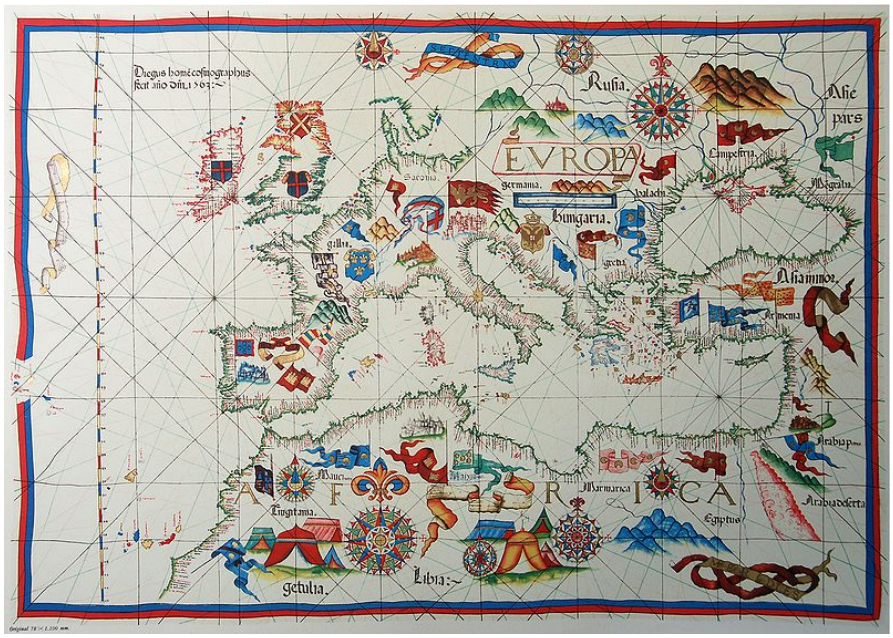
Welcome to the World of Shipping



2010 Annual Conference of the International Association of Maritime Economists, Lisbon 7-9 July 2010

THE APPLICATION OF SIX SIGMA PRINCIPLES IN MARITIME PORT SECURITY

INTERNATIONAL ASSOCIATION OF MARITIME ECONOMISTS

CARGO Edições, Lda

THE APPLICATION OF SIX SIGMA PRINCIPLES IN MARITIME PORT SECURITY

Risto Talas
Cass Business School, City University London
106 Bunhill Row, London, EC1Y 8TZ
United Kingdom
Email: Risto.talas@virgin.net
Telephone: n/a
Fax: n/a

David A. Menachof [1]
Peter Thompson Chair in Port Logistics
Logistics Institute, Business School
The University of Hull, Kingston upon Hull
HU6 7RX, United Kingdom
Email: d.menachof@hull.ac.uk
Telephone: +44 (0)1482 347527
Fax: +44 (0)1482 463484

ABSTRACT

The paper will examine the principles behind Six Sigma as described by Pyzdek (2003) and create a conceptual model in which they can be applied in the field of maritime security, specifically for ports and port terminals. It will be shown that contemporary port security initiatives such as the International Ship and Port Facility Security (ISPS) Code can be adapted to accommodate Six Sigma principles and the conceptual model will demonstrate how an ISPS Code compliant terminal can measure the improvement in the performance of its security systems. Pyzdek (2003) describes Six Sigma as "a rigorous, focussed and highly effective implementation of proven quality principles and techniques." It is based on the define-measure-analyse-improve-control methodology which was pioneered by Motorola in the 1980s. Some particular features of Motorola's programme were:

- Goal-deployment of business objectives to process objectives
- Strong project-management of process-improvement activities
- Emphasis on visibility of financial benefits of improvement

The literature shows only one example of the application of Six Sigma principles to port security. Ung et al (2007) demonstrate an application of Six Sigma to port security process control. Their project case is the security process of the delivery of ships stores from the gate of a port terminal to alongside the ship. They defined the measuring unit critical to quality to be the time taken in the process and deemed the security process as unacceptable if performance exceeded 50 minutes. While the authors perceived their contribution to be useful, they failed to create a comprehensive model for all of the significant aspects of the ISPS Code. These omissions will be addressed in this paper. The paper concludes with recommendations to port terminal operators regarding implementation of the method.

Keywords: Six Sigma, Port Security, ISPS Code, Port Performance

1. INTRODUCTION

The paper applies the principles behind Six Sigma to create a conceptual model which can be used to assist port facilities to ensure compliance with the ISPS Code and introduce a framework for continual improvement in port security. The paper begins with a brief examination of the literature on Six Sigma followed by a discussion on port security, including

[1] Author for correspondence and presenting the paper

proposals for new definitions of port security, port security management and port security risk. Subsequently, the conceptual model is presented to show how Six Sigma principles can be used by ISPS Code compliant port facilities to measure the performance of their security processes in the Six Sigma framework.

2. SIX SIGMA

Pyzdek (2003) describes Six Sigma as a rigorous, focussed and highly effective implementation of proven quality principles and techniques. It is based on the define-measure-analyse-improve-control (DMAIC) methodology which was pioneered by Motorola in the 1980s (Sodhi and Sodhi, 2008; Denton, 1991; Kumar and Gupta, 1993; Dambolena and Rao, 1994; Hendricks and Kelbaugh, 1998). Some particular features of Motorola's programme were:

- Goal-deployment of business objectives to process objectives
- Strong project-management of process-improvement activities
- Emphasis on visibility of financial benefits of improvement

The achievement of Six Sigma goals relates to reducing variability of manufacturing or service processes to 3.4 defects per million opportunities (Sodhi and Sodhi, 2008; Linderman et al, 2003). Processes that produce more than 3.4 defects per million occurrences have lower levels of Sigma, thus:

- 2 Sigma = 308,537 defects per million occurrences
- 3 Sigma = 66,807 defects per million occurrences
- 4 Sigma = 6,210 defects per million occurrences
- 5 Sigma = 233 defects per million occurrences

Nonthaleerak and Hendry (2006) conducted a literature review of over 200 papers in Six Sigma research and classified the Six Sigma literature in terms of research contents and research methods; the research contents being sub-divided into implementation focus and methodology focus. Northaleerak and Hendry (2006) reviewed the implementation of Six Sigma in the non-manufacturing sectors (Taghaboni-Dutta and Moreland, 2004; Dasgupta, 2003; and Wang et al, 2004) combined with the use of Critical Success Factors (Voehl, 2004; Lynch et al, 2003; and Brewer and Bagranoff, 2004). Northaleerak and Hendry (2006) state that while current research into the identification of critical success factors (CSFs) in Six Sigma may be sufficient, more empirical research is required.

Nakhai and Neves (2009, p670) state that the central contribution of Six Sigma philosophy is the fact that variation of the operation can have a significant impact on the whole of the process, which is often interrelated in nature.

Dasgupta (2003) applies six sigma methodology to measure and improve supply chain performance by creating a six sigma framework for supply chain management involving supply chain network mapping and specifying the critical characteristics for the stages in producing defect-free products.

2.1. Six Sigma and Port Security

The literature shows only one example of the application of Six Sigma principles to port security. Ung et al (2007) demonstrate an application of Six Sigma to port security process control. Their project case is the security process of the delivery of ships stores from the gate of a port terminal to alongside the ship. They defined the measuring unit critical to quality to be the time taken in the process and deemed the security process as unacceptable if performance exceeded 50 minutes. They carried out 100 simulations and the mean (42.39 minutes) and standard deviations (8.56 minutes) of the times calculated produced 186,700 defects per million opportunities (DPMO) which equates to a process sigma metric of 2.4. However, the value of their research is questionable because neither the analysis of the root

cause and identification of solutions, nor the improvement of the process nor control of the process were addressed in their paper. Nevertheless, the literature on the application of Six Sigma in supply chain security is sparse and it is proposed that this research addresses this gap.

3. PORT SECURITY

Given that ports are considered nodes in a supply chain network (Yap & Lam, 2004), it is necessary when proposing a new definition for port security to examine the literature on supply chain security (SCS). Williams et al (2008, p256) state that few formal definitions can be found in the literature and draw their definition of SCS from Closs and McGarrell's (2004, p8) definition of SCS management. The Closs and McGarrell (2004, p8) definition is: "the application of policies, procedures and technology to protect supply chain assets (product, facilities, equipment, information and personnel) from theft, damage, or terrorism and to prevent the introduction of unauthorised contraband, people or weapons of mass destruction (WMD) into the supply chain." In pursuit of a definition of port security it would be easy simply to substitute 'port' for 'supply chain'. However, this would not distinguish between port security and port security management, in the way that Williams et at (2008) do not distinguish between SCS and SCS management. Furthermore, this would limit the definition simply to the port's assets and exclude cargoes and, specifically, the ship-port interface which the ISPS Code seeks to protect. Also, the Closs and McGarrell (2004) definition is in some ways too specific in its reference to terrorism and weapons of mass destruction given that by naming threats they run the risk of excluding others such as sabotage or criminal damage arising from strikes and riots by locked out workers (see Miller, 1994, p452 for a fuller description of named threats to ports covered by marine insurance). The ISPS Code does not single out terrorism as a threat per se but refers to measures which provide protection from security incidents (which include terrorism), while the MTSA refers specifically to the threat of terrorism in the maritime domain. This is understandable given that the MTSA was drafted in the United States in the wake of the attacks on 9/11. However, the MTSA focus on terrorism also potentially excludes other forms of unauthorised acts such as maritime fraud, which is included in Regulation (EC) No. 725/2004. Furthermore, the focus on WMD appears to be centred more on the United States, specifically in consideration of containerised trade (Harrald et al, 2004; Gerencser et al, 2003).

Therefore, it would be appropriate to amend the named threats in the Closs and McGarrell (2004) definition to 'unauthorised acts', which is wider in scope. 'Unauthorised acts' is chosen in preference to 'illegal acts' in order to avoid any confusion arising from differing definitions of legality between jurisdictions.

The proposed definition for port security is: the absence of and/or the perception of the absence of threat to port assets, cargoes and the ship-port interface from unauthorised acts. From this, it follows that port security management is: the application of measures (personnel, procedures and technology) to reduce the threat and/or the perception of threat to port assets, cargoes and the ship-port interface from unauthorised acts. The choice of words is significant for while it may be preferable to try to eliminate threats rather than to reduce them, it will never be possible to eliminate all security threats absolutely (Price, 2004, p335).

3.1. Port Security Risk

As risk is present in all walks of daily life, it is logical that an extensive literature exists on the subject. Whether considering individuals' attitudes to risk and decision making under uncertainty (Kahnemann and Tversky, 1979), or risk as a factor in decision making (March and Shapira, 1987), the interpretation of risk varies from person to person. Definitions of risk

also vary according to the discipline in which the discussion is framed, be it supply chain (Rao and Goldsby, 2009; Christopher, 2005; Juttner et al, 2003; Zsidisin et al, 2004; Chopra and Sodhi, 2004), supply chain security (Williams et al, 2008), port security (Bichou, 2004, 2007; Talas and Menachof, 2009), terrorism (Sheffi, 2001; Woo, 2003; Raymond, 2006; Price, 2004, Greenberg et al, 2006), sociology and psychology (Heimer, 1988) or more established disciplines such as economics, finance or management (Juttner et al, 2003). Rao and Goldsby (2009) present selected definitions of risk from the literature including from Lowrance (1980) "risk is a measure of the probability and severity of adverse effects" and Yates and Stone (2002) "risk is an inherently subjective construct that deals with the possibility of loss."

Definitions of risk relevant to this paper can be found in Robinson (2008), March and Shapira (1987), Bedford and Cooke (1996), Markowitz (1952), Broder (2006), Greenberg et al (2006) and Price (2004). Robinson (2008, p182) describes risk from a security perspective as "the probability that harm may result from a given threat." March and Shapira (1987, p1404) review managerial perspectives on risk and risk taking and define risk as "reflecting variation in the distribution of possible outcomes, their likelihoods and their subjective values." Bedford and Cooke's (1996) analysis of probabilistic risk analysis describes risk as having two particular elements: hazard and uncertainty. Markowitz (1952, p89) describes risk as "variance of return." Broder (2006, p3) describes risk as "the uncertainty of financial loss, the variations between actual and expected results or the probability that a loss has occurred or will occur." Greenberg et al (2006, p143) state that terrorism risk "does not exist without existence of threat, the presence of vulnerability and the potential for consequences." Price (2004, p335) claims that ports (in the context of terrorism) are actually faced with uncertainty, not risk because uncertainty implies that while the range of events is known, the associated probabilities of each type of event are not. To an insurance underwriter, risk can represent not only the vessel, aircraft or property under consideration for insurance (Broder, 2006, p3) but also the product of the probability of the occurrence of an insured event and the financial consequences of such an event. Drawing on this distinction and the definitions by Robinson (2008), Broder (2006) and Bedford and Cooke (1996), the proposed definition for port security risk is: the product of the probability of a threat to port assets, cargoes and the ship-port interface which may give rise to a loss and the size of the financial consequences that might follow.

3.2. Port Security Risk Management

Williams et al (2008) present a comprehensive overview and research agenda for supply chain security. They categorise the literature into four organisational approaches to supply chain security: an intra-organisational approach, an inter-organisational approach, a combination of the two and an ignore approach. In the intra-organisational approach they discuss the security processes and technology used by companies to secure their supply chains and the scope for adopting a total quality management (TQM) or Six Sigma philosophy. The inter-organisational approach is focussed on organisational relationships with other supply chain members, public entities and competitors and some key contemporary supply chain security initiatives are listed. Furthermore, they propose an update to the Juttner et al (2003) model for supply chain risk management by adding an additional dimension to supply chain risk mitigating strategies which includes three of the above approaches (intra-organisational, inter-organisational and combination) to supply chain security. As this paper is concerned with ports which have adopted the risk mitigating strategies as set out in the ISPS Code, it is just as appropriate to frame the discussion on port security risk in Juttner et al's (2003) original four constructs of supply chain risk management: supply chain risk sources, risk consequences, risk drivers and risk mitigating strategies. However, the discussion begins by considering some methodologies for port security risk assessment.

3.3. Port Security Risk Assessment

Bichou (2009, p116) describes the process of risk assessment as "the assessment of risk in terms of what can go wrong, the probability of it going wrong and the possible consequences." Drawing on the system safety literature he states that "the empiricist approach is to regard accidents as random events whose frequency is influenced by certain factors" and that under this approach the cause of an accident is a hazardous event. Bichou (2009, p117) classifies the major hazard analysis tools as either sequence dependent or independent and following either consequence or cause analysis (see table 1).

Table 1 – Major hazard analysis tools

	Consequence analysis	Cause analysis
Sequence dependent	Event Tree Analysis	Markov Process
Sequence independent	Failure Modes and Effects Analysis	Fault Tree Analysis

(Source: Bichou, 2009)

Event tree analysis (ETA) and Failure Modes and Effects Analysis (FMEA) are two forms of hazard analysis which analyse the consequences of an event, whereas Fault Tree Analysis (FTA) and the Markov process analyse the causes of an event. Pyzdek (2003) describes FTA as providing a graphical representation of the events that might lead to failure.

Bichou and Evans (2007) describe how precursor analysis combined with other techniques such as near-misses and probabilistic risk analysis provide an effective framework for risk assessment and risk management in the context of maritime security. They define 'precursor' as "any internal or external condition, event, sequence, or any combination of these that precedes and ultimately leads to adverse events." Bichou and Evans (2007) argue that the benefits from introducing programmes of security assessment based on precursor analysis include the identification of previously unknown failure modes (for FMEA analysis) and the analysis of the effectiveness of actions taken to reduce risk.

In addition to the risk assessment tools described by Bichou (2009), other industry-specific methods exist in the security field. One seaport-specific method of risk assessment can be found in the Navigation and Vessel Inspection Circular (NVIC) No. 11-02 dated 13 January 2003 issued by the United States Coast Guard. Enclosure 5 (Guidance on Assessing Facility Security Measures) includes a simplified risk-based security assessment methodology which seaports can conduct themselves in pursuit of their compliance with the requirements of the United States Maritime Transportation Security Act (2002).

Another industry-specific document which contains a methodology on risk assessment is the International Standard ISO 28001 (2007) "Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance."

Rosqvist and Tuominen (2004) describe the methodology behind the Formal Safety Assessment (FSA) which was first developed by the UK's Maritime and Coastguard Agency and later incorporated into the International Maritime Organisation's interim guidelines for safety assessment (Bichou, 2009).

Talas and Menachof (2009) develop a conceptual model for calculating a port facility's residual security risk. The conceptual model examines the following characteristics:

- the security threats that the port facility faces and their probabilities
- an estimate of the economic damage to the port facility from each prescribed security threat
- the port facility's security components and systems and their performance in the face of the potential security incidents
- the port facility's security components' costs.

3.4. Port Security Risk Sources

Juttner et al (2003) describe supply chain risk sources as environmental (accidents, socio-political actions such as terrorism), organisational (labour, production uncertainties or IT-system uncertainties) or network-related (risks arising from interactions from companies within the supply chain.)

3.4.1. Environmental Risk Sources

The environmental risks that ports face include but are not limited to acts of terrorism. While the focus on terrorism appears to be uppermost in the literature, only three such attacks were directed at port facilities in the last decade: in April 1996 when the Tamil Tigers launched an attack on the port of Colombo and succeeded in damaging three vessels (Aryasinha, 2001), in 2004 Jamaat al-Tawhid attacked the Khawr Al Amaya and Al Basrah oil facilities in Iraq and in the same year suicide bombers from Hamas and the al-Aqsa Martyr's Brigade launched an attack in the Port of Ashdod (Greenberg et al, 2006). Furthermore, terrorist attacks against maritime targets constitute only two percent of all international terrorist incidents over the last thirty years (Raymond, 2006, p240). Ports also face threats of unlawful entry and activity by thieves, smugglers and potential stowaways as well as individuals bent on destruction or the interruption of international trade on political or ideological grounds.

Prior to 9/11 the main threats to ports were considered to be from drug smuggling and organised crime. These threats resulted in the creation in the United States of the Business Anti-Smuggling Coalition (BASC), which has now been superceded by the Business Alliance for Secured Commerce, a security initiative initially aimed at reducing the risk of legitimate cargo being used by illegal organizations for the narcotics trade (Gutierrez et al, 2007, p168). Nevertheless, the potential for terrorist attacks to disrupt ports and supply chains dominates the literature post-9/11. According to Raymond (2006, p242) ports are vulnerable to attack by terrorists: they are extensive in size and accessible by water and land. Furthermore, their accessibility impedes the deployment of the types of security measures that, for example, can be more readily deployed at airports. Bichou (2004) highlights the additional security threats that ports face due to their "close spatial interactions with large city-agglomerations and seashore tourist attractions." Table 2 lists examples of potential attack characteristics against US maritime targets (Parfomak and Fritelli, 2007).

According to Nincic (2005, p623), the Sri Lankan Liberation Tigers of Tamil Eelam (LTTE), Hizballah, the Popular Front for the Liberation of Palestine, the Abu Sayyaf Group, Gama al-Islamiya, the Moro Islamic Liberation Front and the IRA are all believed to have varying levels of maritime expertise. According to Raymond (2006, p240), the terrorist groups that are known to have a maritime capability include "Polisario, the Abu Sayyaf Group, Palestinian groups, Al Qaeda, the Moro Islamic Liberation Front and the Liberation Tigers of Tamil Eelam." However, Raymond (2006, p244) points out that "in order to be considered a threat, it is not necessary for a terrorist group to have already carried out a maritime terrorist attack against shipping or port facilities."

With the potential for maritime terrorists to deploy a mothership with tenders, their geographic reach is, in theory, considerably extended from their homelands' territorial waters. Somali pirates are reported to use this mode of transport to attack ships hundreds of miles offshore (Ould-Abdallah, 2008) and the Mumbai bombers are rumoured to have arrived in Mumbai via inflatable boats from a highjacked fishing vessel, which was later found adrift with the body of a man onboard (Greenberg, 2008).

Table 2 – Example Maritime Attack Characteristics

Dimensions	Example Characteristics
Perpetrators	• Al Qaeda and affiliates • Islamist unaffiliated • Foreign nationalists • Disgruntled employees • Others
Objectives	• Mass casualties • Port disruption • Trade disruption • Environmental damage
Locations	• 360+ U.S. ports • 165 foreign trade partners • 9 key shipping bottlenecks
Targets	• Military vessels • Cargo vessels • Fuel tankers • Ferries / cruise ships • Port area populations • Ship channels • Port industrial plants • Offshore platforms
Tactics	• Explosives in suicide boats • Explosives in light aircraft • Ramming with vessels • Ship-launched missiles • Harbor mines • Underwater swimmers • Unmanned submarine bombs • Exploding fuel tankers • Explosives in cargo ships • WMDs in cargo ships

(Source: Parfomak and Fritelli, 2007)

3.4.2. Organisational Risk Sources

Organisational risk sources in port security stem chiefly from the security labour force and the operational aspects of security systems, including IT-systems. Examples of labour force risks include security guard manpower shortfalls and security guard violations. Security guard violations cover not only on-site breaches in working practices but include the unauthorised copying, lending or sale of security passes. According to Raymond (2006, p243), seafarer certificates can easily be forged and identity documents can be bought on the black market so it must follow that this can be done onshore as well. Operational aspects of security systems include failure by the security workforce to adhere to security procedures, failure of CCTV camera units, intruder detection devices, scanning equipment or any IT security system.

3.4.3. Network-related Risks

Juttner et al (2003) describe network-related risk sources as those "which arise from interactions between organisations in the supply chain." Network-related security risks which ports face are those which had their origins in supply chain interactions and can result from the failure of any company's security systems or the exploitation of a security weakness. For example, in the containerised trade, the possibility of the introduction of a chemical, nuclear, biological or radiological (CNBR) device which is detonated in a port will have considerable consequences for the port as well as cause severe supply chain interruption. In the port security war game Gerencser et al (2003) showed that a dirty bomb, a conventional explosive device used to scatter nuclear or radiological material, found at the port of Los Angeles followed by the discovery of another shipped through the port of Savannah could

ultimately lead to supply chain interruptions and stock market falls which could cause up to $68 billion in direct and indirect losses.

Other network-related risks include the use of the containerised trade to transport stowaways or even terrorists through ports and across national boundaries, as in the case of the suspected member of al-Qa'eda found on the quay in an Italian port in a container converted into a mobile hotel room (Raymond, 2006, p246; OECD, 2003).

3.5. Port Security Risk Consequences

The consequences of port security risk events are typically negative and can be classified as direct or indirect losses. Direct losses include physical damage to port infrastructure. The disruption of port activities resulting from direct losses will invariably lead to indirect losses such as business interruption through supply chain shocks, increased insurance costs and increased cost of working through the implementation of a tougher security regime which restricts cargo movements through the port.

3.6. Port Security Risk Drivers

Juttner et al (2003, p205) describe how supply chain risk drivers "impact directly on network-related risk sources." Supply chain risk drivers such as globalisation of supply chains and the trend to outsourcing have their equivalents in their effect on network-related security risks. The globalisation of terrorist and criminal networks and the trend to outsourcing security in the supply chain act as potential port security risk drivers. Miller and Talas (2007) state that there are approximately twenty terrorist groups that have aligned themselves to al-Qaeda, signing up to Osama bin Laden's fatwa of November 2000 and in effect globalising bin Laden's terrorist organisation. In particular, the outsourcing of security in the supply chain can lead to a lack of transparency of implemented security measures and with it confidence in the third party provider of security. Security initiatives such as the ISPS Code and ISO 28000 are designed to counter this type of port security risk driver by introducing a given set of minimum security standards in a transparent manner. The importance of identifying port security risk drivers becomes clear in the examination of port security vulnerability.

3.7. Port security vulnerability

Juttner et al (2003) describe supply chain vulnerability as "the propensity of risk sources and risk drivers to outweigh risk mitigating strategies, thus causing adverse supply chain consequences." Translating this to port security, a description of port security vulnerability can be the propensity of port security risk sources and risk drivers to outweigh port security risk mitigating strategies, thus causing adverse security events. Broder (2006) defines vulnerability as "the probability of failure and the probability of occurrence after countermeasures are implemented. It measures the likelihood of threat and its ability to cause damage." In this context, port security risk drivers combine with port security risk sources to derive a port's security threats. Considering the earlier proposed definition of port security risk, port security vulnerability can thus be defined as the product of the probability of a security event and the inability of a port's security systems to prevent the occurrence of the event.

3.8. Port Security Risk Mitigating Strategies

Pinto and Talley (2006, p268) describe the security incident cycle of ports in four phases: prevention, detection, response and recovery. They describe prevention as barriers that deny terror plans and events; detection provides early apprehension; response pursues an event and mitigates its impact; and recovery involves the return to normal operations. There are two key port security risk mitigating strategies which were introduced after 9/11. The main one is the ISPS Code introduced by the IMO at the Diplomatic Conference in December 2002.

The other is the Maritime Transportation Security Act which was passed by the US Congress in November 2002 and relates to US port facilities, or facilities in US parlance. According to Bichou (2004, p323), the ISPS Code is "the most important global security initiative ever."

3.9. The ISPS Code

The predominant security initiative which internationally trading port facilities have been subjected to is the ISPS Code, which was introduced into European Union legislation in the form of EC Regulation 725/2004 (Dekker & Stevens, 2007; Anyanova, 2007). U.S. implementation of the ISPS Code for port facilities was accomplished through the Maritime Transportation Security Act (MTSA) 2002 (Helmick, 2008). The main provisions of the ISPS Code came into force on 1 July 2004, eighteen months after the Code was introduced by the IMO's Diplomatic Conference of 12-14 December 2002 by amending the International Convention on the Saving of Life at Sea (SOLAS) 1974 by the addition of a new chapter XI-2.

The ISPS Code was drawn up by the IMO's Maritime Safety Committee and its Maritime Security Working Group in little over a year following the adoption of resolution A.924(22) on the review of measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships, in November 2001 (ISPS Code, 2003, p iii.) The ISPS Code was adopted on 12 December 2002 by the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS) 1974 when the existing chapter XI was amended and re-identified as chapter XI-1 and a new chapter XI-2 was adopted on special measures to enhance maritime security. Amendments were also made to chapter V.

The ISPS Code is divided into two parts, A and B. Part A establishes the new international framework of measures to enhance maritime security by introducing mandatory provisions while part B provides non-compulsory guidance on the procedures to be undertaken in order to comply with the provisions of chapter XI-2 and of Part A of the ISPS Code (Bichou, 2004.) Certain countries, such as the European Union under EC Regulation 725/2004, have made compliance with part B of the ISPS Code mandatory through legislation (Dekker & Stevens, 2007; Anyanova, 2007).

The objectives of the ISPS Code are to enable the prevention and detection of security threats within an international framework; to establish roles and responsibilities; to enable the collection and exchange of security information; to provide a methodology for assessing security and to ensure that adequate security measures are in place. The objectives are to be achieved by the designation of appropriate personnel on each ship, in each port facility and in each shipping company, to prepare and to put into effect the approved security plans. The ISPS Code is applicable to vessels engaged in international trade including passenger vessels with 12 or more berths, cargo vessels of 500 gross tonnes and over, mobile offshore drilling units and all port facilities serving such vessels engaged in international trade.

The ISPS Code definition of responsibilities determines the responsibilities of Contracting Governments, ship operators and port facility operators. Contracting Governments must identify the Designated Authority (for port facilities), set security levels, perform port facility security assessments, coordinate with port facility security officers and issue and inspect International Ship Security Certificates. In turn, ship and port facility operators must designate the appropriate security officers and develop and implement the security plans. Each Contracting Government (or a Recognised Security Organisation appointed by the Designated Authority) must carry out a Port Facility Security Assessment (PFSA) which will include the following elements (ISPS Code Part A.15.5):

- Identification and evaluation of important assets and infrastructure it is important to protect;
- Identification of possible threats to the assets and infrastructure and likelihood of their occurrence, in order to establish and prioritise security measures;

- Identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and
- Identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

Each Contracting Government (or Recognised Security Organisation appointed by the Designated Authority) must then prepare a port facility security plan (PFSP) which addresses at least the security measures listed in ISPS Code Part A.16.3.

4. COMBINING SIX SIGMA PRINCIPLES WITH PORT SECURITY

Ng et al (2005) show how Six Sigma principles may be applied to reduce the risk of accidents among cargo stevedores operating on small container transhipment barges in Hong Kong harbour. In their analysis they show the critical factors which result in the falls of stevedores from the tops of the containers at the public cargo working area. They list a series of critical factors including not concentrating at work; disregarding safety issues; using worn out hooks and slings; consuming alcohol in the workplace; and standing on top of a container which is being lifted into midair.

In the same way in which Ng et al (2005) have identified critical factors which affect the safe operation of cargo handling, it is necessary in the Six Sigma define phase to arrive at the factors critical for the success of security of an ISPS Code compliant port facility. They are listed in section A.14.2 of the ISPS Code and relate to the security activities which are required "to identify and take preventive measures against security incidents:

1. ensuring the performance of all port facility security duties;
2. controlling access to the port facility;
3. monitoring of the port facility, including anchoring and berthing area(s);
4. monitoring restricted areas to ensure that only authorised persons have access;
5. supervising the handling of cargo;
6. supervising the handling of ship's stores; and
7. ensuring that security communication is readily available."

It is these critical success factors which guide the selection of the key performance indicators which need to be measured and analysed before any improvements and control measures can be introduced in the port facility's security regime. The methodology for measurement and analysis are outlined below. Ung et al (2007) referred to critical factor #6 in their paper but the metric they employed in their simulation was time and its variation from a given mean, rather than measuring the performance, say, of a detection device such as a CCTV system used to monitor the supervising of the handling of ship's stores.

The framework for the conceptual model is based on the actual key performance indicators of a major ports company. They are:

1. Guardforce shortfall
2. Unauthorised persons detected in the port facility
3. Unauthorised persons detained in the port facility
4. Unauthorised persons refuse to show ID in the port facility
5. Access control violation (main gate)
6. Access control violation (perimeter fence)
7. Access control violation (terminal building)
8. Access control violation (restricted area)
9. Access control violation (cargo handling area)
10. Access control violation (ship-port interface)
11. Weapons detected in the port facility
12. Explosives detected in the port facility
13. IT system failure

14. Fake biometric ID detected
15. Unauthorised act by employee
16. Unauthorised act by visitor
17. Truck drivers not staying with the cab
18. CCTV camera failure
19. Security communications equipment malfunction
20. Other security equipment malfunction

Each of the twenty key performance indicators listed above are monitored and measured on a per security-shift basis of eight hours each shift and any security non-conformities are reported to and recorded by the Port Facility Security Officer. For example, in the event of a security guardforce shortfall, which would have a direct bearing on the ability of the port facility to monitor the access control points and muster security patrols, it is necessary to calculate the number of guards who fail to make up the full complement of guards for each eight-hour shift. For a port facility which employs 10 security guards per shift, given that there are three shifts in a day and that the port facility maintains 24 hour operation 365 days per annum, the total number of guardforce man shifts equates to 10,950 per annum. In the event that on 13 occasions during the year there were guardforce shortfalls of one guard for each shift, this means that there were 1,187 defects per million, a figure between 4 and 5 Sigma. In order to improve the performance of guardforce shortfalls to a level of 6 Sigma, the number of guardforce shortfalls reported must be reduced from 13 per annum to less than 2.55, i.e. only two guardforce shortfalls reported for any one eight-hour security shift during the annum.

The other nineteen key performance indicators can be measured and analysed in the same way as for the guardforce shortfalls by recording the number of security violations or non-conformities per eight-hour shift. Furthermore, the data which will be built up over a long period of time can be analysed by the Company Security Officer to assess and address any weaknesses in the security regime leading to targeting training of security staff or replacement of poorly performing security equipment.

Table 3 shows the relationship between the port security critical success factors and the key performance indicators.

Table 3 – The relationship between port security critical factors and key performance indicators

Critical Success Factor	Key Performance Indicator
Ensuring the performance of all port facility security duties	1, 13, 18, 19, 20
Controlling access to the port facility	2, 3, 4, 5, 6, 7, 8, 14, 15, 16
Monitoring of the port facility, including anchoring and berthing area(s)	11, 12, 15, 16, 17, 18
Monitoring restricted areas to ensure that only authorised persons have access	8
Supervising the handling of cargo	9
Supervising the handling of ship's stores	10
Ensuring that security communication is readily available	19

(Source: Authors)

The key to linking the key performance indicators to the critical success factors becomes apparent in the next stages of the Six Sigma process: by being able to measure how the critical success factors are performing. In theory, it is easier to conduct analysis of the root cause of any security issues which do arise. Furthermore, following any subsequent identification of solutions or the introduction of any process improvements, the collection of key performance indicator data will enable the company security officer to monitor how the solutions or process improvements perform compared to the status quo.

5. CONCLUSIONS

The paper examined the literature on maritime port security and proposed new definitions for port security, port security management and port security risk before describing a conceptual model which can be applied in a Six Sigma setting to measure and assess prescribed port security key performance indicators which match the critical success factors for port security as described in the ISPS Code. The Six Sigma process provides the statistical tools for an experienced company security officer to be able to measure the performance of the security systems in the port facility against his/her preset levels of acceptable performance while the model allows for continued improvement in port security systems. Future research in this area may revolve around measuring the success of actual implementation of the Six Sigma process in port security management.

REFERENCES

Anyanova, E (2007). The EC and Enhancing Ship and Port Facility Security, Journal of International Commercial Law and Technology, (2)1, pp 25-31.

Bichou, K. (2004). The ISPS Code and The Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management, Journal of Maritime Economics & Logistics, (6)4, pp.322–348.

Brewer, P. and Bagranoff, N.A. (2004). Near Zero-defect accounting with Six Sigma, Journal of Corporate Accounting and Finance (Wiley), (15)2, pp.67–72.

Broder, J. (2006). Risk Analysis and the Security Survey, 3rd Edition, Boston, Butterworth-Heinemann

Chopra, S. & Sodhi, M.S. (2004). Managing Risk to Avoid Supply Chain Breakdown, MIT Sloan Management Review, (46)1, pp. 53-61

Christopher, M. (2005). Logistics and Supply Chain Management, 3rd Edition, FT Prentice Hall

Closs, D. & McGarrell, F. (2004). Enhancing Security Throughout the Supply Chain, IBM Center for the Business of Government Special Report Series

Dasgupta, T. (2003). Using the Six-Sigma metric to measure and improve the performance
of a supply chain, Total Quality Management and Business Excellence, (14)3, pp.355–366.

Dekker, S. & Stevens, H. (2007). Maritime security in the European Union – empirical findings on financial implications for port facilities, Maritime Policy and Management, (34)5, pp. 485-499.

Gerencser, M., Weinberg, J. & Vincent, D. (2003). Port Security War Game, Booz Allen
Hamilton

Greenberg, M. (2008). The Terror Attacks in Mumbai: Background, Operational Uniqueness and Implications, [WWW]<URL: http://www.ict.org.il/NewsCommentaries/Commentaries/tabid/69/Articlsid/538/currentpage/3/Default.aspx> [Accessed 3 August 2009]

Greenberg, M, Chalk, P, Willis, H, Khilko, I & Ortiz, D (2006). Maritime Terrorism: Risk and Liability, RAND Corporation Centre for Terrorism and Risk Management Policy

Harrald, J., Stevens, H.W. & van Dorp, J.R. (2004). A framework for sustainable port security, Journal of Homeland Security and Emergency Management , Vol. 1 (2): Article 12.

Heimer, C. (1988). Social structure, psychology and the estimation of risk, Annual Review of Sociology, (14) pp. 491-519.

International Ship and Port Facility Security Code (2002), International Maritime Organisation

Juttner, U., Peck, H. and Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research, International Journal of Logistics: Research and Applications, (6)4, pp. 199-213.

Kahneman, D. & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk, Econometrica, (47)2, pp. 263-292.

Lowrance, W.W. (1980). The nature of risk, in: Schwing, R.C. and Albers, W.A. (eds) How Safe is Safe Enough?, Plenum Press, New York

Lynch, D.P., Bertolino, S. and Cloutier, E. (2003). How to scope DMAIC projects, Quality
Progress, (36)1, pp.37–41.

March, J. & Shapira, Z. (1987). Managerial perspectives on risk and risk taking, Management Science, (33)11, pp. 1404-1418.

Markowitz, H (1952). Portfolio Selection, The Journal of Finance, (7)1, pp. 77-91.

Miller, M.D. (1994). Marine War Risks, Lloyd's of London Press Ltd, 2nd Edition

Miller, N. & Talas, R. (2007). War, terrorism and associated perils in marine insurance, in: Marangos, H. L. (ed.) "War Risks and Terrorism", Insurance Institute of London Research Study Group 258

Nakhai, B. & Neves, J. (2009). The challenges of Six Sigma in improving service quality, International Journal of Quality & Reliability Management, (26)7, pp. 663-684.
Nincic, D. (2005). The Challenge of Maritime Terrorism: Threat Identification, WMD and Regime Response, The Journal of Strategic Studies, (28)4, pp. 619-644.
OECD (2003). Security in Maritime Transport: Risk Factors and Economic Impact, Maritime Transport Committee, Directorate for Science, Technology and Industry
Ould-Abdallah, A. (2008). Piracy off the Somali Coast: Workshop commissioned by the Special Representative of the Secretary General of the United Nations to Somalia. p19, Nairobi, 10-21 November 2008. [WWW]<URL: http://www.imcsnet.org/imcs/docs/somalia_piracy_intl_experts_report_consolidated.pdf.
[Accessed 3 August 2009]
Parfomak, P. & Frittelli, J. (2007). Maritime Security: Potential Terrorist Attacks and Protection Priorities, CRS Report for Congress, 9 January 2007
Pinto, C.A. & Talley, W.K. (2006). The Security Incident Cycle of Ports, Maritime Economics & Logistics, (8) pp. 267-286.
Price, W (2004). Reducing the Risk of Terror Events at Ports, Review of Policy Research (21)3, pp. 329-349.
Pyzdek, T. (2003). The Six Sigma Handbook, McGraw-Hill
Raymond, C.Z. (2006). Maritime Terrorism in Southeast Asia: A Risk Assessment, Terrorism and Political Violence, (18)2, pp. 239-257.
Sheffi, Y. (2001). Supply Chain Management Under the Threat of International Terrorism, International Journal of Logistics Management, (12)2, pp. 1-11.
Sodhi, M. & Sodhi, N. (2008). Six Sigma Pricing: Improving Pricing Operations to Increase Profits, FT Press
Talas, R. & Menachof, D. (2009). The efficient trade off between security and cost for sea ports: a conceptual model, International Journal of Risk Assessment and Management, (13)1, pp. 46-59.
Taghaboni-Dutta, F. and Moreland, K. (2004). Using Six-sigma to improve loan portfolio
performance, Journal of American Academy of Business, Cambridge, (5)1–2,
pp.15–20.
Voehl, F. (2004). Six Sigma community improvement projects, Annual Quality Congress
Proceedings, Milwaukee, pp.351–363.
Wang, F.K., Du, T.C. and Li, E.Y. (2004). Applying Six Sigma to supplier development, Total Quality Management and Business Excellence, (15) 9–10, pp.1217–1230.
Williams, Z., Lueg, J.E. & LeMay, S.A. (2008). Supply chain security: an overview and research agenda, International Journal of Logistics Management, (19)2, pp. 254-281.
Yap, W.Y. & Lam, J.S.(2004). An interpretation of inter-container port relationships from the demand perspective, Maritime Policy & Management, (31)4, pp.337-355.
Zsidisin, G.A., Ellram, L.M., Carter, J.R. & Cavinato, J.L. (2004). An analysis of supply risk assessment techniques, International Journal of Physical Distribution & Logistics Management, (34)5, pp. 397-413.

ABOUT THE AUTHORS

Risto Talas is a PhD student at City University's Cass Business School in London, UK. He began his career at Lloyd's of London working as an Underwriter of marine war, terrorism and political risks and subsequently worked as a Consultant for a maritime security company in London. He is also a Visiting Lecturer in port and maritime security at City University's School of Engineering and Mathematical Sciences. His current research interests include port and supply chain security risk and efficiency.

David A. Menachof is the Peter Thompson Chair in Port Logistics at The University of Hull and former Director of the MSc in Logistics, Trade and Finance degree at City University's Cass Business School in London, England. Dr. Menachof received his doctorate from the University of Tennessee, and was the recipient of the Council of Logistics Management's Doctoral Dissertation Award in 1993. He has previously taught at the University of Charleston, South Carolina, and the University of Plymouth, England. In addition, he is a Fulbright Scholar, having spent an academic year in Odessa, Ukraine as part of the grant and is currently on the roster of the Fulbright Senior Specialist Candidates list, as an expert in Logistics and Distribution. Most recently, Dr. Menachof was the recipient of a £500,000 research grant on Cargo Screening sponsored by the UK's Engineering and Physical Sciences Research Council. He is also involved with Cargo Security International, a new company focused on Supply Chain Security solutions, acting as project manager during the product development phase. Dr. Menachof's work has been published and presented in journals and conferences around the world. His current research interests include supply chain security and risk, global supply chain issues, liner shipping and containerisation, and financial techniques applicable to logistics.

Bronze Sponsors

Supporters

The Blue MBA