CIT2016 – XII Congreso de Ingeniería del Transporte
València, Universitat Politècnica de València, 2016.
DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

Security assessment in harbours: parameters to be considered

David Romero Faz
Universidad Politécnica de Madrid. Dpto. Ing. Civil: Construcción, Infraestructura y Transporte. Madrid, España, david.romero@upm.es
Alberto Camarero Orive
Universidad Politécnica de Madrid. Dpto. Ing. Civil: Transporte y Territorio
Madrid, España, alberto.camarero@upm.es

SUMMARY

The ports are the main node in the supply chain and freight transportation. The terrorist attacks of September 11, 2001 marked a turning point in global security. Following this event, and from then on, there is a widespread fear of an attack on commercial ports. The development of the International Ship and Port Facility Security (ISPS) Code of the International Maritime Organization (IMO), and the implementation of the measures derived from it, have significantly improved security at port facilities. However, the experience in recent decades indicates the need for adjustments in the security assessment, in order to improve risk assessment, which is sometimes either underestimated or overestimated. As a first result of the investigation, new parameters for assessing security are proposed considering new aspects on the basis of an analysis of the main methodologies specific to port facilities, the analysis of surveys of the responsible managers for the security of the Spanish port system, and the analysis of the security statistics obtained through security forces.

1. INTRODUCTION

Since 2003, the International Maritime Organization (IMO) and the International Labour Organization (ILO) have defined a methodology for port facilities risk assessment, have developed methodologies directly applicable to quantify risk and, based on the results, proposed various measures to mitigate the risk. However, the specific methodologies for the assessment of port security are still few and generally are formulated theoretically, but not based on real conceptual or theoretical insights. The purpose of this study is to define a new methodology for assessing the risk based on real data and information obtained directly from the Port System, that allows to determine those aspects not considered so far in the security analysis in port facilities to terrorist acts, sabotage, theft, etc., not being considered here the losses due to technical problems associated with the installation, etc.. In order to identify new parameters reflecting unpublished aspects, a comparison between the selected methodologies for ports and further surveys, and revision of existing statistics of crime in ports has been carried out. Subsequently, by applying a panel of experts, the proposed parameters have been validated.

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

2. METHOD

The investigation began with a review of the state of the art on risk analysis in infrastructures, describing the existence of several methodologies, but only those that are meant to evaluate any type of infrastructure and to consider the risks of any kind or acts specifically terrorism, sabotage, etc., were selected. Thus, a total of 16 different methodologies for risk assessment in critical infrastructure, including ports, were selected and analyzed. Once collected and analyzed, a few methodologies were selected that met the following criteria:

1. Specifically targeted on security assessment of terrorist acts, sabotage, intrusion, etc.
2. Specifically developed for application on port/harbours facilities. Those that focused on specific risks cited in port infrastructure or related to these were considered. This is the case of airport facilities due to large organizational and functional similarities with ports.

Based on these criteria the following methodologies were retained for its comparative analysis:

1. CIVIL AVIATION (COLOMBIA). This is the International Civil Aviation Organization (ICAO) methodology for aviation security applied in Colombia airports and other three countries in the region. Colombia is a country with serious security problems due to the existence of terrorist groups for decades and therefore it is of interest to consider.
2. CARVER (US Army). This methodology has been already used especially in risk assessments in port environments of the American continent which goodness has been largely proven, having been used also as the base for the development of other methodologies such as SECUREPORT (Spain).
3. RBDM. Navigation and Vessel Inspection. US Coast Guard. This is the methodology used for the risk assessment in the USA ports and it is highly followed because its application comes out of the borders of the USA, having been introduced in most of the American countries due to the commercial relations with the USA.
4. SECUREPORT. Ports of the State (Spain). The Spanish methodology, was developed by Ports of the State specifically for this sector, being approved and put into practice in 2004.
5. THREAT AND RISK ANALYSIS MATRIX (TRAM). International Labour Organization (ILO) and International Maritime Organization (IMO). This methodology was originally proposed by IMO and, therefore, it is the basic reference for the study and risk assessment in ports all over the world.

2.1 Comparative analysis

Methodologies are qualitatively analyzed in order to obtain more information about the features, detail the scope, format of the outcome of the risk assessment, scope of the

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

evaluation, etc. To carry out such a comparative analysis, the following issues are discussed:

• Risk assessment method employed: does it use the classic formula?
• Way the risk assessment is done, is it qualitative or quantitative?
• Simplicity and ease of application
• Does it consider the probability of the event?
• Types of attacks considered, are they specified? What type?
• Accurate identification of vulnerabilities with different rates for each specific parameter of vulnerability
• Is the vulnerability analysis broken down by parameters or is there a global analysis, instead?
• Scheme for determining the consequences, specifically or globally valued?

The assessment made between the different methodologies selected is summarized below:

• CIVIL AVIATION (Colombia): it assesses the risk by a preliminary analysis of the capabilities of the infrastructure to repel an attack, based on historical events. It does not perform a detailed analysis of the threat based on a formulation, but it does study - for each threat – the different aspects and as a result a probability of occurrence is assigned. It also assesses the consequences only in terms of loss of operation of the installation.

• CARVER (USA): it identifies very well the vulnerabilities of a given facility so that the measures to take can be fit in detail. It is designed to evaluate the possible targets of attack, giving it an interesting objectivity to the result from the viewpoint of definition of possible attacks. It does allow neither the assessment of direct consequences on targets or population, which is a major disadvantage, nor the assessment of the probabilities of occurrence.

• RBDM (Risk Based Decision Making). Navigation and Vessel Inspection Service (US Coast Guard) is an easy-to-use methodology and it is designed specifically for evaluating risks in ports, also considering risks included in the scope of this research. The consequences are pre-established according to the type of traffic and terminals and - as in the above described case – it does not consider the consequences of loss of life. Besides, the consequences are neither evaluated nor specified (not measurable). The vulnerabilities are measured on the basis of accessibility and security, in three levels.

• SECUREPORT (Spain): it is a comprehensive methodology that includes multiple parameters and sub-parameters that makes it - to the security assessors - neat and unattractive for its application. It focuses primarily on three types of attacks and considered the probability of the event. Accessibility and security are assessed only qualitatively, without defining general acceptable characteristics to these.

• TRAM (IMO-ILO): This method is simple to use and considers the same risks as the subject of this research. It considers the probability of occurrence of the event, but the assessment of the vulnerabilities and consequences is very general, without detailing specific aspects to value.

Once the comparison between the different methodologies selected is done, a preliminary comparison between the parameters that are defined in each of them is performed,

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

evaluating them from the perspective of the classical formulation of risk assessment:

Risk = Threat x Vulnerability x Consequences

In order to evaluate them, they are reviewed and analyzed with the following criteria:

• Description of parameters
• Scope of the parameter; similarities and differences
• Relationship between qualitative parameters

For the compliance of the targets defined in this section, a matrix which relates the methodologies to be studied and the parameters that each of them considers in the evaluation of the risks has been created. In that matrix, the parameters used for every methodology are indicated in the rows along with the parameters of other methodologies that could be considered to be homologous or comparable in content and target, in order to analyze them later in a joint way. When the matrix is analyzed, it becomes obvious the existence of a number of parameters that - on a general way - are repeated in almost all of the formulations; parameters of probability, vulnerability and consequences, and the second group of parameters derived from the previous ones that, therefore, have the same meaning or assignment (Table 1).

METHODOLOGY / PARAMETERS	Civil Aviation (Colombia)	Carver	RBDM	Secureport	TRAM
Threat -Probability	X	O		O	X
Vulnerability (measurements of security and accesses)			X		X
Impact - Consequence	X		X		X
General probability				X	O
Symbolic character		O		X	
Accessibility to the installation-Vulnerability		O		X	O
Susceptibility to the destruction				X	
Operative inefficiency-Vulnerability				X	O
Damages to the human life	O	O		X	
Economic damages	O	O		X	
Redundancy of elements that assure the functionality				X	
Time of recoverability		O		X	
Social and environmental consequence		O		X	
Criticality		X		O	

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

Accessibility		X		O	O
Recoverability		X		O	
Vulnerability		X	O	O	O
Effect on the population	O	X		O	
Recognizable targets		X		O	

X parameter used in the methodology
O parameter considered in an implicit way in the methodology

Table 1 – Parameters Matrix

Below, as a summary, those parameters identified which define different aspects from the classics are described. These are:

• Redundancy elements: it rates quantitatively the possibility that the port facility being analyzed may continue working without the goods affected by the event that is considered.

• Criticality-symbolic character: it values the increased probability of occurrence of an event in relation to the general level due to the symbolic nature of the system or analyzed component that could make it become a preferred target of attack.

• Recoverability: it rates quantitatively the required period of time to recover the port facility to fully functional and operational capabilities (same as before the attack), provided that recovery is possible.

• Recognizable objectives: It tries to assess the degree to which an object can be recognized without confusion with other objects or elements. The easily recognizable goals always better serve the purposes of a terrorist.

In short, it is possible to say that all the considered methodologies are structured on the same basis of assessment in all indices, although there are nuances in the range offered by each methodology's parameters, except for the CARVER methodology, which does not evaluate or assign the event probability or study the consequences of this.

2.2 Surveys

Once the parameters defined in the reference methodologies were analyzed, the detection of gaps or aspects not covered by those methodologies has been undertaken. With that goal, a survey was made to several port terminals of the Spanish Port System in order to obtain their type of threats, their frequency of occurrence and the security level to be considered in the assessment of risk in the facilities. The main objective of the surveys is to provide the study with a better reality-based knowledge of the existing lack of definitions in port risk assessment that nowadays are operating and which have been evaluated previously with other methodologies. The procedure implemented is described below:

1. Definition of case studies for the Spanish Port System. The following types of terminal were considered to be evaluated: Solid Bulk, Liquid Bulk (oil, LNG, etc.), General Goods, Containers, and Cruise Passengers A questionnaire was set out according to the type of terminal in order to gather the relevant information to be used in the study.

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

2. Survey development to the responsible of terminals' security. The surveys were sent to 25 public and private terminals of the Spanish Port System. The following conclusions were achieved:

- In general, larger threat risks do exist for goods than for they do for persons.
- The intrusion risk differs from port to port, playing a key role the location of the port along the Spanish coastline - major threat frequency in the ports located in the south coast which are nearer to the Maghreb (Africa).
- The potential of threats depends on the type of goods moved by the terminal. The terminals that present major risk are, according to the survey, Passenger terminals followed by Liquid Bulk terminals.
- The lay-out of the facilities inside the terminal has a direct impact on the possibilities of having an attack.

2.3 Security statistics analysis

Later statistics on incidents against the security registered by the Coastal and Border Service of the Directorate General of the Guardia Civil (DGGC) responsible for security in the Spanish commercial ports were evaluated. Security Bulletins of the 46 commercial ports of Spain (28 Port Authorities), with data of two years were reviewed. From its analysis the following relevant information is deduced to the study by type of threat:

• Illegal immigration. The breach of security is mentioned due to numerous interceptions of irregular migrants in merchant ships in various ports of southern Spain as ports of origin and as a destination port in the north of Spain or Europe.

• Stowaways and intrusion on the premises (theft ...). It proved feasible the access to the facilities of some ports and even ships, and therefore there are clear risk of detection of intrusion problems despite the access to terminals has been improved.

• Sabotage. There are a reduced number of them, but there have been several cases in some ports. Physical or electronic sabotage of the systems themselves was considered, or of the communications control centers, or of the security forces in the port. All these are violations that showed the greatest weakness of the systems, while by themselves they constitute a situation of risk prior to the completion of criminal acts.

• Terrorism. Although to date there have been few, there have been several attacks by the terrorist Basque group ETA, particularly in the same Port during July 2009. This highlighted the shortcomings and lack of effectiveness of the security controls in shipments of passengers and vehicles in some Spanish ports and the lack of security controls at landing at the destination. Also, several interviews were made with experts in security, and the following conclusions were obtained:

- Lack of homogeneous criteria with regards to the capacity of dissuasion of the access to the terminals. This implies the need to better define the accessibility levels to be able to consider more objectively the threats, which at present are underestimated.
- Need to improve the security (accessibility) in the pre-loading at the passengers' terminals where many potential threats do exist.
- The security of a facility is determined by its proximity to other terminals of larger

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

potential risk and that may pose a threat for that facility.

- The geographical location and proximity to "hot spots" of a port increases clearly the possibilities of threats of the evaluated type.

3. RESULTS

As a result of the development of the surveys, the analysis of the security statistics, and with the development of an expert panel, it was verified the existence of some aspects of the risk not being considered till now. It is deduced from the analysis that questions such as the specific evaluation of the risk (that can be linked to the type of terminal), or the implicit risk of a port according to its location on the coast, must be gathered in different parameters that may be combined in a formulation of risk assessment together with the consequences.

The different factors to be considered and its transposition to parameters are described:

- Port (IP). This parameter is intended to value the general risk against the security, named "intrinsic risk of the port", that is the threat level for every port measured/value based on its physical location along the Spanish coast. The location of the port impacts perceptibly the level of general security facing possible threats.
- Terminal (IT). This parameter is intended to consider the "intrinsic risk of the type of terminal", that is the threat level which is linked or defined for every type of terminal. It becomes clear that the risk can be linked, from a point of view of the probability of occurrence of an event of a threat, to each type of terminal according to the kind of facilities that it has and the activity that it develops. Therefore, different threat levels are defined for every type of terminal: container, passenger, liquid bulk, solid bulk, etc. based on the particular characteristics of the type of goods and on the characteristics of design of every typology of terminal.
- Accessibility (Iac). This parameter is re-defined, since it already existed, although now it is intended to assess the vulnerability of the facilities based on different physical and operative aspects, taking into account the degree of roadway or railway access that would facilitate the access to the terrorist (the easier accessibility the larger risk). Also, other aspects are considered such as: the type of closing of the facility, the control of access systems and the control of vehicles, the technology used (motion sensors, CCTV, radars, scanner, video analysis, etc.).
- Layout (ILo). The influence of the layout in the security of a terminal is verified especially for what concerns the adjacent facilities, since it might be possible to access to a target by crossing an adjacent facility or even being impacted by a foreign attack. This parameter is valued according to the proximity of the terminal to the port access Also, the location of terminals with regards to liquid bulk terminals is considered due to the fact that the effect of an attack with explosives or shots to the liquid bulk terminal might reach other terminals in the vicinity.
- Operative relevance (IRo). This parameter values the importance that certain facilities or elements have for port operation such as structures, railroad facilities, stores, etc.

DOI: http://dx.doi.org/10.4995/CIT2016.2016.3181

and that can suffer the effects of a terrorist attack, rendering useless an important part of the terminal, with the resulting consequences.

As noted, the proposed parameters constitute a significant improvement in the risk assessment as it is been done nowadays, adjusting their value and therefore their importance to more realistic values, which will undoubtedly improve planning security and measures to take to the threats considered by those responsible for the installation.

4. CONCLUSIONS

Based on the study carried out and the information gathered, the main conclusions are presented: in spite of the implementation of security plans for 10 years, vulnerabilities not considered do exist. Therefore, their analysis needs to be adjusted on a continuous basis. Nowadays, the risk assessment does not fit to reality in many cases, overestimating its negative evaluation or - on the contrary – underestimating as limited risks those that are not. The geographical location of the port on the shoreline can be determinant for what concerns to the existence of a threat. The key to prevent most of the threats is the accessibility to the port facilities; hence it is relevant to improve its assessment.

REFERENCES

Dirección de Seguridad y Supervisión Aeroportuaria. Grupo Estudios y Proyectos de Seguridad Aeroportuaria (2010). Circular 4302-082-16.10, Procedimiento de Evaluación de Riesgo en Aeropuertos de Colombia

European Commission (2012). DELIVERABLE D2.3. Integrated report on the link between Risk Assessment and Contingency Planning Methodologies

Ed Clarke & Don Philpott (2011). CARVER+Shock Vulnerability Assessment Tool, Longoat Place, Florida.

International Labour Office (ILO) and International Maritime Organization (IMO), (2004). Security in Ports. ILO and IMO Code of Practices.

National Infrastructure Simulation & Analysis Center (2011). Fast Analysis Infrastructure Tool.

Sanchidrian, C. (2008). VIII Curso de Transporte Marítimo y Gestion Portuaria. La seguridad, el código ISPS y la legislación comunitaria

Sandia National laboratories (2002). A Scalable Systems Approach for Critical Infrastructure Security.

The Institution of Engineering and Technology (2013). Infrastructure Risk and Resilience: Transportation. ISBN 978-1-84919-696-3.

US Coast Guard, (2003). Navigation and Vessel Inspection. Circular N° 11-02 (NVIC 11-02).