Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2016, 48 (120), 176–181
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/192

Received: 29.04.2016
Accepted: 02.12.2016
Published: 15.12.2016

Methodology for identification of potential threats and ship operations as a part of ship security assessment

Katarzyna Prill[1]✉, Marcin Szymczak[2]

Maritime University of Szczecin
[1] Education and Certification Department, [2] Ship Department
e-mail: {k.prill; m.szymczak}@am.szczecin.pl
✉ corresponding author

Key words: threats, security assessment, ISPS Code, terrorism, system, identification methods, safety of navigation

Abstract
This paper presents the development of a methodology for the identification of possible intentional threats and key ship operations that may be significant for a ship's security assessment, carried out by a Company Security Officer. The applicable international and domestic legal regulations regarding ship security systems are here analysed. Key factors and parameters that may provide support for the proper identification of realistic threats are also identified, giving practical relevance to this paper. The information reported here may be of support to those responsible for the development and revision of a ship's security assessment as it addresses an important part of the maintenance of navigational safety of ship operations under the provisions of the International Ship and Port Facility Security Code – ISPS Code.

Introduction

The adoption of the International Ship and Port Facility Security (ISPS) Code in 2002, which resulted from Conference Resolution 2 of the Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS), has led to an obligation for marine vessels to implement a system supporting security against intentional threats (IACS, 2008; UKMTO, 2011; IMB, 2016). An unlawful intentional act may be either a terrorist or a piracy act. An intentional threat is mostly defined as a use of force or violence against people or property in contravention of the law, aimed at intimidation and extortion on a group of people or country concessions to meet specific goals (Ślączka, Prill & Cieszyńska, 2010).

Legislative activities of the International Maritime Organisation (IMO) in regards to navigation safety improvement, including in particular an implementation of formal marine vessels' security systems, were a result of the events of September 11th 2001 (UKMTO, 2011). They led to the introduction of additional forces and measures improving navigation security, in particular in the areas specified as dangerous (e.g. the Somalia coast, the strait of Malakka) (Fernando et al., 2015; Knyazeva & Korobeev, 2015; IMB, 2016). The first part of this paper presents a legal analysis regarding maritime vessels' security systems, and also the legal requirements on ship security assessment, with respect to both domestic and international regulations (Stec, 2011). The second section of the paper refers to an identification process of key parameters, operations and factors that may affect a correct definition of threats. Therefore, this paper is of practical nature and may be of support for individuals responsible for the development and revision of ship security assessment as it addresses an important part of the maintenance of navigational safety of ship operations under the provisions of the International Ship and Port Facility Security Code – ISPS Code.

Ship security system with respect to domestic and international legal requirements

Under the Vienna Convention on the Law of Treaties (VCLT) of May 23rd 1969, each State adhering to the IMO is obliged to sign an international agreement, also known as a treaty, act or convention, respecting its provisions and implementing them into domestic law. The Republic of Poland, as a State belonging to the International Maritime Organisation and a Member State of the European Union, is obliged to comply with the requirements on ship security included in the following international acts:

1. International Convention for the Safety of Life at Sea concluded at London on November 1st 1974 (Journal of Laws of 1984, No. 61, Item 318 and 319 and of 2005, No. 120, Item 1016 as amended) along with the Protocol of 1978 relating to the International Convention for Safety of Life at Sea of November 1st 1974 concluded on February 17th 1978 (Journal of Laws of 1984, No. 61, item 320 and 321 and of 1986, No. 35, Item 177) hereinafter referred to as the "SOLAS Convention";
2. The International Ship and Port Facility Security Code (ISPS Code) adopted on December 12th 2002, Conference resolution 2 of the Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (Journal of Laws of 2005, item 1016) hereinafter referred to as the "ISPS Code";
3. Regulation No. 725/2004/EC of the European Parliament and of the Council of March 31st 2004 on enhancing ship and port facility security (O.J. WE L 129 209.04.2004, page 6; O.J. EU, Polish special edition, part 7, 7.8, page 74);
4. Directive No. 2005/65/EC of the European Parliament and of the Council of October 26th 2005 on enhancing port security (O.J. UE L/310/28 of November 25th 2005);
5. Commission Regulation (EC) No. 884/2005 of June 10th 2005 laying down procedures for conducting Commission inspections in the field of maritime security (O.J. UE L 148/25 of June 11th 2005).

The legal requirements included in the above mentioned international documents have been incorporated by the aforementioned Vienna Protocol to the domestic law. In the Polish legal system, provisions and requirements for the security system of ships may be found in the following documents:

1. The Ratification Act on the amendments to the International Convention for the Safety of Life at Sea 1974 SOLAS (Journal of Laws No. 2005.120.1016 of July 5th 2005);
2. The Maritime Security Act of September 4th 2008 (Journal of Laws No. 2016, item 49);
3. The Regulation of the Minister of Infrastructure of February 19th 2008 on the ship pre-arrival security information form (Journal of Laws No. 34, item 268);
4. The Regulation of the Minister of Infrastructure of February 25th 2009 on the form of declaration of security between a ship and a port facility (Journal of Laws No. 39, item 315);
5. The Regulation of the Minister of Infrastructure of February 25th 2009 on the forms regarding the Continuous Synopsis Record (CRS) for the ship and the list of last ports of call (Journal of Laws No. 39, item 314);
6. The Regulation of the Minister of Infrastructure of June 23rd 2009 on detailed activities and methods of actions for contact point designated to act upon receiving an alert and the requirements for the operation of alert systems (Journal of Laws No. 102, item 843);
7. The Regulation of the Minister of Infrastructure of November 5th 2010 on the transmission and information flow in the field of maritime security (Journal of Laws No. 217, item 1431);
8. The Regulation of the Minister of Infrastructure of November 17th 2010 on the list of prohibited items and substances and methods and means of securing the transport of weapons on ships (Journal of Laws No. 233, item 1529 as amended);
9. Regulation of the Council of Ministers of April 15th 2011 on the control methods and measures in the field of maritime security (Journal of Laws No. 93, item 539);
10. The Prime Minister Announcement of July 22nd 2015 on the publication of the consolidated text of the Regulation of the Council of Ministers on the procedure and method of co-operation of bodies in order to prevent threats to ships, port facilities and ports and related infrastructure, resulting from the use of ships or floating objects for terrorist attacks (Journal of Laws No. 2015, item 1139).

Ship Security System: goals and objectives

The goal of developing a ship security system is to identify and analyse potential threats that may occur with respect to a particular ship during its travel or

stay at a port, and to then implement activities that mitigate the threat. A key element of the entire security system is a company declaration stating that appropriate forces and measures shall be provided in order to perform basic ship security activities.

The basic tasks for the ship security system are (ISPS, 2004; Benny, 2015, pp. 41–42; Liwäng, Sörenson & Österman, 2015):

1. The prevention against unauthorised access on shipboard, in particular to special security areas.
2. The prevention against carrying weapons and other dangerous materials on board.
3. The prevention against smuggling drugs and other dangerous substances.
4. The prevention of sabotage, theft of goods or engineering solutions.
5. The protection of the ship and port facility against terrorist attacks, criminal assaults or threats caused by technical failures or natural disasters.
6. The establishment and implementation of procedures for responding to life or health-threatening situations of the shipboard personnel and any other individuals on board or at the port facility where the ship is berthed.

In order to complete the above mentioned tasks, the company, through the Company Security Officer – CSO, is obliged to verify periodically the actual state of the ship covered by the system, including (ISPS, 2004, A/8.4):

1. An identification of existing security measures, procedures and operations;
2. An identification and evaluation of key ship board operations that are important to protect;
3. An identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritize security measures;
4. An identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

Correct identification of the actual status of the ship security allows to indicate the steps that should be taken in order to systematically increase the ship's degree of security (Urbański, Margaś & Sprecht, 2008). An obligation to possess, develop and review periodically the Ship Security Assessment (SSA) for each ship belonging to the company, in fulfilment of the requirements of the A/8 of the ISIP Code and Art. 4, point 12 of the Maritime Security Act, dated September 4th 2008. This constitutes the grounds for drawing up a Ship Security Plan – SSP. The correct identification of threats with a high probability of occurrence on an assessed ship

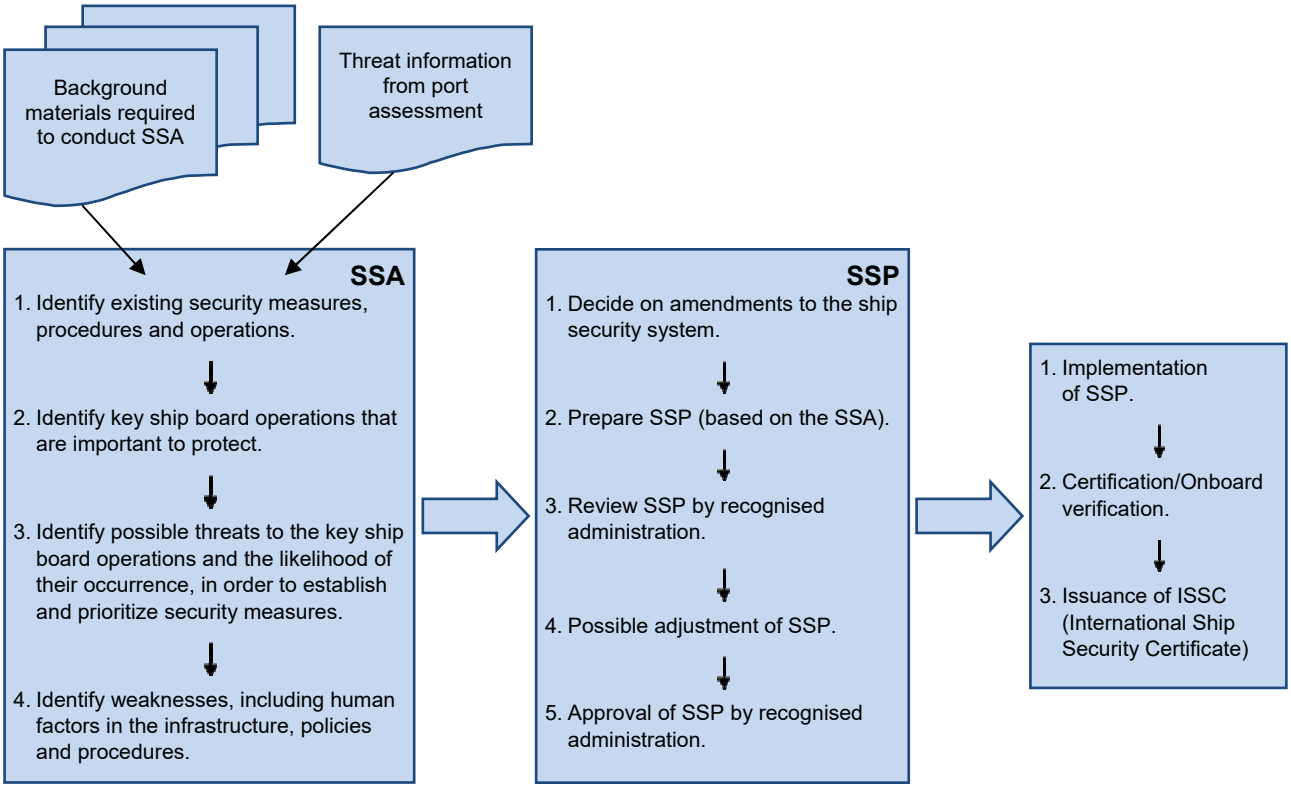

Figure 1. Mutual relations between SSA and SSP (based on NSA, 2012)

and the determination of key ship operations which may affect ship security should result when drawing up procedures and instructions that shall sufficiently protect a vessel against intentional threats.

The mutual relations between SSA and SSP are illustrated in Figure 1 (NSA, 2016).

Methods of assessment and review of SSA

The ship security assessment process is conducted periodically on the basis of the existing status, using methods such as FMEA, HAZID, and brainstorming (in contrast to the analysis of dynamic approach (Stróżyńska & Abramowicz, 2015)). It is divided into stages during which the Company Security Officer, on the grounds of the gathered information, identifies potential threats to the assessed ship and analyses the risk of their occurrence (Urbański, Margaś & Sprecht, 2008). The following steps of the ship security assessment process have been established (ClassNK, 2004; ABS, 2005).

Stage 1: Identification of the ship's characteristics and voyage areas.

Stage 2: Identification of possible threats and potential security risks for the ship and the crew (according to A/8.4.3, B/8.2 of the ISPS Code).

Stage 3: Identification and evaluation of key shipboard operations that are important to protect (according to A/8.4.1, A/8.4.2, B/8.3, B/8.6, B/8, 7, B/8.8 of the ISPS Code).

Stage 4: Identification of possible scenarios of threat to key shipboard operations and crew, and assessment of the likelihood of their occurrence (according to A/8.4.3, B/8.9, B/8.10 of the ISPS Code).

Stage 5: On-scene Security Survey (according to A/8.4.4, B/8.5, B/8.14 of the ISPS Code).

Stage 6: Re-identification of possible threat scenarios to key shipboard operations and crew and assessment of the likelihood of those occurrences (according to A/8.4.3, B/8.9, B/8.10 of the ISPS Code).

For the purpose of this paper, the first, second and third stages are subject to a detailed analysis.

Stage 1: Identification of the ship's characteristics and voyage areas

1. Prior to commencing the identification process of threats that may occur, with a specific probability, for the assessed ship, the vessel specification should be performed (Randić et al., 2015). The assessment should be conducted based on the criteria including, in particular: Design parameters of the assessed ship, voyage area and cargo description, legal requirements – When preparing for the identification process of intentional threats and key threats for the security of ship operations, one must pay attention to the parameters of the assessed ship. Apart from the ship design parameters, the knowledge of waters where the ship operates or will be operating in the near future is also very significant, as well as the specification of the type of cargo carried.
2. Characteristic factors for the ship requiring protection and possible weaknesses – It is necessary to report the devices and measures with which the ship is equipped by the company and the procedures applicable in the up-to-date operation. On the basis of this criterion, information should cover weaknesses in the field of the applicable procedures, infrastructure, crew qualifications and human factors.
3. External documentation providing information and affecting proper identification of threats and key operations of an assessed ship – During the threat identification process, the CSO should make use of, inter alia, the ship general arrangement plan, the list of restricted areas enumerated in the SSP and other spaces indicated in Chapter II-2 of the SOLAS Convention, including a description of every determined and potential access point to the ship as well as a list of key equipment for security purposes and safe ship operation, a list of exit routes and assembly points allowing for safe abandon of the ship. If available, all ship security procedures should be taken into consideration, including procedures regarding inspections, searches, people, supplies and property identification, monitoring, inspection of security equipment, alarms and access control.

Stage 2: Identification of possible threats and potential security risks for the ship and the crew

At this stage, the Company Security Officer should, based on the information gathered at the first stage, answer to the below questions to gradually determine the probability of occurrence of a threat (ClassNK, 2004):

1. Is there the existence of political (incl. religious, ideological, ethnical, nationalistic) threats that may affect the security of the ship, crew, or cargo? If so, what are the threats?
2. Does the ship operate in waters (enter ports) with unstable political situation? If so, which waters? What is the current political situation?

3. Can the ship, when staying in a port, be used to destroy/damage symbolic (historic) buildings/ structures?
4. Does the ship visit ports where mass events take place? If so, what kind of events?
5. Can the ship be used to damage ecologically important areas?
6. Does the ship itself possess a symbolic value?
7. Does the visibility or profile of the ship, company or brand represent a motive for unlawful acts?
8. Does the ship carry a special cargo? If so, what cargo?
9. Is it likely that terror related smuggling takes place from ports your ship is visiting?
10. Is it likely that your crew can take part in or embrace terror related smuggling? What are the ethnic characteristics of the crew? Are there any political – ethnic conflicts?
11. Does the ship operate in areas known for piracy?
12. Do the ship, cargo or passengers represent risk of hijacking? Can the ship damage infrastructure significant for industry and society?
13. Is the ship itself a critical infrastructure for society and industry?
14. Can the activities jeopardising ship security affect community safety and industry protection?
15. Can the ship be used as a means of threat and create fear in society?

Stage 3: Identification and evaluation of key shipboard operations that are important to protect

At the third stage, the subject of an analysis is the ship itself. The Company Security Officer should identify and specify the likelihood of an attack threat for every ship operation and its crew in the field of the procedures related with cargo loading, unloading or transportation and operations related with current ship operations (BV, 2003, Bichou, 2015). In order to identify correctly the operations affecting ship security, the CSO should take into consideration the following:

1. Control of access to the ship, ship spaces and rooms – the Company Security Officer should determine the security degree for the ship's structural elements such as: gangways, ladders, passages, corridors, platforms, doors, hatches, portholes, stairs, storage rooms for mooring lines and anchor chains, access to the ship from the sides, the bow, the aft, the storage room, loading equipment. The CSO should also identify every individual who is not a crew member and has an access to the ship rooms and spaces (company representatives, inspectors, technicians, guests, visitors etc.).
2. Limited access areas and restricted areas – the Company Security Officer should identify spaces that should be subject to a particular protection due to their function, and that would significantly affect the possibility of reacting to attacks if they were to be compromised. Such areas include, inter alia, the bridge, engine room, citadel, if present, emergency exit from the engine room, crew spaces, steering gear room, storage rooms, emergency power generator room, fire stations, battery rooms, air conditioning and fan rooms, storage rooms, anchor rooms, the Medical Room, hatches and access points to the air conditioning system and other specific for the assessed vessel.
3. Operations improving security – The Company Security Officer should identify equipment, systems, devices and procedures having an impact on the improvement of ship security. Such operations may include, inter alia, alarm procedures, drill schedule, monitoring systems, fire protection systems, signal systems, rescue systems, communication and alert systems, etc.
4. Deliveries and cargo management – Deliveries management should be understood as any operation related with loading and unloading cargo, ship storage and waste discharge from the ship. The CSO should determine the points where deliveries will be loaded and stored and waste discharged.

Conclusions

The ship security assessment process should be divided into stages at which the Company Security Officer, based on the gathered information, identifies potential threats for the assessed ship and analyses the risk of their occurrence. The identification of threats and key ship operations is a process that determines the development of the following elements of the ship security system against threats resulting in the deterioration of navigational safety. In order to complete successfully the security activities, specified by the international and domestic laws, the identification process should be comprehensive and cover the ship (its structure, equipment, systems, etc.), crew (trainings and engagement in the ship security process), transported cargo and the area where the ship operates. It must be noted that the above described identification process should be carried out individually for every assessed ship and should result in the development of appropriate procedures ensuring that ship security is maintained at a proper level.

References

1. ABS (2005) Guide for Ship Security (SEC) 3 ed. [Online] Available from: https://www.eagle.org/eagleExternalPortalWEB/ShowProperty/BEA%20Repository/Rules&Guides/Current/111_ShipSecurity(SEC)Notation/Pub111_ShipSecurity [Accessed: April 19, 2016]
2. Benny, D.J. (2015) *Maritime Security: Protection of Marinas, Ports, Small Watercrafts, Yachts and Ships*. CRC Press.
3. Bichou, K. (2015) The ISPS Code and the Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management. In: Haralambides H. *Port Management*. pp. 109–137.
4. BV (2003) *Ship security assessment – VentiSTAR, Maritime Division Ship in Service*. [Online] Available from: www1.veristar.com [Accessed: April 20, 2016]
5. ClassNK (2004) *Steps of Ships Security Assessment, ClassNK*. [Online] Available from: https://www.clasnk.org.jp [Accessed: April 19, 2016]
6. Fernando, D., Martinez, A., Sidoti, D., Mishra, M., Han, X. & Pattipati, K. (2015) *Context-based models to overcome operational challenges in maritime security, Technologies for Homeland Security (HST)*. IEEE International Symposium on Technologies for Homeland Security 14–15.04.2015. pp. 1–6.
7. IACS (2008) *Rec. No. 81. Guidance on the ISPS Code for Maritime Security Auditors*. [Online] Available for: www.iacs.org.uk/publications/publications.aspx?pageid=4&sectioned=5 [Accessed: April 04, 2016]
8. IMB (2016) *Violent attacks worsen in seas of West Africa despite global piracy downturn*. International Maritime Bureau report 27.04.2016. [Online] Available for: https://iccccs.org/icc/imb [Accessed: April 28, 2016]
9. ISPS (2004) Międzynarodowy Kodeks dla ochrony statków i obiektów portowych, przyjętym w dniu 12 grudnia 2002 r., Regulacja Nr 2 Konferencji Umawiających się Rządów – Stron Międzynarodowej Konwencji o bezpieczeństwie życia na morzu, 1974 r. (D.U. z 2005 r., poz. 1016), zwana „Kodeksem ISPS".
10. Journal of Laws (2008) Ustawa z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (D.U. nr 2016, poz. 49).
11. Knyazeva, N. & Korobeev, A. (2015) Maritime terrorism and Piracy: The Threat to Maritime Security. *Mediterranean Journal of Social Sciences* 6. pp. 226–232.
12. Liwäng, H., Sörenson, K. & Österman, C. (2015) Ship security challenges in high-risk area: manageable or insurmountable? *WMU Journal of Maritime Affairs* 14 (2). pp. 201–217.
13. NSA (2012) *Guideline for performing Ship Security Assessment*. p. 4. Norvegian Shipowners' Association. [Online] Available from: http://www.tradewindsnews.com/incoming/article262521.ece/binary/report%20report [Accessed: April 19, 16]
14. Randić, M., Matika, D. & Możnik, D. (2015) SWOT analysis of deficiencies on ship components identified by Port State Control Inspections with aim to improve the safety of maritime navigation. *Shipbuilding* 66 (3). pp. 61–72.
15. Ślączka, W., Prill, K. & Cieszyńska, K. (2010) Określenie potencjalnych zagrożeń dla terminali LNG na przykładzie terminala LNG w Świnoujściu. *Logistyka* 4. pp. CD–CD.
16. Stec, K. (2011) Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce. *Bezpieczeństwo Narodowe* 19, III. pp. 181–197.
17. Stróżyńska, M. & Abramowicz, W. (2015) A Dynamic Risk Assessment for Decision Support Systems in the Maritime Domain. *Studia Ekonomiczne* 165. pp. 295–307.
18. UKMTO (2011) *Best Management Practice for Protection against Somalia Based Piracy*. Livingston, Edinburgh: Witherby Publishing Group Ltd.
19. Urbański, J., Margaś, W. & Sprecht, C. (2008) Bezpieczeństwo morskie – ocena i kontrola ryzyka. *Zeszyty Naukowe Marynarki Wojennej* 2(173). pp.