommending specific steps to address those vulnerabilities.

2.4 Risk analysis

According to the ISO GUIDE 73:2002, "Risk is the combination of the probability of an event and its consequences". Inversely, an enterprise manager should decide to make a financial effort to harden a specific asset if the cost of securing it is less than the risk of loss of the asset. In other words, the manager must be sure that the cost of security in every transaction involving the asset is less than the risk of loss. This is the foundation of security risk management, as detailed by Dan Geer (2003).

In fact security can be seen as risk management, because we do not want to spend too much on security, comparing to what assets we are protecting. Many times, the big questions posed in an enterprise when it needs to calculate the budget is how to measure of the potential loss and lack of knowledge of where it is likely to occur.

A Threat is, in a general approach, anything that might trigger a Risk. However, it is important to point out that a Threat is not directly connected to Risks. A Threat is effective only if it is connected to a Vulnerability. The Risk is thus dependant on the Vulnerability rather than on the Threat itself. If there is a Vulnerability but there is no Threat using it, the Risk remains. Hence,

Threats are mitigated through Vulnerability Analysis over the Assets. According to the Vulnerability Analysis, the Threats can be eliminated or reduced to a point where the value of the Risk is acceptable. The process of mitigating the Vulnerabilities is on the scope of the Security Policies and it is implemented with the Countermeasures.

At the system level, the risk deliberated can be defined by the following equation (1):

*Risk = Likelihood of the Threat * Vulnerability * Consequences of the Exploitation (1)*

The assessment of likelihood takes into account statistical analyses. The assessments of the consequences in terms of loss of security will be considered as the consequence on the operational reliability in the sense that each threat scenario will be evaluated regarding the consequence of the loss of a corresponding security criteria and cost of the primary asset on the operational reliability.

2.5 Countermeasure identification/risk treatment

The main purpose of any security countermeasure is prevention. Therefore, after the first step to *identify* the threat or threats is completed, the next task is to devise an appropriate security response commensurate with that threat. This task employs the *implement* principle.

If the assumption is made that potential perpetrators with the intention to interfere can defeat a security system if given enough information, time and opportunity, then the logical objective is how best to deter the perpetrators from carrying out a successful act of unlawful interference. It is therefore essential that the implementation of suitable preventive security measures be considered.

This operational intervention leads to the third principle, *sustain*, which can be described as an Organisation having the political will and accompanying capability to maintain appropriate reliable security practices. Without the commitment to *sustain* effective security measures, the efficacy of the other principles is diminished.

Countermeasures/security controls will be identified for risk management. A countermeasure is any system, *passive* or *active*, aimed at resolving a risk occurrence. By nature it is reactive rather than proactive, and is aimed at mitigating the loss due to the risk occurrence. Depending on the nature of the risk and the kind of countermeasure, the risk outcome can be only partially mitigated or totally mitigated.

The security countermeasures identified will be spread over the VTMS architecture (ref. to Geer, 2003).

3. CASE STUDY: VTMS

For demonstrative purposes, we will apply our methodology to a case study on a VTMS. Maritime traffic control requires an integrated response, to guarantee safety of human lives at sea, prevent environmental pollution, improve the efficiency of commercial traffic, fight illegal activities at sea.

The system's "open" architecture facilitates integration with other pre-existing structures and enables rapid expansion and/or modification of the system to adjust it to the needs of the maritime sector, the characteristics of which are continuously changing.

Specific functions are dedicated to the preventive identification of possible critical situations, such as collisions, running aground and passages under bridges or restricted areas. More severe safety margins are applied in the case of vessels carrying dangerous goods. During Search and Rescue (SAR) operations, the VTMS provides the Coast Guards with specific tools for supporting decision making procedures.

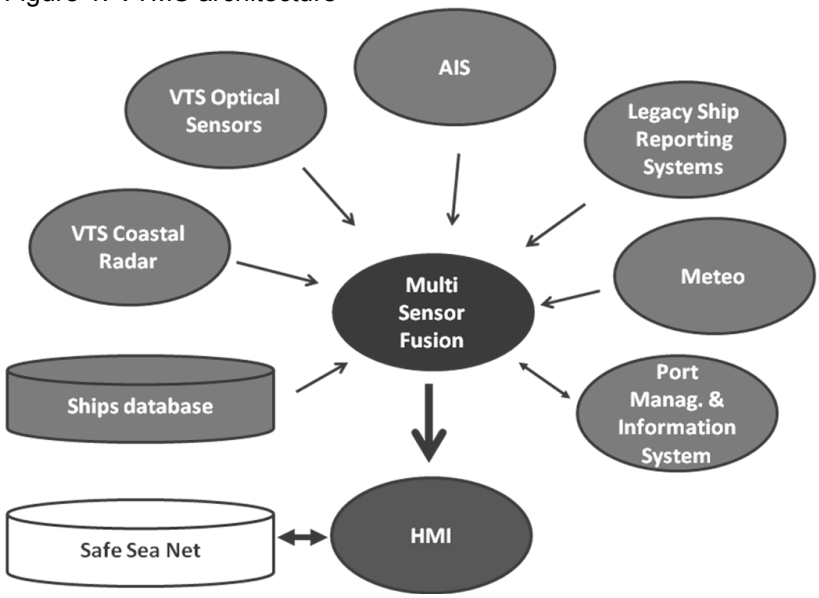
In navigation through straits or in ports, traffic separation lanes and access areas to ports there is often high traffic density, which requires precise allocation of times and space for manoeuvring. With its overall view of traffic and weather and sea situation, VTMS is an ideal support for ship masters. Indeed, VTMS does not only help ships, but guarantees the best possible use of waterways in terms of transport capacity and economic returns.

For these reasons, VTMS is considered a critical port facility (ref. to ICAO, 2002).

3.1 Assets identification

The architecture of the VTM net-centric and service-oriented system is shown in
. The VTMS is formally decomposed using Data Flow Diagrams to obtain the list of assets and their interconnections.

Figure 1. VTMS architecture



The heart of the system is the Multi Sensor Fusion (MSF) process, which has the ability to use the “track” data from several sensors. First and foremost the data comes from radars (VTS Coastal Radar), the only sensors capable of continuously detecting any object on the surface of the sea, independently of its physical characteristics and/or its intention to be localised. Other sensors are the VTS Optical Sensor consisting in a set of closed circuit video cameras mainly covering areas that the radars cannot sense. The integration of the Automatic Identification System (AIS) enables positioning and identification of all the vessels involved. The VTM system is capable of accepting and integrating all the information provided by other maritime traffic control systems or sensors, like the Meteo, and obviously all the information provided by manual ship-reporting procedures (Legacy Ship Reporting Systems). All this is integrated with the Ships database that contain the data about every vessel in transit or inside the port facilities.

The system appropriately weighs to all information and provides the best possible traffic image from the available data. The VTMS enables the definition of any criteria and level of navigation control based on the position, speed and type of vessel involved, or on any sort of Boolean combination. Should a rule of navigation be breached, the system generates an appropriate alarm. Other types of control can also be implemented, which are aimed at supporting the identification of suspect situations, such as trace splitting, rendez-vous in deep waters, and coastal approaches in areas with no surveillance posts.

The complete overview of traffic provided by the Multi Sensor Fusion process, and the data gathered by the individual sensors, are continuously recorded on highly reliable mass memory devices with pretty much unlimited memory.

The VTMS includes a powerful Port Management and Information System (PMIS) enabling the "just-in-time" allocation of resources and provides port authorities with intelligible complete and up-to-date information concerning the navigation plan of ships, their arrival times, their load sheets and all the data that enable the optimisation of port management operations.

The output of the VTM system is sent to the Human Machine Interface (HMI) to support ship masters and guarantee the best possible use of waterways in terms of transport capacity and economic returns.

3.2 Threat analysis

VTMS *Hardware security threats* will be investigated. First of all, hardware assets will be categorised, then the following main sources of threats will be analysed:

- *"Physical threat"*

  An attack aimed at interrupting, disturbing or in any case damaging the infrastructure. The basic key point is that the attack is done in the physical domain rather than in the information domain. This includes theft, and acts of sabotage and vandalism on physical structures. This type of threat is much easier to prevent than the others because it is well known and their effects are quite visible.

- *"Environmental threats"*

  It can be classified as a special case of Physical attacks, whereas the point is that the threat can also arise from natural causes. Typically, this is the case for climatic phenomenon seismic phenomenon, meteorological phenomenon or flood, which can directly lead to physical damages like fire, water, pollution, major accident, destruction of equipment of media, dust, corrosion, freezing. As a secondary consequence, events like loss of power, failure of telecommunication equipment, electromagnetic or thermal radiation may occur that can bring down electronic and computing systems.

VTMS *Software security threats* will be investigated. First of all, software functionalities will be categorised, then the following main sources of threats will be analysed:

- *"Intrusion"*

  Any form of attack that leads the attacker to gain unauthorized access to one of the VTM subsystems. The attack can be performed in a number of ways, mainly dependant on software and protocols bugs and vulnerabilities. It can be done through deliberate software attacks like Virus, Worms, Trojan Horses that can install a back door in the system. A back door is a component that allows the attacker to access the system remotely, usually with administrator privileges.

VTMS *Information security threats* will be investigated. First of all, communication assets and functionalities will be categorised, then the following main sources of threats will be analysed:

- *"Data corruption and stealing"*

  It can arise from two different events:

  a) Communication security failure
  b) System security failure

  The first is a consequence of an attack aimed at the communication infrastructure, hence on the data being transmitted. Recall that network attacks are still on the most common type. The use of legacy systems and procedures, make it easy to exploit them as new attacks are being developed. For example, the widely used wireless encryption WEP is completely broken by now, but still used in many places. The second kind arises from an attack to a working server or client, i.e., an intrusion. Both of them can be exploited to affect the quality of service that the VTM system should be able to provide. This can be done with a denial of service attack, which is usually quite simple to achieve, but with disastrous consequences. For example, if a critical sensor is preventing to provide its information the Port authorities may delay the entrance of vessels in the Port.

- *"Identity usurpation"*

It is usually the consequence of a successful attack either at communication or system level, i.e., data stealing or system intrusion. The usurper can use the stolen identity to perform actions of systems that, at first, might seems perfectly legit. This threat can be performed by an exploitation of a software weakness (as stated previously), by a social engineering process or by an employee error or failure (intentional or not). It is widely accepted that human related threats are among the most common causing a huge amount of losses (ref. to CSI, 2011). The use of right controls and policies, along with effective training can help mitigate this threat.

3.3 Vulnerability assessment

The software subsystems shown in Table 1 represent two of the most relevant sources of vulnerabilities internal to the VTMS, considering the criticality and the impact on the system if affected by malicious attacks.

Table 1. VTMS vulnerabilities

Subsystem	Description
MSF	Multi Sensor Fusion (MSF) process, uses the "track" data from several sensors and fuses them with information coming from databases and legacy ships reporting systems.
PMIS	Port Management and Information System (PMIS) enabling the allocation of resources and provides port authorities with information concerning the navigation plan of ships, their arrival times, their load sheets and all the data that enable the optimisation of port management operations.

3.4 Risk analysis

There is no statistic data available related to VTMS attacks to justify a likelihood analysis. For this reason, risk will be evaluated considering just the impact of potential threats on the system and assuming the probability equal to 1 (i.e. 100%). Countermeasures are so identified, initially, on the basis of the threat analysis and the architecture of the system.

The following Table 2 reports VTMS risk analysis:

Table 2. VTMS risk analysis

CSCI	Threat	Local Effect	System Effect	Severity
MSF	Data corruption and stealing: loss of message coming from external networks (meteo, AIS)	Inability of communicating with external networks. Operator is aware of this. Increased workload.	Loss of data exchanged with external networks	Significant
MSF	Data corruption and stealing: loss of data coming from internal network (VTS, DB)	Loss of tracks data. Inability of updating trajectories. Operator is not aware of this and continues working with existing data.	Corruption of data exchanged with HMI	Major
MSF	Data corruption and stealing: undetected corruption of data coming from PMIS	The corrupted message is not recognised. Incorrect editing of plans.	Corruption of data exchanged with HMI	Major
MSF	Data corruption and stealing: corruption of message toward external networks (SafeSeaNet)	Corrupted messages are checked and discarded by receivers. Inability of communicating with external networks (SafeSeaNet).	Loss of message data exchanged with external networks	Significant

CSCI	Threat	Local Effect	System Effect	Severity
		Operator is aware of this. Increased workload.		
MSF	Intrusion: overload of messages that causes a memory leak.	Data not available at HMI. Loss of automatic warnings. Inability of editing plans.	Loss of data exchanged with HMI	Major
PMIS	Data corruption and stealing: loss of received message from MSF	The PMIS database is not updated.	No effect	Significant
PMIS	Data corruption and stealing: detected corruption of received message from MSF	The corrupted message is discarded and the PMIS database is not updated.	No effect	Significant
PMIS	Data corruption and stealing: undetected corruption of received message from MSF	The corrupted message is not recognised and the PMIS database is contaminated.	Corruption of data exchanged with HMI	Major
PMIS	Data corruption and stealing: loss of sent message toward MSF	MSF doesn't receive data from PMIS but is aware of it. Inability to edit plans.	Loss of data exchanged with HMI	Major
PMIS	Data corruption and stealing: undetected corruption of sent message toward MSF	The corrupted message is not recognised. Incorrect editing of plans.	Corruption of data exchanged with HMI Loss of message exchanged with external networks	Major
PMIS	Intrusion: overload of messages that causes a memory leak	Resource availability not available at HMI. Loss of automatic warnings. Inability of editing of plans.	Loss of flight data exchanged with CWP	Major

3.5 Countermeasures identification/risk treatment

The set of countermeasures are the most important output from this security assessment methodology as they can be seen as the recommendations or the security requirements for VTMS.

According to the risk analysis, the following countermeasures can be identified in order to limit the effects of attacks that cause corruption of data:

- Syntactic and semantic check algorithms at the interface of MSF and PMIS.
- Syntactic and semantic check algorithms at the interface of HMI.

Regarding the loss of data, no countermeasure can be identified internal to VTMS. Other measures can be identified to protect VTMS system from intrusions, as encryption and decryption algorithms passwords.

4. CONCLUSION

The objective of this paper is the definition of a new methodology for carrying out security risk assessment in the port security domain. This process is carried out by modelling the system, identifying the assets, threats and vulnerabilities, prioritizing the threats and proposing countermeasures for the weaknesses found.

For demonstrative purposes, we have applied our methodology to a case study on VTMS.

The methodology presented allows:

- the identification of assets, as services given by the system,
- the analysis of threats, as potential attacks,
- the assessment of vulnerabilities on assets that are remotely accessible,
- the analysis of risks, considering the effects of successful attacks,
- and, finally, the identification of countermeasures to limit those effects.

The proposed methodology allows the identification of countermeasures in a systematic way. Countermeasures can then be adopted as security system requirements at design level.

ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013), in the frame of Marie Curie Industry-Academia Partnerships and Pathways Call (FP7-PEOPLE-2008-IAPP), under Grant Agreement No. 230672 ("CRITICAL-STEP" Project).

REFERENCES

Avizienis A., Laprie J.-C., Randell B., Landwehr C. E. (2004) "Basic concepts and taxonomy of dependable and secure computing" IEEE Transactions on Dependable and Secure Computing, 1(1), 11-33, doi:10.1109/TDSC.2004.2, 2004.

Bakir N.O. (2007) "A brief analysis of threats and vulnerabilities in the maritime domain" Managing Critical Infrastructure, NATO Science for security and Peace, 2007.

CSI (2011) "2010/2011 CSI Computer Crime & Security Survey" Computer Security Institute, 2011.

EC (2006). European Commission's Directorate-General for Energy and Transport "Maritime transport policy, Improving the competitiveness, safety and security of European shipping" 2006.

Farrow S., Shapiro S. (2009) "The Benefit-Cost Analysis of Security Focused Regulations" Journal of Homeland Security and Emergency Management, vol. 26, issue 1, 2009.

Geer D. (2003) "Risk management is still where the money is" Computer, 36(12), 129-131, doi:10.1109/MC.2003.1250894, 2003.

Helmick J. S. (2008) "Port and maritime security: A research perspective" Journal of Transportation Security, 1, 15–28, 2008.

ICAO (2002). International Civil Aviation Organization "Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference" ICAO, Sixth Edition, 2002.

IMO (2002). International Maritime Organization "International Ship and Port Facility Security Code (ISPS Code)" 2002.

Pallis A. A., Vaggelas G. K. (2007) "Port and Maritime Security: A Critical Analysis of Contemporary EU Policies" International Symposium on Maritime Safety, Security and Environmental Protection, 2007.

Swiderski F. (2004) "Threat Modeling" Window Snyder, Microsoft Press, 2004.

Whitman M., Mattord H. (2012) "Principles of Information Security" 4th edition, Cengage Learning, 2012.