New Indices of Risk Assessment for Security in Port Infrastructures

David Romero-Faz, Alberto Camarero-Orive

Abstract— **The risk assessment in infrastructures is present in the daily policy of the different countries all over the world. From the 11th September and the bombings in Madrid and London, the most countries began to consider the international terrorist threat like a real one. Regarding to the port facilities security, in 2003 the International Maritime Organization designed its own methodology to assess the impact of an attack to any port infrastructure. From that moment the different countries implemented in few years this methodology and some countries their own one to assess the risk of an attack to their ports infrastructures.**

Despite this and may be because of most countries implemented their Protection Plans in their ports very quickly as the result of the risk assessment, there are some aspects which are not really well studied nowadays. After more than ten years with the Protection Plans implemented in the Spanish Port System now there are good statistics of threats to be considered to review the existing methodologies. With the target of improving the knowledge of the real risks and also the scope of the risk assessment in ports, a revision of the main methodologies was taken together with a survey to the Port Security Officers and the analysis of the threats statistics. As the result of the investigation several new indices were defined for risk assessment. Indices like intrinsic risk of the port, intrinsic risk of the type of terminal, the redefinition of accessibility, the layout of the terminal or the operative relevancy that some elements have for port operation.

***Index Terms*— Risk assessment, port security, threat, vulnerability**

I. INTRODUCTION

After the 11th September 2001 attacks a change took place in the world and concept of global security, including security in ports. These changes in the concept of security were incorporated in 2001 by means of the Resolution A.924 (22) in which one appeals to a more global term, the "Maritime Protection", like part of the amendments realized to chapters V and XI of the International Agreement of Safety for the Human Life in the Sea (ALONE), incorporating them into the International Ship and Port Facility Security Code (ISPS). Since then, several specific methodologies have been developed for the evaluation of the risk attacks on harbours in several countries, although - still nowadays - there keeps on being investigations on how to improve the assessment of risk trying to fit the risk obtained to the real risk of the facilities.

The objective of this study is to determine possible aspects not considered till date in the security analysis of harbours facing terrorist acts, sabotage, thefts, etc., without being considered here decreases of the security due to technical problems associated with the facilities, networks etc. Therefore the aim is the identification of new parameters which improve the assessment of security facing the above mentioned events in the Spanish ports.

II. METHOD

The procedure followed to identify new parameters consisted of a review of the state of the art of existing methodologies, selecting later those from exclusive application to ports, considering the particular characteristics of its facilities and activity. In order to identify new parameters that reflect unpublished aspects, initially a comparative between the selected methodologies for ports has been performed and later through the achievement of surveys, and reviewing of existing statistics of criminal acts in ports. Finally and through the application of an expert panel, the proposed indices have been validated.

It is possible to define the risk (R) as the measurement of the economic loss and/or damage for human life, resulting from the combination between the frequency (f) of an event and the magnitude of the losses or damage (consequences, c) within a period of time.

$$R=\mathrm{f}\,(f, c) \qquad \text{(a)}$$

where,

R is the risk
f is the frequency of occurrence of an event
c is the consequences

Based on this theoretical definition Fine [1] defined the following formula to assess the risk:

$$Risk = Exposure \times Probability \times Consequences \qquad \text{(b)}$$

The concepts contemplated are:

a) Exposure (Threat). It is the frequency with which the risk occurs. As such, the first undesired event initiated the accident sequence.

b) Probability (Vulnerability). The possibility that once the risk is presented, the accident arises.

c) Consequences. Damage because of the risk that is considered the most serious possible including personal misfortunes and property damage.

The study began with a review of the state of the art [2] on risk analysis, describing the existence of several methodologies,

but only those that are described to evaluate any type of infrastructure and to consider the risks of any kind or acts specifically terrorism, sabotage, etc., were selected. A total of 16 different methodologies for risk assessment in transport infrastructure were identified and analyzed in the initial stage. The methodologies preliminarily analyzed are listed below:

1. Civil Aviation, Colombia [3]
2. ARMS, UK [4]
3. BMI Protection of Critical Infrastructures, Germany [5]
4. CARVER, US Army [6]
5. CIPDSS Critical Infrastructure Protection Decision Support System, IET [7]
6. COUNTERACT, Generic Guidelines for Conducting Risk Assessment in Public Transport Networks, European Commission [8]
7. DECRIS , Norway [9]
8. GUIDELINES FOR COMBINED TRANSPORT TERMINALS, Union of Combined Road-rail transport companies (UIRR) [10]
9. EURACOM, European Commission [11]
10. Fast Analysis Infrastructure Tool (FAIT), National Infrastructure Simulation & Analysis Center [12]
11. FEDERAL AVIATION ADMINISTRATION (FAA), USA [13]
12. THREAT AND RISK ANALYSIS MATRIX (TRAM), International Labour Office (ILO) and International Maritime Organization (IMO) [14]
13. RAM. Sandia National Laboratories, USA [15]
14. RBDM, Navigation and Vessel Inspection, US Coast Guard [16]
15. SECUREPORT, Ports of the State (Spain) [17]
16. INLAND CONTAINER TERMINAL, Austria [18]

Once collected and analyzed, from the above methodologies a few 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 between them.

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

1. CIVIL AVIATION (COLOMBIA). This is the OACI's methodology for aviation security applied in Colombia airports and other three countries of 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). The CARVER methodology has been already used specially 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 proposal for the IMO-ILO and therefore it is the basic reference to the study and risk assessment in harbours over the world.

III. COMPARATIVE ANALYSIS

A comparative analysis was carried out between the retained methodologies beginning with the analysis of its advantages and disadvantages and which is summarized next.

A. Methodological comparative

CIVIL AVIATION (COLOMBIA)

Advantages

- o The assessment follows the traditional formula
- o The risk assessment is quantitative simplified.
- o It is simple and easy to apply.
- o It considers specially the risk of terrorist attack, sabotage, intrusion, etc.

Disadvantages

- o The evaluation of risk attack, although it is described in its bases, is unspecific when having quantified it, since the elements that can be an attack target or those aspects that are liable to value facing a security threat are not detailed.

CARVER (US Army)

Advantages

- o The risk assessment is quantitative simplified.
- o It identifies very well the vulnerabilities of the facilities; therefore the measurements to be taken on this matter can fit in detail.
- o It values the importance (criticality) of the target in terms of economic, social, operative, restoration of service, etc.
- o It considers specifically the risk of terrorist attack, sabotage, intrusion, etc.
- o It values the effect of the measurements adopted on the population.

Disadvantages

- o The risk assessment does not follow the traditional formula.
- o It does not make an evaluation of probabilities or frequency of occurrence.
- o It does not allow determining the consequences of a terrorist attack.

RBDM (US Coast Guard)

Advantages

- o The assessment follows the traditional formula.
- o The risk assessment is quantitative simplified.

o It is simple and easy applying.

o It considers specially risk of terrorist attack, sabotage, intrusion, etc.

o It is developed specially for threats assessment in ports.

o It allows selecting specific threat situations to evaluate its potential risk and applying specific measurements.

Disadvantages

o Consequences are valued strictly based on the size and destination (national or international) of the ship and its load and, for the worst case, the danger of the transported goods is valued.

o Vulnerability is valued exclusively based on the accessibility and the organic security without considering other factors. Also accessibility is not valued on detailed form.

SECUREPORT (Ports of the State (Spain)

Advantages

o The assessment follows the traditional formula.

o The risk assessment is quantitative simplified.

o It considers specially the risk of terrorist attack, sabotage, intrusion, etc.

o It consider the likelihood of the event.

o It makes a detailed study of the vulnerabilities of the facility.

Disadvantages

o It is prolix and complex to apply.

o It only considers three global threat situations, namely: attack with explosives (on a generic form), biochemical attack, and cybernetic attack.

o Very detailed quantification of vulnerabilities and consequences, this implies an assessment and complex analysis of every situation of threat to be valued, considering the difficulties that it involves from the point of view of the allocation of score.

o The accessibility, as part of vulnerabilities, is valued on a very qualitative fashion, without considering specific characteristics of the access.

TRAM (IMO-ILO)

Advantages

o The assessment follows the traditional formula.

o The risk assessment is quantitative simplified.

o It is simple and easy to apply.

o It considers specifically the risk of terrorist attack, sabotage, intrusion, etc.

o Developed specifically for threats assessment in ports facilities.

o It allows selecting specific threat situations to evaluate its potential risk and applying specific measures.

Disadvantages

o The evaluation of the vulnerabilities is unspecific; concrete aspects that could affect security not being valued.

o Consequences are valued on a very global way, specific damage to the human life or environmental damage etc., are not valued although it seems that on an implicit form they could be valued.

B. Comparison of Indices

After evaluating the advantages and disadvantages of each methodology, a detailed comparative between the indices of their formulations is done with a trifold objective:

1. To analyze which aspects are considered in the definition of every index,

2. To verify the differences between different indices with the same or similar purposes, and

3. To find similarities between indices

For the compliance of the targets defined in this section, a matrix which relates the methodologies to be studied and the indices that each of them considers in the evaluation of the risks has been created. In that matrix, there indices used for every methodology are indicated in the rows along with the indices 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 indices that - on a general way - are repeated in almost all the formulations; indices of probability, vulnerability and consequences, and the second group of indices derived from the previous ones that, therefore, have the same meaning or assignment (Table 1).

Table 1. Indices Matrix

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	
Accesibility		X		O	O
Recoverability		X		O	
Vulnerability		X	O	O	O
Effect on the population	O	X		O	
Recognizable targets		X		O	
Probability of success of the attack or mistake of the security systems					

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

The different indices are analyzed next in order to detect analogies between them and to be able to summarize the content of each used formulation and their interrelations. The evaluated indices can be grouped as follows:

Threat - General Probability – Criticality.

In general, the threat is defined as the probability of occurrence of that an event, damage, offense, etc. As such it is defined in two out of the six methodologies studied, although in other two methodologies this criterion is described in a very similar fashion with the same reason; estimating the probability of occurrence of an event. These indices are named General Probability and Criticality (SECUREPORT and CARVER).

The General Probability is an index that values from a global perspective the possibilities of a terrorist attack to the facilities. Its value is determined by the security Authority, although it is neither specified nor justified a value or a score criterion.

Criticality defines the probability occurrence of the event based on the importance of the facility under study, using as the main judgement criterion the potential impact of the terrorist action in public security, in the facility staff, and in the facility operation.

As it is observed, the principle that applies for the definition of the threat in all the cases is identical - the

probability of an attack to take place -, and therefore it is possible to conclude that three indices define this fundamental aspect of the risks assessment although with slight differences.

Vulnerability – Accessibility to the facility – Operative Inefficiency – Probability of success of an attack.

Vulnerability is defined, in a common way, as the existence or disposition of security measures aimed at the elimination or reduction of access to the protected target to groups or individuals not authorized, and the training of the above mentioned groups. Nevertheless, there exist slight differences in its definition that concern the scope according to the analyzed methodologies. For instance, the definition given in SECUREPORT is more complex and it includes more aspects than the basic aspect relative to the systems of access and security to the facilities, making use of three different coefficients. The first index, named IAI (Index of Accessibility to the Installation/Facility), values quantitatively the ease that persons or means have to cause a threat to the installation. The existence of alarm systems, or the existence of armed patrols permanently operative with the possibility of a rapid intervention are taken into consideration.

The second index, named ISD (Index of Susceptibility to the Destruction), values quantitatively the susceptibility of the element which eventual destruction is considered caused by the analyzed threat, considering the protection systems that the facility has in place.

And, finally, the IOI (Index of Operative Inefficiency) values the inefficiency of the operative procedures to be followed in order to face possible threats.

As described, the evaluation of vulnerability done by SECUREPORT is more complex than the common definition of this parameter.

The RBDM methodology defines two measurable basic criteria, such as the accessibility to the facility and the operative inefficiency. These two criteria fully coincide with the described on SECUREPORT through the indices IAI and IIO.

The CARVER methodology uses two indicators to analyze and to value the vulnerability, namely Accessibility and Vulnerability. Both indicators completely coincide with the previously described in its content. In this case, vulnerability is applicable not only to persons but also to goods and, therefore, it values the security on facilities (material damage) in addition to the security of the persons (physical damage). Also for this vulnerability parameter a variability of the vulnerability is defined according to the nature and construction, the quantity of wished or necessary damage, the available assets, etc.

From the previous analysis it is possible to conclude that vulnerability is a term defined by all the analyzed methodologies, with a common base between them although with scopes or breakdowns of the above mentioned concept according to the case, although they always value essentially two questions: the accessibility to the target and the training of the security teams to avoid an attack to such a target.

Impact-Consequences-Damage to human life/ economic-social/environmental consequence.

The result of any terrorist act over a target is named "impact or consequence". It is certainly the parameter or indicator that presents less difference in the methodologies, although it is - at the same time - the most broken down because of the different effects that this impact may have on the facility. As such, in some of the methodologies it is defined in a simple way through only one parameter or index that quantifies all the consequences, independently of its type, while in other methodologies this index is broken down in several more. The latter is the case of SECUREPORT and CARVER which break down the consequences into damage to human life, economic damage, social and environmental damage or even effects over the population.

Therefore "impact or consequence" is a wide term in content and scope according to the methodology followed, although it is the authors' opinion that it must gather all possible effects derived from a terrorist act on the infrastructure, bearing into consideration:

- Damage to the human life
- Damage to the infrastructure
- Environmental damage
- Damage to the society (Emotional)
- Damage to the production or development of the terminal

Matrix analysis showed that once the different analyzed indexes are grouped into three blocks, there remain some other indicators which scope or meaning differ from those and complement them. This is the case of the next indicators: redundancy of elements, criticality, symbolic character, recovery of the functioning and the property, and recognizable targets.

A summary of the assignment and scope of the above mentioned indicators follows.

Redundancy of elements. This index assesses quantitatively the possibility that the analyzed facility could keep on working without the goods that could be affected by the event under study, considering the possibility that the impacted function could be replaced by another existing facility in the port.

Criticality. This index assesses the global importance of the function executed by the facility. The importance of this factor is based on the potential impact of the terrorist act in the public security, on that of the staff and on the operating of the facility. Also it is based on the impact that on the public opinion would have a terrorist attack and the perception that about the attack would have the society.

Symbolic character. This indicator assesses the increase of the probability of occurrence of an event due to the symbolic character of the facility or element analyzed and that could make it turn into a preferable target.

Recovery of the functioning and the property. By this indicator there is assessed the ease or difficulty that would suppose the recovery of the normal daily development of the proper activities of the economic sector to which the facility belongs, substituting, or reconstructing such facility.

Recognizable targets. This indicator evaluates how recognizably from the point of view of a potential attack the facility is. This fact will turn it, undoubtedly, more vulnerable.

As synopsis of the previous analysis, Table 2 sums up and relates the analyzed indicators grouped into blocks according

to its meaning, in spite of the existence of slight differences, as it was previously mentioned.

The initial matrix is now simplified, being the nineteen indices grouped into only seven categories. Out of the seven categories, three of them (probability, vulnerability and consequences) are considered directly in most of the analyzed methodologies.

Table 1. Matrix of relations between indices

METHODOLOGY / THEMATIC SUBSCRIPTS	CIVIL AVIATION (COLOMBIA)	CARVER	RBDM	SECUREPORT	TRAM
Probability (threat)	X			X	X
Vulnerability (measurements of security and accesses)		X	X	X	X
Consequences	X		X		X
- Damages to the human life /economics				X	
- Repercusión social/ambiental		X		X	
Social and environmental consequence				X	
Criticality - Symbolic character		X		X	
Recoverability		X		X	
Recognizable targets		X		X	

IV. 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 security level to be considered in the risk assessment of 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 (commercial ports). The following types of terminal were considered to be evaluated: Solid Bulk, Liquid Bulk (oil, LNG, etc.), General Goods, Container, and Passenger. A questionnaire was set out according to the type of terminal in order to gather the relevant information to be used in the study.

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, major threats risks do exist for goods than 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.

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 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.
- Facilities do have a certain operative relevancy against a threat and therefore an attack on those is considered to be critical, for example the access, the facilities for loading or the load manipulation teams.

V. Security Statistics Analysis

Later statistical data relative to events were evaluated against the safety registered by the Service of Coasts and Borders of the General Directorate of the Guardia Civil (DGGC), police service responsible for the security in the Spanish Ports. *Security Bulletins* were checked belonging to the 46 commercial ports of Spain (28 Port Authorities), with information of about two years. From this review, the following information concerning the type of threat may be drawn:

- *Illegal immigration.* The rupture of security is documented by the many interceptions of irregular immigrants in merchant ships with origin in several ports of the south of Spain and destination in the north of Spain or Europe.
- *Stowaways and intrusions in the facilities.* It is verified that the access to the facilities of some ports, and even to ships, is feasible and that, therefore, clear problems of detection of the risk of intrusion do exist - in spite of the accesses to terminals having been improved.
- *Terrorism.* Although up to date they have been limited, there have happened several attacks perpetrated by the terrorist group ETA particularly in the Port of Palma de Mallorca (July 2009). This fact showed the shortage and lack of effectiveness of security control panels in the boarding of passengers and loading of vehicles in some Spanish ports and the absence of security control panels when unloading in the destination.

VI. 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 indices that may be combined in a formulation of risk assessment together with the consequences.

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

- *Port (P).* This index 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. This way a port located on the Cantabrian coast will have a probability of general threat lower than any port arranged in the South Atlantic Ocean or the Mediterranean Sea. The shoreline facades that are proposed to be considered for its evaluation will be: North Atlantic, South Atlantic, Mediterranean or Cantabrian.

• *Terminal (T).* This index 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 (Ac).* This factor 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 accessibility 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 (Lo).* 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 factor 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 relevancy (Ro).* This factor values the importance that certain facilities or elements have for port operation such as structures, railroad facilities, stores, etc. and that can suffer the effects of a terrorist attack, rendering useless an important part of the terminal, with the resulting consequences.

VII. Discussion &Conclusions

As shown, the proposed indices suppose a notable progress in the evaluation of the risk as compared to how it is being performed at present, since its value is adjusted - and therefore its importance - to more realistic values. This fact will undoubtedly allow improving the planning of the security and the measures to carry out for the threats considered on the part of the manager of the terminal.

The study's main contribution is the consideration of new factors that stem from the analysis of direct surveys to security managers of the terminals, as well as of the analysis of the security statistics. As shown, a terminal will have a major potential risk of attack if it is located along a stretch of shoreline with respect to another, as drawn from the security bulletins. The proposal of this first index will suppose, in a later stage, that the threat under study could be increased in its presentation risk or not according to the port in which it takes place.

It is proved that the risk level changes according to the type of terminal under consideration, turning out to be different for example in cruise terminals opposite to terminals of solid bulks (of less interest for an attack, which are intended generally to produce casualties in addition to material damage to the facility).

Accessibility determines highly the viability of most of the threats and therefore its detailed consideration results of great interest. The layout will be of large interest since, if the facility under study is next to another one of high risk, it can in turn be impacted. The viability of an attack increases if the target turns out to be simple to reach, and therefore the evaluation of its proximity to the accesses to the port and to the exterior perimeter is considered important.

Structures located in the port terminals, transshipment equipment and storage facilities are key for the correct operating of these terminals. All of them will have its importance and therefore a certain weight to assess in the analysis of risk.

A future consideration of these parameters in the real estimation of risks of terrorist threat in ports will suppose an advantage in the short term for the commercial ports obtaining from it a better fit of the risk according with the experience of the security staff and after years of establishment of security plans in ports. Also they will allow the General Directorate of the port to better focus the human and material resources to those elements of the facility that are detected as major risk or interest, fitting the assessment of the already considered risks.

The *main conclusions of the study* are shown below:

• In spite of the implementation of security plans for 10 years, not considered vulnerabilities do exist. Therefore, its analysis needs to keep adjusting.

• Nowadays, the risk assessment does not fit to reality in many cases, overestimating its negative evaluation or - on the contrary – valuing as limited risks that are not.

• The geographical location of the port on the shoreline can be determinant for what concerns 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.

• Future work will have to focus on producing a new formulation that considers the described indices in a comprehensive way.

Acknowledgment

Author thanks the Chief in Service of Coasts and Borders of the Guardia Civil General Directorate for its collaboration in the supply of the *Security Bulletins* as well as for his expert opinion about the target of the study.

Author thanks the Chiefs of Security of the Ports survey respondent for his cooperation.

Author thanks the experts who attended the call for provide their opinions to the initial results of the study.

REFERENCES

[1] Fine, W. T. "Mathematical Evaluations for Controlling Hazards", 1971.
[2] Romero. D. and Camarero, A. Science and Engineering Journal [Translation]. Vol. 35, No. 2, pp. 85-94, April-June, 2014.
[3] ISSN 1316-7081 "Review of the state of the art of risks assessment in port facilities"
[4] Dirección de Seguridad y Supervisión Aeroportuaria. Grupo Estudios y Proyectos de Seguridad Aeroportuaria. "Circular 4302-082-16.10, Procedimiento de Evaluación de Riesgo en Aeropuertos de Colombia", 2010.
[5] The Institute of Risk Management, UK. "A Risk Management Standard", 2002.
[6] Federal Ministry of the Interior, Germany. "Protection of Critical Infrastructures–Baseline Protection Concept", 2005.
[7] Ed Clarke & Don Philpott. "CARVER+Shock Vulnerability Assessment Tool, Longoat Place", Florida, 2011.
[8] The Institution of Engineering and Technology. "Infrastructure Risk and Resilience: Transportation". ISBN 978-1-84919-696-3, 2013.
[9] Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities, European Commission, "PT4: Generic Guidelines for Conducting Risk Assessment in Public Transport Networks", 2009.
[10] Utne, I. B. et al, "Risk and Vulnerability Analysis of Critical Infrastructures-The DECRIS Approach", 2008.
[11] Union of combined road-rail transport companies (UIRR). "Risk Analysis Guidelines for Combined Transport Terminals", 2007.
[12] European Commission. DELIVERABLE D2.3. "Integrated report on the link between Risk Assessment and Contingency Planning Methodologies", 2012.
[13] National Infrastructure Simulation & Analysis Center. "Fast Analysis Infrastructure Tool", 2011.
[14] Hunt, A. R., Kellerman, K. F. FAA Office of Civil Aviation Security. "Development of an Analysis Tool for Performing Civil Aviation Security Risk Assessment", 1998.
[15] International Labour Office (ILO) and International Maritime Organization (IMO). "Security in Ports. ILO and IMO Code of Practices", 2004.
[16] Sandi National laboratories." A Scalable Systems Approach for Critical Infrastructure Security", 2002.
[17] US Coast Guard." Navigation and Vessel Inspection. Circular N° 11-02 (NVIC 11-02)", 2003.
[18] Sanchidrian, C. "VIII Curso de Transporte Marítimo y Gestion Portuaria. La seguridad, el código ISPS y la legislación comunitaria", 2003.
[19] Gronalt, M., Häuslmayer H., Jammernegg W., Schindlbacher E., Weishäupl, M. "A risk assessment approach for inland container terminals", 2007.

David Romero-Faz is MSc Civil Engineering, MEng Logistics, Transportation and Road Safety (UNED) and University Expert in Shipping and Port Management (UPM). He is an Adjunct Professor in the Technical University of Madrid (UPM) from 2005. He has published two technical books as co-author and he has several communications in different national and international congress of engineering. He also has published several security articles in different technical journals. He also works as a consultant engineer in the port and transportation field working at this moment for ISDEFE, a public consulting company specialized in security which belongs to the Defense Ministry of Spain, He has been General Manager and Manager of different departments in mayor companies like *Eptisa Engineering and Services, INC Group or Consultrans Consulting.* At this moment he is finishing his doctorate.

Alberto Camarero-Orive is PhD Civil Engineering, Bachelor of Economics Bachelor of Administration and Business Management. He is Professor of the Technical University of Madrid from 2000 and adviser in Logistics, Maritime transport and Ports from 20 years ago. He is a researcher with more than thirty paper published in different international journals and he has also more than then books published in matters like transshipment, logistics and maritime transportation.