ACT ABOUT SAFETY PROTECTION OF MERCHANT SHIPS AND PORTS OPEN TO INTERNATIONAL TRAFFIC AND ITS IMPLEMENTATION

Josip Kasum, Pero Vidan, Krešimir Baljak
Faculty of Maritime Studies in Split
Zrinsko-Frankopanska 38
21000 Split
jkasum@pfst.hr, pvidan@pfst.hr, kbaljak@pfst.hr

ABSTRACT

After tragic events occurred in the USA on 11th September 2001, International Maritime Organisation – IMO proposed to increase security measures for protection of ships and ports. Measures for security protection of ships and ports are determined by the International Ship and Port Facility Security Code – ISPS. ISPS code has been accepted as an amendment to the 1974 SOLAS Convention (Safety of Life at Sea) and has been obligatory since 1st July 2004. It does not refer to military ships, government ships and other government ships for non-commercial usage. ISPS code is obligatory for ships on international routes, and refers to:
- Passenger ships,
- Light passenger ships,
- Cargo ships,
- Fast cargo ships above 500 GRT and
- Mobile sea platforms.

Modern ships transporting oil, liquefied and natural gases, radioactive and poisonous waste, oil platforms, port terminals for hazardous substances, are all potential ecological bombs. Various technical and technological processes with hazardous cargo are performed in ports and terminals. The existing technical and technological achievements for increased security of people and the environment are partly or fully vulnerable to attempts of security threat. It is assumed that disturbances in such processes may lead to damages of the ports, surrounding settlements and cities. It is also assumed that the reason for the increased number of attacks is also the increased number of ships in traffic in countries which are not capable to prevent such threats by proper forces.

The implementation of ISPS code as a means against various threats has certain advantages and drawbacks, some of which will be presented in this paper and proposals for the improvement will be suggested.

Key words: security, terrorism, protection, suggestions for improvement

1 INTRODUCTION

Ships and ports which are obliged to implement ISPS code have to satisfy the following: legal regulations of the signatory countries of convention of the State of the port, requirements of the shipping registry, requirements of local authorities, port authorities, concessionaires, etc. Obligations of the State of the ship refer to respecting the ISPS code recommendations while undertaking the necessary measures on the ship. This particularly
refers to declaring the security level on ships and ports, to advising about defence and to protection of the jeopardised ports and ships. The obligations of the ship operator refer primarily to the obligation of designing an adapted ship security plan coordinated with the captain of the ship. It must not be in collision with the Convention about protection of life at sea. Also, a person must be in charge of implementation of the plan and communication in case of the threat to the ship, which is a person responsible for security protection of the company (Security Officer – CSO). They will cooperate with Ship Security Officer – SSO. The government obligation is to entrust an individual responsible for the Port Facility Security Officer – PFSO. The duty of PFSO is to cooperate with SSO to achieve better implementation of the security protection of the port and the ship. The Ship Security Plan – SSP includes the layout of the ship with critical security points, presentation of the areas with restricted access to unauthorised persons, lightning system of the ship, security number of the ship, data about the ship security officer, plan and procedures of protection, etc. Also, social obligation is to supply the ship with obligatory security equipment of the ship:

- Automatic Identification System – AIS, and
- Ship Security Alert System – SSAS.[8]

AIS device emits data about the ship through Very High Frequency – VHF radio waves. The data refer to: ship's security number, name of the ship, State of the ship, port of departure, port of destination, estimated arrival time, number of the crew, etc.

Security warning system is obligatory for all ships required so by 1st July 2006. This silent alarm is emitted from the ship to the coast. Security alarm system is located in the position known to the captain of the ship and to the Ship Security Officer. A ship may also be equipped with non-obligatory equipment: metal and explosive detectors, monitoring video cameras and security high-voltage fences.

Implementation of ISPS has demonstrated different results. Some practical experiences and suggestions for the improvement have been presented further in this paper.

2 LIABILITIES OF THE SHIP SECURITY OFFICER AND PROCEDURE IN CASE OF SECURITY THREAT

The ship security officer shall announce the arrival of the ship in the port not later than 24 hours prior to the arrival. In the shortest possible period after the arrival they shall contact the person in charge for the security of the port, exchange the data about security level, provide data about the ship and the crew, etc. The ship security officer shall proclaim the security level of the ship in accordance to the security level of the port. Depending on the expected events or expressed doubts about possible security danger the officer may change the security level. They shall inform about it the Company security officer and the Port security officer. They shall also organise the following: monitor the access to the ship, control embarkation of people and their effects, identification of persons and inspection of visitors’ personal belongings aimed at minimising the risk of taking weapons and dangerous substances onto the ship which may endanger the security of the crew, the ship and the port, control of the areas with access allowed to authorised persons, control of the deck and the area surrounding the ship, control of cargo and cargo hold manipulation, communication among the crew aimed at better control of security, drills pursuant to the security plan and testing of the ship security equipment, etc.

Nowadays, piracy is becoming more widespread. The objective of piracy is to hijack the valuable part of the cargo or all the cargo together with the ship, potentially with consequential casualties (Figure 1). ISPS determines the procedure in case of security threat trying to avoid danger for the crew. [7]
ISPS defines course of actions of the crew in case of terrorists’ or pirates’ attack to the ship, aimed at reducing the threatening danger. In such situation the ship security officer shall raise security level. If there is an indication of security threat, the security level will be raised to the second level and PFSO and CSO will be informed. The crew shall act in accordance to the rules about searching the ship and restricting the access to areas of restricted access for unauthorised persons. If there is a security threat, attack or similar, the security level will be raised to the third level.

If the ship is in the port the crew will have to be mobilised and PFSO and CSO will be informed about the situation. If the ship is at sea CSO shall inform the coastal bodies using the alarm system or a nearby ship via AIS system. All actions are to be recorded in the Security log. ISPS determines that actions of the crew are not risky for their own lives. When seizing the ship, pirates and terrorists usually engage qualified men (captains and officers), who are capable to operate the ship without its crew, and each resistance might result in casualties. It is also recommended to communicate with terrorists, and possibly try to
discover their further plans and their identity. Briefly, it is necessary to do everything to protect human lives.

3 SECURITY AT SHIPS

According to the Standards of Training Certification and Watchkeeping – STCW, the crew, the company (ship operator) and port authorities need to meet up and perform drills aimed at protection and prevention of the risks. The ship, the port and the state have to respect the standards, means and methods of implementing ISPS.

3.1 Security at ships and rescuing human lives at sea

In the present situation of lowered tariffs, the implementation of improved security of ships and port facilities create additional costs. They also refer to the acquisition of new equipment, e.g.: AIS, SSAS, video surveillance, voltage fence on ships, and in ports: video surveillance, port radars, AIS receivers, security service, metal detectors, explosive detectors, devices for controlling the cargo, etc. Introducing the ISPS affects the increase of the crew and personnel engaged in control and supervision of cargo and access to the ship.

In order to lower the ship operator's costs for the new requirements, ISPS code has been accepted without the increase of the minimum number of the crew. Obligatory devices are now: AIS, security alarm system, and in some types of ships like RO-RO and passenger ships, also video surveillance.

It is assumed that most part of the implementation tasks are performed by mariners. Along with the minimal number of the crew and increased volume of work in the ship’s operation, they have additional tasks.

3.2 Implementation of the ISPS security plan

A group of measures for providing security protection of ships and port facilities have been determined by the Ship security plan. The Ship security plan consists of: the layout of the ship with critical security points, areas with restricted access to unauthorised persons, lightning system of the ship, security number of the ship, data about the ship security office, protection procedures and plan, etc. Because of its importance, the document is secret and is not liable for inspection. The flag State, the shipping registry as the authorised representative of the state for ISPS code implementation, CSO and SSO are responsible for the implementation of the ISPS ship security plan. Only authorised persons, i.e. the crew, has access to the restricted areas. Visitors may have access to the restricted areas only if accompanied by members of the crew. [4]

In practice it is sometimes exaggerated when marking the restricted access area. In fact, it is considered that there is little possibility for security threat arriving from such areas. Restricted areas in the ship should be the bridge, engine room, pumping room, etc. However, sometimes not dangerous areas are categorised as restricted area: kitchen, superstructure rooms, ventilation openings, storeroom for toiletries, ship offices, storage for ropes and tools, cargo holds in general cargo ships, etc.

3.3 Control of entering/leaving the ship

According to the ISPS one member of the crew is liable to be on the gangboard and monitor entrance and exit of persons with personal luggage, and pay attention that weapons and dangerous substances are not brought aboard.
However, the minimum number of the crew is not able to control simultaneously entrance/exit from the ship and cargo handling. Furthermore, the member of the crew on the gangboard is not armed. Mariners are not obliged to be trained for using arms, and there is no safe method of disarming a terrorist. Official visitors like government and administrative bodies’ officials, police and customs officers, and coastal guard regularly wear official arms. According to the ISPS code they should not have it on board, and according to their national and professional regulations, they are not to leave the arms with an unauthorised person like a member of the crew on the ship’s gangboard.

During cargo manipulation dockers’ identity and personal items have to be controlled when entering and leaving the ship. In this way the time of stay of the ship in the port is increased. It is not uncommon that crew members in charge of the control of entrance/exit let dockers onto the ship without detailed control, in order to decrease the delay as requested by the shipper or ship operator. This problem is known to port authorities and it may happen that inspectors disguise as dockers and enter the ship unnoticeably. The failure to implement security procedures is presented to the captain who is then charged for maritime violation.

3.4 Non-Convention ships and ISPS

ISPS code does not refer to non-Convention ships and ships for transportation of passenger and cargo, for economy, sports and entertainment, under 500 GRT. One of the reasons for that is a high number of such ships and impracticality (unprofitability) to control them. However, because of their great number and absence of security procedures, such ships are potentially highly dangerous (Figure 2).

Merchant navy ships under 500 GRT are exempt from pilotage, and may approach, almost without any control, the port facility or its threatened parts, like oil terminals, chemical terminals, liquefied and natural gas terminals, terminals for hazardous substances, etc.

![Figure 2: Share of Convention and non-Convention ships in the Republic of Croatia [3]](image)

As of 2004, the system of separate navigation in southern, middle and northern part of Adriatic has been introduced. All ships above 500 GRT have to navigate according to the system of separate navigation. Navigation without pilotage along the Middle channel has been forbidden for all ships above 500 GRT and for all ships with hazardous cargo. In this way the coast, e.g. national park Kornati, has been safeguarded both from ecological and security aspect.

Control of the ships above 500 GRT can also be done by AIS device through the Maritime Rescue Coordination Centre – MRCC in Rijeka. The problem is the control of non-Convention ships, which are not obliged to install AIS device, especially because of the increase of their number in summer. Such ships navigate all over the world without port authorities’ awareness about the purpose and method of their navigation. [2]
3.5 Equipping ships with security equipment

In order to facilitate the control, ships are equipped with minimum equipment for inspection and control. Such equipment is standardised according to its type, efficiency and quantity. Passenger ships and RO-RO ships are obliged to have AIS device, security alarm system and video surveillance. Metal detectors are not obligatory for the control of entrance/exit from the ship. However, metal detectors ensure faster and easier control of clothes and personal luggage of visitors. Detectors for explosives are not new, and their use detects the degree of explosiveness of suspicious objects. A number of such detectors on the ship should be determined. ISPS code introduced ID cards in use on ships. ID cards contain the name of the holder with or without a photograph. The guard on the ship is authorised to request other identity documents from the ID card holder. The information about the person entering the ship is recorded in the ship’s entrance/exit log.

3.6 Proposals for improvement

A set of measures are proposed relating to:

- Security of the ships and rescue of life at sea,
- Implementation of ISPS security plan,
- Control of entrance/exit from the ship,
- Non-Convention ships and ISPS, and
- Safety equipment of the ship.

In relation to the security on ships it is necessary to propose to engage trained personnel and services aimed at protection of ships, crew and cargo during their stay in the port. What is recommended is that security personnel are authorised to be armed and to use force for the purpose of improving security. The services should be organised by port authorities, with or without corresponding fee. It is expected that the mariners would engage in handling cargo, that is, in jobs they are qualified and trained for.

In relation to the implementation of ISPS security plan, it is proposed to define critical points on the ship, i.e. the restricted access areas. These areas refer to important points, like: the bridge, the engine room, the valve room, the room for cargo operations, for fuel operations, areas with hazardous material, like paint locker, storage for inflammable chemical substances, rooms with access to probes, water tanks and fuel tanks covers, etc. The areas of restricted access have to be monitored and locked in ports. It is necessary, however, that because of security, protection of life at sea is jeopardised. Ventilation openings, emergency exits, entrance and exit points from ship’s superstructure, rooms with instructions for quick shutting of fuel valves, switches for stopping engines, parts of ship for evacuation or for fire protection, etc., must not be locked, but have to be accessible at any time.

Control of entrance and exit from the ship and safeguarding of the gangboard and other monitoring tasks could be transferred to port security services, that is, to personnel trained for handling arms and guarding property. Every port should engage the guard immediately upon the arrival of the ship. The number of the guard personnel would depend on the size and purpose of the ship, and the number of the crew and passengers.

For non-Convention ships ISPS code should be applied in its modified version, as has already been proposed by some authors [3].

By implementing AIS devices and ISPS code procedures to non-Convention ships, which means to all ships except the military ships, government ships, and ships for public purposes, a number of unidentified vessels would be decreased, control of coastal and port traffic
would be easier and security threat would be lowered. Moreover, AIS could be used for easier locating of ships in distress. ID cards should be obligatory for the official visitors to the ship, for instance, for port authority personnel, dockers, agents, etc. ID cards could use the technology of integrated circles and optical readers. This will allow automatic acquisition of information about the person and a record in the device memory. In this way the number of forged ID cards would be lower, as well as the time needed for identification of the visitor to the ship. For the purpose of better and faster control the ships should be equipped with metal and explosive material detectors and with batons as a repressive means. They should be kept locked and their use should be monitored by the captain and CSO. The crew would use them when necessary, for instance, when searching the ship looking for stow-away, possible attackers and the like.

4 SECURITY OF THE PORTS

The current trend in maritime transportation is the increase of larger ports and the decrease of smaller ports. Larger ports are more easily controlled in relation to smaller, often scattered ports. Each port for international traffic is strictly controlled for various reasons, e.g. for emigration or immigration of people, various smugglers, thefts of cargo and inventories. By applying ISPS code the regime in ports have become more rigorous. The same as ships, ports are also required to have the security plan, meet the requirements, have PFSO.

![Figure 3: SAIC vessel for protection from terrorist attacks in the port](image)

New control devices in the ports are video surveillance, surveillance of traffic by integrated use of port radar and AIS device. Some ports perform the control of people and goods at entrance/exit points. Such control complicates the traffic of the port as there is time delay in operations, huge crowds and lower productivity of the port. In order to implement ISPS code some other ports use specially trained unit in the situation of a terrorist act or third security level. Special units are trained how to deal with explosives, and use robots or armoured vessels for deactivation of explosive devices (Figure 3).

In order to simplify control of personal luggage and smaller cargo at the entrance to the port, detectors for metals and explosives should be included in the port equipment. The devices should be standardised, and IMO should recommend their number in accordance to the size of the port and the number of its entrance/exit points. Most difficult is the control of loading and unloading of cargo in container traffic. Some ports are already applying the latest technical achievements in the control of such cargo.
For instance, X-rays are used in X area. One of the devices used for detecting the content of the cargo like metal, explosives, dangerous substances, etc., is Mobile VACIS system (Figure 5). This system scans the content of the container in several radiographic images (Figure 4). The average scanning time is 6 seconds for a 40 ft. container. There is possibility of fast scanning and of recording information. One of the new systems is ICIS system (Figure 6), positioned at the exit point of the port. It can produce multiple scanning of radiographic images, also in combination with optical reader (OCR) (Figure 7). The device may be used for monitoring the traffic and the content of the container goods in the port. SAIC Mobil VACIS system may be combined with OCR system to determine the radiation level of the interior of the container [11].

Financially more suitable form of such system is the scanner of empty containers. It can raise alarms when containers are not totally empty, as presented in the accompanying documents.
5 MARITIME VIOLATIONS

All ships obliged to apply ISPS code failing to do so will commit a maritime violation. The obligation of the captain and SSO is to organise and train the crew, and to equip and protect the ship. This refers to the control of the officer on duty on the gangway in the port, whose duty is to identify the visitors and crew members, and their personal belongings at ship’s entrance/exit points. Their duty is also to control proper loading and unloading of the cargo in the port, and security aimed at protection from security threats. It is necessary to monitor all access to the ship and areas with restricted access, i.e. the areas suitable as shelter for attackers. Non-observation to the described procedures in the ports is also considered as maritime violation. Ship security equipment has to be in working order and in good condition. AIS has to be properly installed and be constantly working, and emitted data need to be updated. Lightning, marking and control of the restricted access area have to be in compliance with SSP. Security log has to be kept regularly. Both security log and SSP are considered as secret and are not subject to inspection. If the competent inspection bodies assume that the ship does not have SSP and that it does not observe ISPS code, the inspection may be requested with prior agreement with the captain. The Ship security officer shall keep the SSP in a safe location, if possible in the ship’s safe-deposit box. Port authorities need to be informed about the arrival of the ship 24 hours before through the Pre Arrival Report. Failure to observe the procedure shall be considered as violation. All restricted access areas have to be clearly marked, and during the stay in the port the gate have to be locked and monitored. The security number needs to be clearly visible and written in a contrast colour on the superstructure and on the body of the ship. All digits and letters have to be welded or carved. The crew has to be trained, introduced to the procedure and the SSO of the ship, and to the CSO in charge of the ship, and informed about their phone numbers.

6 THE PORT OF SPLIT AND PROPOSALS FOR IMPROVED IMPLEMENTATION

The port of Split is international port for passenger and cargo traffic. Gradska luka (City port) is aimed for passenger traffic, while Sjeverna luka (Northern port) is designed for cargo traffic. Sjeverna luka consists of several terminals: grain terminal, bulk cargo terminal, oil terminal in Kaštela, cement factory in Kaštela and Adriavinil in Kaštela. The port of Split has annual increase of both passenger and cargo traffic. The increase of traffic requires increasing security of the port in terms of better organisation and technical equipment. The passenger port has video surveillance of passengers and vehicles. A great number of non-Convention ships enters and departs from the port of Split and thus make it vulnerable in terms of security. With current equipment of the port such ships may approach the coast almost unobserved. The port of Split does not have adequate lightning system. Unlike exceptionally well lit passenger port and its video surveillance, Sjeverna luka does not have video surveillance nor adequate coast lightning. Inadequate lightning is dangerous for ships in terms of life protection at sea, especially at entering and departing, but also in terms of security, because ISPS code requires lightning of ships and port facilities. It is proposed to introduce security and special units in the cargo port. Security unit would perform regular control of people and goods at the entrance and exit points of the port, and protection and control of people at the entrance and exit of the ship. Special unit would provide direct protection during terrorist attacks and take active participation in case of raising security level to level 2 and 3. Special unit should provide service to both passenger and cargo ports. The cargo port should have video surveillance and use metal and explosive detectors, and optical ID readers. It is considered that VACIS or ICIS systems are
indispensable for container/RO-RO terminal, in order to reduce the possibility of arms smuggling, human trafficking and harmful substances in containers and trucks.

It is proposed to implement adapted ISPS code to non-Convention ships, with parallel implementation of AIS system [3]. Non-Convention ships are exempt from pilotage. Since the port of Split has several critical security points, like, for instance: oil terminal, Adriavinil terminal, it is necessary to make some advancement in order to improve the control of the traffic in the port. Therefore, for better control of ships and traffic management, radar, combined with AIS system, should be obtained for security and attack protection.

For the purpose of port protection and shorter time for identification of persons, it is proposed to install optical or similar reader of seaman’s books in international ports obliged to implement ISPS code. Such a reader would be more efficient in interpreting and identifying data contained in seaman’s book.

Besides control of the cargo in cargo ports, it is necessary to extend control of passengers and vehicles in passenger ports. Similar to air traffic, the tickets for persons and vehicles should be issued in the name of the person or the owner of the vehicle. The tickets would be bought upon presenting an ID, and using an optical or similar reader and a computer, the data would be directly entered into the ticket and remain recorded in the computer memory.

CONCLUSION

After 11th September the security level was raised in all aspects of traffic, and such a tendency did not exclude ships and port facilities. They appeared to be the areas subject to terrorist attacks. Relatively large areas of ports and terminals are a demanding effort for the organisation of security protection. Ships for special cargo have been produced to serve people. However, no producer of such ships took into account protection from a terrorist attack. ISPS code introduces new procedures in ports and ships aimed at raising security level. ISPS can be adapted to the situation in the field. Many ports have not reached the level of development to implement ISPS code.

For the purpose of better general protection it is necessary to recommend obligatory equipment of ships, and reassign a part of obligations to coast personnel. This would increase the costs of ships and ports, but with the justified objective of increased security.

The present situation and mariners acting as “policemen”, accompanied by more difficult ordinary tasks have made mariners’ everyday tasks too demanding.

REFERENCES

4) ISPS Code, IMO, 2003
5) http://sms.classnk.or.jp/ispshp/html/pdf
6) http://www.iho.org
7) http://www.imb.com
8) http://www.imo.org
11) http://www.saic.com