航　運　季　刊
第十九卷　第二期
民國九十九年六月
頁　77～　頁　97

Maritime Quarterly
Vol. 19 No. 2
June 2010
pp. 77~97

Implementation of Container Security in Northern America Area

北美地區執行貨櫃保安之探討

Chih-Ching Chang (張志清)[1]
Nora Suh-Jiun Jeng (鄭夙君)[2]
Shy-Tzong Liou (劉詩宗)[3]

摘要

1960年代貨櫃興起，逐漸取代傳統散裝運輸，紓解了長久以來散雜裝運輸有關偷竊之問題。但隨著科技進步，再加上日新月異的犯罪手法層出不窮，貨櫃封條已不再是貨物唯一的安全保障，再者美國世貿中心以及911的恐怖攻擊，更引起全世界對貨櫃保安的重視。然而，船公司和託運人所重視的安全，其實與保安有著不同的意義。本研究以美國地區為主要目標，探討貨櫃保安的相關法源、船公司和港口貨櫃集散站，以及內陸運輸的實務作業。如何因應貨櫃保安之要求，從接受訂艙到完成運送建立標準作業程序，以避免因為貨櫃保安之要求而增加運送時間，所造成客戶的抱怨以及產生客訴問題，進而追求更有服務品質、效率以及確保貨櫃安全的整合運送方式。貨櫃保安的要求只會增加不會減少，況且主導增修法的國家大多為已開發國家，其購買能力不容小覷，大多數的出口國顯少有談判籌碼，所以只能接受，因此兼顧貨櫃保安以及安全為業界當下所追求的目標。然而，相關法源要求的增加對於運送時間以及客戶滿意度則是呈反比，船公司、貨櫃場以及相關業者如何在夾縫中求生存？本研究進一步探討業界的實務作法，從以往各個獨立系統（如運務、櫃務、會計等系統）之間傳送的作業方式，至今已有業者發展出同一平台整合性的系統，建立各個子系統上下游的關係，不但可以避免輸入重複的資料來節省人力成本，然後進一步做系統勾稽以除錯，另外，更重要的是遇有異常或緊急狀況時，系統會自動通知相關單位以立即採取配套措施。單一平台之整合性系統不但可以減少系統間傳送的時間，對於保安以及客戶滿意度的提昇更是不在話下，所以建立整合型系統以因應日益增加的法規是業界當務之急。

關鍵詞：貨櫃保安、服務品質、整合系統、船舶與港口設施保安章程

---

[1] 國立台灣海洋大學航運管理系教授兼海運暨管理学院院長。本文部分改寫自作者接受國科會補助專題研究計畫（ NSC93-2415-H-019-003-SSS）

[2] 國立台灣海洋大學航運管理系碩士。

[3] 國立臺灣海洋大學航運管理研究所博士候選人。

ABSTRACT

After 11th September 2001, the United States of America remains the primary target of terrorist groups. An era of perpetual conflict has emerged. Like fighting crime (economically motivated violence), governments have to develop some organizations to take measures against terrorism (politically motivated violence) every day. With the dawn of the age of networked terrorism, regional governments, terminals & carriers have to develop integrated system with common databases, engage in the exchange of personnel, joint training and operations, resources, expertise and sharing experience. They do have no alternative but to allocate more resources on implementing security measures and recruiting qualified staff. How to meet the challenge of security with lower cost is the goal which all carriers' intend to achieve. Hammering out the integrated system with comprehensive functions under unique platform from booking to delivering of goods may reduce operation costs and improve the service quality. This paper aims to provide solutions to the carriers which shall meet the requirements of relevant security laws and regulations.

Keywords: Container security, Service quality, Integrated system, ISPS Code

I Introduction

Heightened security concerns in the US following the World Trade Center terrorist attacks were clearly indicating that new legislation would be passed by Congress and all of these national rules would have to be observed by ships of any flag calling at US ports whatsoever. So the way forward seemed to be an international convention regulating maritime security issues. In the post 911, security requirements are getting increasingly strict and complicated for developed countries. To elaborate new laws, better laws and additional international instruments may safely be in the negative as far as issues of criminal law and jurisdiction are concerned. Is it really important for all of us?

By virtue of American viewpoints, security is the responsibility of sovereign states. The regulations on the preventative technical measures musgt be constantly updated both on the US domestic and international level. Implementation and enforcement of such measures requires a constant oversight and verification. While the As views are American views points are projected from the podium of unilateral power, they do not reflect an awareness of the probability that a shift in the balance of trade will dictate business activity and thus domestic politics. Creating political cleavages and increased trade barriers to combat the fact of terrorism in the short term may advance the inertia of trade into other, or new, markets.

On the other hand, by virtue of Asian viewpoints, safety is more significant

than security to be concerned in Asia area. In terms of safety, it’s crucial to carriers whether they could complete shipments or not. Every ship master hopes to pass canals safely. Safety is a daily routine job. Nevertheless, security is in case something happens. Therefore, underwriters and shipowners would argue that maritime security has been a universal and continuing concern.

II Security Laws and Regulations

Despite a comparatively incident, developed countries deem merchant shipping should have been singled-out as an industry posing a major threat to world security. The International Maritime Organization (the IMO), arguably at the behest of the current US administration, has acted swiftly and conceived the International Ship and Port Facility Security Code (the ISPS Code), which was added as a new chapter in International Convention for the Safety of Life at Sea (the SOLAS). SOLAS has been regarded as an appropriate requirement for the new secure standard because this regulation was generally employed to passenger vessels, cargo vessels over 500 metric tons, and mobile offshore oil and gas rigs. The purpose of the provision is to improve security for ships, persons (passenger and crew) on board, offshore terminals, and port facilities. These amendments will affect all passenger carrying ships and other ships over 500 gross tonnage sailing in international waters, and the ports that serve such ships. The ISPS Code was set to come into effect on 1 July 2004.

2.1 IMO Conventions and Regulations

The IMO deeply considered about the worldwide escalation of acts of terrorism in all its forms to attack ships, ports, offshore terminals or other facilities to adopt new regulations to enhance ship and port security and avert shipping from becoming a target of international terrorism in December 2002. The ISPS Code was to set up international criteria of the risk management for identifying high-risk containers before the departure for US. It is the crux of the marine industry.

2.1.1 Ship Security Regulations Provided by SOLAS and ISPS CODE

Before the enactment of the ISPS Code, for sea-going mariners, the main source of training requirements is derived from the Seafarers' Training, Certification and Watch keeping Code (STCW). Within STCW, there is a general requirement for masters and chief mates on ships of 500 gross tonnages or more to be trained to maintain safety and security of the ship's crew and passengers. The specific focus of the generic STCW requirement, however, is on safety rather than

security. The competencies to be demonstrated under STCW include the detection of alarms; fire and boat drills; maintenance of safety systems; on board emergency procedures; damage control; and salvage. The generic provisions of STCW do not cover security except where it is incidental to the provision of safety.

The ISPS Code requires shipowners and ship operators to develop a ship security plan, which shall be submitted to the Administration or its recognized security organization for approval. In accordance with such a ship security plan, the shipowners and ship operators shall assign company security officers and ship security officers, and adopt appropriate security measures based on different security levels. The ship security shall be audited, reviewed, verified, and examined in order to ensure the implementation of the requirements. The major security regulations imposed on ships by the ISPS Code, and the potential problems, which might arise from the implementation of the Code.

As the requirements of this Code, Contracting Governments, Government agencies, local administrations and the shipping and port industries are responsible to establish the respective roles at the national and international level for ensuring maritime security. The ISPS Code is an extension of SOLAS mandated by IMO. ISPS Code is basically aimed at expanding the scope of safety of life at sea and navigation, and further to prevent the threats that terrorists may bring to the maritime industry.

As a final note on the training required for the ISPS Code, the initial emphasis in the implementation phase has been upon the development of formal training programs. There is an on-going requirement for drills and exercises to keep the skills of shipboard and port facility personnel up-to-date after the ISPS Code has been implemented. The ISPS exercising requirement echo the requirements for oil-spill preparedness exercises contained in the International Convention on Oil Pollution Preparedness, Response and Co-Operation. Within Canada, a national exercising program has been established for oil spill exercises that require oil handling facilities and response organizations to exercise at least once every 3 years. It remains to be seen if a similar structure will be put into place for security purposes.

2.2 US Laws and Regulations

Owing to there are about 44% of the world containers flow going to US, and cargo owners are much concerned about the security requirements in the United States. If a flag state did not meet the required compliance with Part B of the ISPS Code when it issued its International Ship Security Certificate, a ship calling at a US port would therefore be detained. These above requirements had exceeded that in the ISPS Code, and the deadline was six months earlier than the International

Convention. The issue caused immense anxiety and industry confusion worldwide. Many maritime industry leaders had no choice but to conclude they must at that moment.

2.2.1 The Customs-Trade Partnership Against Terrorism (C-TPAT)

The C-TPAT program is a voluntary security compliance program directed at establishing uniform standards for secure facilities, assets and equipment, procedures, and personnel for various parties throughout the shipment supply chain. The members of the C-TPAT include the US Customs Service, the international trade community and industry. All of the importers, carriers, and third parties enter the C-TPAT voluntarily.

The C-TPAT is a good idea, but the costs of membership outweigh the advantages. The shipping industry still supports the C-TPAT program establishing a government-industry partnership. Many complained about the lack of resources devoted to the program, and the need for greater knowledge and skill on the part of C-TPAT validators. The consensus along the supply chain favoring an Industry-wide security initiative, but industry pressures to join C-TAPT do not outweigh the perceived lack of advantages to participating in the program or the costs a firm must bear in order to be validated.

2.2.2 The Container Security Initiative (CSI)

The CSI is a program intended to help increase security for containerized cargo shipped to the United States from around the world. CSI is a revolutionary program to extend US zone of security by pre-screening containers posing a potential security risk before they leave foreign ports for U.S. seaports. It is a multinational program protecting the primary system of global trade-containerized shipping-from being exploited or disrupted by international terrorists. CSI adds security to the movement of maritime cargo containers to the United States, while at the same time moving those containers faster, more efficiently and more predictably through the supply chain at USA side. However, carriers and shippers have to invest huge capital on system development at loading ports in comply with the CSI.

2.2.3 Advance Cargo Reporting and the 24-hour Rule

Automated Manifest Systems (AMS) is a multi-modular cargo inventory control and release notification system with an electronic system that automates the customs clearance process for each mode of transportation – rail, air, vessel and truck. AMS interfaces directly with Customs Cargo Selectivity and In-Bond systems allowing faster identification and release of low risk shipments. It also supports a 24-hour rule that requires cargo manifests to be submitted to U.S.

Customs 24 hours prior to loading of containers. This ruling is in response to the need to identify dangerous cargo before it reaches the U.S. The potential threat of terrorists using containers poses a significant risk to the global economies and societies. Each carrier (also including Non-Vessel Operating Common Carriers, "NVOCCs") is now required to file manifest data with the US Customs Service (renamed as Customs and Border Protection, "CBP") 24 hours before loading containerized cargo in a foreign port aboard a ship bound for the US. This is required so the US government can conduct a Mass Destructive Weapon screening of all such shipments.

Before the full implementation of this 24-hour rule, carriers were asked to file manifest data three days before vessels arrived in US waters. In reality, however, the 24-hour rule's shortened practice has caused a serious disruption of the information flow and documentation procedures for the international shipping trade, especially for NVOCCs. Moreover, the most significant change NVOCCs encountered refers to their status/roles in the global supply chain. They are now considered carriers, rather than the shippers or consignees they were. As a result, with the 24-hour rule NVOCCs are permitted to file the manifest data to Customs and Border Protection (CBP) directly. It is strongly argued, however, that a complete and effective transportation service in international trade requires much more than manifest data filing. It is acknowledged that NVOCCs encounter difficulties in providing customers a smooth cargo release/Immediate Transport Cut (IT Cut) as requested. Such a situation is often attributed to the lack of sufficient operational infrastructure and experienced manpower in the offices of NVOCCs.

2.3 Relevant Regulations and Rules of Canada/Panama

2.3.1 Electronic Data Collection System (EDCS)

The EDCS provides the electronic means to submit all required pre-arrival information to visit and/or transit the Panama Canal. The EDCS' primary goal is to provide the highest level of security and service to all customers; it allows the execution of an on-line risk assessment matrix to properly comply with international security regulations, and to safeguard the Panama Canal and the customers' assets.

Panama Maritime Authority appointed the firm "Phoenix Management Services (Phoenix)" as her only recognized security organization. Ship owners must submit their ship security plans to the Panama attorney, and then the attorney will relay the security plans to Phoenix for approval and vice versa. Phoenix will not accept the security plan and documents from owners directly. Any comment or suggestion, which is confidential due to the nature of security sensitive, on the

security plan by the attorney in Panama will response to the owner for improvement or correction. Once the ship security plan is approved by the Phoenix, the owner can take the next step of submitting assessment application to the recognized Class or of applying on-scene assessment for the ship. If there is no outstanding or deficiency, the International Ship Security Certificate will be issued. Ocean carriers need to provide (1) Ship Due, (2) Cargo Declaration, and (3) Crew List pre-arrival visit information requirements within 96 hours prior to arrival at Canal waters.

2.3.2 The Advance Commercial Information of CBSA

The Advance Commercial Information (ACI) program introduces more effective risk management processes and tools to identify threats to the health, safety, and security prior to the arrival of cargo and conveyances in Canada. In accordance with the Canada-U.S. Smart Border Declaration, the focus is on marine cargo and conveyance information initially. Marine carriers are required to electronically transmit marine cargo data to the Canada Border Services Agency (CBSA) 24 hours prior to the loading of the cargo in the foreign port.

III Safety and Security Problems Arising from Inland Transport

Safety is the basis of the security. If the quality of safety is poor, needless to say security. In other words, safety is the foundation to bolster security.

3.1 Safety Problems of Container Transportation

Cargo transportation, with the inherent dynamics of an intermodal environment, faces increased and complicated opportunities for theft, pilferage, and smuggling. Discussion of these opportunities within the transportation industry historically has been splintered by modal differences that often dictate competing priorities and specialized views. In contrast, transportation infrastructure assurance requires the application of a system approach that’s the application of operating, technical, and management techniques and principles to the security of a facility throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources to the identification and resolution of cargo terminal security.

Many analysts believe that motor carriers experience the majority of loss due

to cargo theft (approximately 85 percent of all reported thefts)[4,] followed by maritime, rail, and air. The costs of stolen merchandise are not the only losses associated with cargo theft. When applying the conservative multiplier to determine indirect costs of cargo theft, total costs are estimated at between $20 billion and $60 billion per year. This figure includes the cost of filing, investigating, and paying claims, but does not include all law enforcement and security technology expenses.[5]

3.1.1 Containerized Cargo Crime

Organized crime recognized the potential for big business. Containers, stacked in terminals & rail ramps, could be stolen as a whole, opened and made subject to pilferage, or serve as a conduit for drug smuggling. Cargo terminals are particularly vulnerable to employee penetration at intermodal transfer points, warehouses, rail stacking yards, and docks. The majority of cargo loss claims is involved cargo taken from transportation facilities by personnel authorized to be there and on vehicles controlled or similarly authorized by management.

This immense network of importers, wholesalers, NVOCCs, brokers, truckers, and dock workers create problems for law enforcement and transportation operations in pinpointing instances of bribery, extortion, or purchased information. Estimates indicate that most of all theft and pilferage of transportation cargoes is accomplished by, or with the collusion of, persons whose employment entitles them access to the cargo that is stolen.

Organized criminal groups are becoming transnational, facilitating theft of containerized cargo in one country and trafficking of stolen goods in another. Transnational criminal operations use the entire international shipping cycle, in particular, the maritime and trucking transportation shipping system and the NVOCC sector, to support stolen merchandise trafficking. Organized criminals enjoy the same efficiencies and economies of scale as legitimate transnational businesses, but can elude national efforts to restrict their activities.

3.1.2 Drug Trafficking and Money Laundering

Drug trafficking and money laundering are international problems that take advantage of vulnerabilities in the national transportation system:

---

[4] John A, United States Department of Transportation Research and Special Programs Administration. Volpe National Transportation Systems Center, Intermodal Cargo Transportation: Industry Best Security Practices p.7

[5] John A,United States Department of Transportation Research and Special Programs Administration. Volpe National Transportation Systems Center, Intermodal Cargo Transportation: Industry Best Security Practices p.8

1) Each year 300 tons of cocaine enters the United States[6].
2) High container volume and limited resources for conducting inspections result in a statistically low probability of drug detection. At most major container facilities less than 1 percent of containers can be inspected each day.

The growing volume of containerized trade provides numerous opportunities for smuggling illicit drugs. Containers sealed in one nation may not be opened until they reach a final destination in another country. Both the volume of container trade and the labor-intensive methods required for inspecting containers, severely limit law enforcement personnel and freight transportation operators in identifying and preventing drug smuggling. Commercial containerized shipments conceal money as well as illicit drugs. Currency smuggling is essential to the money laundering process, where money laundering is defined as the legitimization of proceeds from any illegal activity. Currency must be collected from local drug distributors, and then transported to specialized organized crime operations devoted to money laundering.

3.2 Security Rules and Regulations on Container Inland Transport

3.2.1 SAFE Port Act

The Security and Accountability For Every Port Act (SAFE Port Act) of 2006 is the most significant piece of maritime security Legislation in several years, with broad real and potential impact on the international supply chain. The Act codifies into law the C-TPAT program, altering the legal foundation of this program, and will accelerate development of non-intrusive inspection technology for containers headed to the U.S. It also will require new plans to re-open ports following a terrorist incident, with profound implications for delays of shipments in transit.

The Act calls for incremental changes in programs like the C-TPAT program, and authorizes the testing of new technology such as high-tech integrated scanning systems that can inspect container interiors and test for radiation. The Act contains the following features:

1) Provides $400 million for port security grants.
2) Requires the installation of radiation detectors at 22 major U.S. ports by the end of 2007.
3) Requires the Department of Homeland Security (DHS) to develop strategic plans for international supply-chain security, and protocols for post-incident resumption of trade.

[6] John A, United States Department of Transportation Research and Special Programs Administration, Volpe National Transportation Systems Center, Intermodal Cargo Transportation: Industry Best Security Practices p.16

4) Requires DHS to develop additional sources of cargo data for security screening.

The DHS also must develop strategic plans for international supply-chain security, and protocols for resumption of trade following an attack. Relevant Sections are excerpted as following:

1) Section 203 of the SAFE Act addresses possible changes to the Automated Targeting System (ATS). The Act instructs Customs to look at the cost, benefit, and feasibility of requiring additional non-manifest documentation; reducing the time period allowed to revise a manifest and to submit entry data elements, for vessel or cargo, and other actions that would improve the ATS. Customs is also mandated by the Act to consult with its stakeholders in making decisions. Customs is also expected to seek other ways to improve the system. An independent panel will review the effectiveness and capabilities of ATS and how it should be changed or updated, including the use of so-called smart features.
2) Section 204 requires regulations regarding the Container Security Initiative. Compliance is demanded for all containers entering the U.S. Promulgation of international standards is also supported. Subtitle B of the Act deals with the C-TPAT. It requires the formulation of the voluntary program to strengthen and improve the overall security of the international supply chain and to facilitate the movement of secure cargo through the international supply chain. Those eligible to participate are in the international supply chain and intermodal transportation system.
3) Section 405 deals with the International Trade Data System (ITDS), the computer system intended to allow traders to enter trade data once, and have it automatically distributed to all agencies that need it, and mandates all federal agencies that require paper for clearing or licensing imports and exports must participate in ITDS. There is also a section about in-bonds which seeks ways to enhance tracking and reconciliation between ports of arrival and ports of destination.
4) Section 202 requires Homeland Security to develop a program for the resumption of trade in the event of another terrorist incident.
5) The rest of the Act is a hodgepodge of security provisions for ports and includes such things as additional radiation technology. Screening of some sort is mandated for all containers arriving in the United States and 100-percent scanning and searching of all containers identified as high-risk. There are also provisions for assistance/grants to foreign and domestic ports.

IV Better Approaches for Container Transportation Security

As we develop more integrated transportation systems of movement

involving two or more modes of transport, there can be improved mobility and logistical efficiency. However, a potential by-product is the elevated threat or risk associated with safety and security (e.g., terrorism). It seems necessary to specify modes of vulnerability in order to allocate resources for adopting security measures in and ideal situation: effectiveness and efficiency. International goods shipped by sea were logistically designed to move efficiently, reliably and safely however security was not initially considered. Many consider this an indomitable security task, based on the scale of maritime infrastructure and the vulnerability being so massive. Whatsoever the challenge a solution is necessary.

4.1 Service Quality Approach

Both security in trade of goods and efficiency of logistics continue to be critical areas for the shipping development. The ports, terminals, rails, trucks and ship operations are closely connected with the efficiency of global supply chain. If there's any stoppage from aforesaid parties as a terrorist attack, its economic impact will be immense. In order to discover security threat earlier and adopt preventive measures from terrorist attacks, a quality approach for efficiently and effectively is necessary. The concept of service quality approach could be divided into several aspects as hereunder:

1) Cargo tracking system

To develop a proper tracking system will not only record unscheduled door openings, but also triggers an alarm. It would enhance security and safety since a tracking system can also be used beneficially in the supply chain to monitor the progress of the container. This will be of great help in combating simple theft or commercial fraud. Cargo tracking system is the most important issue of e-commerce that customs require and is the threshold of most biddings and global service contracts presently.

2) Better information to facilitate better management of the supply chain

Better monitoring of the container status in ports or terminals can achieve better information flow for the supply chain and may facilitate better management of the supply chain. IMO rather focuses on the AIS and transponder technology to monitor ship movements rather than container movements. The intention is to have not only a short-range AIS system in place but also to have a long-range tracking system.

3) Data transmission

It needs to consider the issue of data transmission and how to prevent terrorists from intercepting and using the information for their purposes. If they want to intercept a ship, they have to do it the hard way or infiltrate the crew. Once the long-range tracking system is in place, all they have to do is check out the movement of the ship and then leave their hide-out for a "JIT capture" or attack.

4) Risk management

Transportation infrastructure assurance advocates a form of risk management that eliminates or controls threats and vulnerabilities through an ongoing resolution process. This approach identifies, evaluates, and controls security threats and issues specific to security through all system life cycle phases, including: (a)Terminal design, (b) Construction, (c) Operation, (d) Replacement, and (e) Disposal. This proactive approach encourages both the design and installation of features which harden terminal elements against criminal activity, and the implementation of security information monitoring systems, which identify and control new threats and security concerns. During all life-cycle phases, the terminal is assessed as an integrated system, rather than a collection of modal transfer and storage hubs.

5) The basic elements of protection

A security program offers the functional and integrated capability of protecting users and operators, as well as the resources of the terminal. The basic elements of protection involve prevention or deterrence of acts or conditions threatening the safety or welfare of those persons or resources, and corrective or remedial action to limit the effects of such acts or conditions when they do occur.

6) An integrated multi-modal approach

Since all transport modes were introduced at different times in the evolution of transportation, the idea of an integrated multi-modal approach has not manifested itself in the U.S. The competition between the modes of transportation has produced transport systems that are typically segmented and non-integrated, as each mode has personally sought to exploit its own advantages and benefits in terms of cost, service, reliability and safety.

More than 100 million[7] laden containers shipped between the world's seaports each year are a tempting conveyance for smuggling a Weapon of Mass Destruction (WMD) into a target country. The US is a prime target for such a weapon, and therefore needs to use a smart layered strategy to sort out the containers that pose a risk to her. The broad range of threat scenarios coupled with the presence of naturally occurring radioactivity in normal commerce add to the complexity of this important problem. The interdiction challenge is to effectively detect and deter smuggling of nuclear weapons and Radiological Dispersion Devices (RDD) in shipping containers without impacting the normal flow of commerce.

4.2 High-tech Application on Containers Transport

Customs organizations and trade entities worldwide use seals to ensure the integrity of containerized cargo while moving from point to point within the supply chain. In order to prevent legitimate containerized cargo from being compromised, the argument is that additional security measures must be undertaken because containers are commonly regarded as the most convenient and possible means used

[7] The report of the Journal of Commerce in 2006.

by terrorists to interrupt the international commerce and peace. Measures can perhaps be classified into four categories, namely the concept of future as (a) Smart container/Radio Frequency Identification (RFID), (b) Container seal improvement, (c) Improvement of locking gear devices, and (d) Installation of electronic tracking devices near door hinges.

4.2.1 Smart Container

Smart container with the electronic Container Security Device (CSD) is one kind of RFID that enables carriers to protect shipments from theft, smuggling, and even terrorist activities while obtaining data from supply chain checkpoints. RFID is a device that keeps tabs on what's going on inside a shipping container and sends out real-time reports. The CSD is easy and economical to deploy, installs with a snap, and is protected inside the container. Discussion of “Future Smart Container” concept usually covers the following issues:

1) Installation of sensors: capable of detecting whether explosives, nuclear/radioactive/chemical substances, or humans are present, or there is foreign intrusion, inside the container.
2) Verification of container interchange during gate-in and gate-out.
3) Capability of writing and reading data, including container numbers, cargo names and contents, container movement status and such.
4) Capability of networking regional and global data.
5) Dispatch of silent reports for container tampering and contraband, and of mayday reports for intrusion and tampering detection for Container Security Device.
6) Installation of nanotech sensors for detecting intrusion.
7) Use of ubiquitous availability of the world-wide web (WWW) to transmit, detect, integrate, and read the data.

4.2.2 Container Seal Improvements

For the “Electronic Seal,” there are four points that are particularly articulated by the industry: (a) Recording the date and time when the seal was activated or sealed, (b) Meeting the minimum ISO physical security standards, (c) Performing reliably in all operating environments, and (d) Capability of receiving signal via radio frequency device.

Carriers are obligated to seal all containers entering the United States with a high-security bullet seal. This applies whether or not the container is empty of loaded. Control and disposition of seals is vital and specific records or logs must be kept. There are several such products available. For example, container seal tape that changes color or appearance when opened also makes theft or tampering more

difficult to conceal. Mounted and high-value containerized shipments should receive special security attention, including:

1) Inspect seals whenever a sealed containerized shipment enters or leaves a facility. If the seals are not intact or there is evidence of tampering or the seal numbers are incorrect, notify security and/or management personnel and tally the cargo.
2) Seal all containerized shipments leaving the facility and note the seal number on the shipping documents. Inspect the contents of containers received in an unsealed condition.
3) Release seals to as few persons as possible, and require strict control of the seals assigned to them.
4) Maintain a seal distribution log, indicating to whom seals have been released.
5) Locate high-value merchandise in mounted containers or trailers in a special security holding area where it can be observed by management and/or security personnel.
6) When containers are mounted on chassis, secure fifth wheel by a pin-lock, which meets the minimum standards for locks and is constructed to withstand normal abuse from equipment. Hold designated management and/or security personnel responsible for storage and control of pin-locks.
7) Restrict access to special security holding areas and permit the release of containers or trailer from such areas only in the presence of management representatives and/or security personnel.
8) Record movements of containers in or out of a special security holding area, showing: date, time, seal number, name of truckman and company making pick-up, and registration number of equipment used.

4.2.3 Improvement of Locking Gear Devices

Regarding the improvement of locking gear device, attention should be paid to the ideas of locking cam and cam-keeper as well as locking bar bracket.

1) Locking cam and cam-keeper: This double action design is to have the seal attached on the hole of cam and cam-keeper, instead of on the hole of locking bar handle and handle-retainer. This design could avoid the entire locking device being removed while the seal is still kept intact.
2) Locking bar bracket: A seal can be attached in the hole drilled through the lower locking bar bracket and locking bar (the so-called “Pardo” hole). The seal will have to be destroyed before swiveling the locking bar to open the door.

4.2.4 Installation of Electronic Tracking Devices Near Door Hinges

As for the installation of electronic tracking device near door hinge, the main concept is this device is fitted close to one of the container upper door hinges, where a small sensor can register door-opening events, including the date and time. Use of high-tech devices and the ubiquitous WWW network for information

exchange can help detect and hence prevent the intrusion or destruction of containers and the cargoes will be the development all relevant industries are attempting to achieve, to strengthen the security control of containers and cargo, and hopefully to deter activists from using the containers as means for terrorist attacks.

4.3 Improvement of Operation Security Procedure

Cargo security is more than a function of physical security measures. It is also one of management resolve and institutional/procedural control. Regardless of the level of resolve and operational security procedures, total cargo security is impacted by the number of individual companies within a shipping route through which a shipment passes, as well as the number of institutional procedures it must pass. As each company has its own procedures, the security of a shipment subjected to several modes during a transit is inversely enhanced according to the number of hands it must pass. The more uniform the security controls and accountability are, the greater the level of transit integrity is. "Exclusive" shippers, i.e., those who own and operate the entire route from start to finish generally suffer the least amount of security breaches and loss from outside sources. The degree of loss and risk increases as more entities are given access and control of shipments. The private sector has made great strides in developing intermodalism providing a seamless customer-oriented transportation system, and economies of scale and efficiency. Global transportation corporation. All means of intermodal transport can be carefully integrated with trunk ocean services to offer seamless connections across continents using feeder services, barges, trucks and block trains.

4.3.1 Carriers' Practices

Carriers who place the most management emphasis on security have the most successful security programs. These carriers tend to have established standards for all contract carriers; subject those carriers to periodic audits to ensure standards compliance; and rely on strict contractual arrangements. Further discussion based on container flow leads to the approach for implementing the industry provided best practices on business and terminal operation are hammered out as below.

1 Customer's Relation Management

It is important for carriers to set up a data center that all offices can key in and read it simultaneously instead of using the data by transmission. Customers' profiles that include basic information likes name, address, telephone can be set up in data base from the first sales call. In other words, all sales can read it and modify it wherever the customers are, especially for the global account.

In case of dangerous cargo, the explosions at sea of Hanjin Pennsylvania on November 11th, 2002 were caused by individual account. The customer of this kind of cases declare fault commodity with lower ocean freight. It's the reason why carriers should establish the customers' profiles to avoid such incidents. Therefore, the abnormal shipment could be detected when the customer make the booking in the integration system.

2. Trucker Management

Truckers would cause loss to ocean carriers if they could not deliver the containers properly. Generally speaking, trucker companies in USA usually get the license within a state. If the trucker needs to deliver the cargo across more than two states, she has to apply the special license. How to know if the trucker gets the suitable license? Carriers should set up the system to establish truckers' data, especially for insurance number. The job order is assigned to qualified trucker companies only. The integration system with customer profile, trucker data base, etc. is required for accepting booking & assigning work order. The alarm mechanism is shown up when the customer has no credit for casher's reference to release B/L or when the truck company's insurance is invalid to stop the work order. Furthermore, carriers could sort out the trouble cases of customers then find out the key point to set up more criteria to avoid it happens.

3. IT Development

Nowadays, the services that carriers could provide are almost the same. The competition of key point is IT that includes integration system for documentation, equipment, pricing, booking, etc. Inland movements can be tracked by EDI no matter in terminal, rail ramp or anywhere en route. Retailer and department store could distribute the containers on the way. Every shipper could monitor where the container is by cargo tracking on web site. Meanwhile, some global customers also ask for electronic B/L printing from web site. In other words, the more movements can be controlled, the more security of containers is secured. In addition, the data between customers and carriers can be read the same simultaneously. If there's any discrepancy from the actuality, both of them can reflect immediately to rectify.

IT could help to set up criteria at every check point with auto message to alarm users such as "abnormal commodity" prior to sending the job order to trucker, etc. Comprehensive system can help carriers to save cost and reduce man power on manual checking time by time. The most important is security can be achieved by system in lieu of man. System runs around the clock without holiday.

4.3.2 Procedures of Port and Terminal Operations

For this phase of "practices" identification indicates that each participant in

the transportation of cargo is actively engaging in practices that are designed to maintain, or in some cases increase, the integrity of security systems while achieving increased security of the cargo in transit. Successful preparedness ensures the selection of optimal policies and procedures, their documentation in clear and widely distributed plans, their integration into Standard Operating Procedures (SOPs) wherever possible, and their effective implementation through comprehensive and effective training programs and drills.

Conduct a program of periodic security seminars for all employees involved in cargo handling and documentation processing, stressing the importance of (a) Maintaining legible and accurate cargo tallies, (b) Processing only legible documents, (c) Writing only in ink or ballpoint pen, (d) Completing all information required by shipping documents, (e) Obtaining clearly written signatures, (f) Safeguarding the confidentiality of shipping and entry documents, (g) Maintaining good cargo security generally, and (h) Including posters, stickers, payroll stuffers, monetary incentives, and properly worded reward signs in the security awareness program.

V Conclusions and Suggestions

5.1 Conclusions

In the matter of relevant regulations and laws, inclusive of international and US domestic stipulations, the problem for loading ports in Asia area might lack of sufficient finance support. The expense of carrying out related stipulations may hinder the cargo flow, incur extra expenses, and result in potential liabilities. Not every country is so rich enough to invest and inspire ports with such capital and award.

Security measures involve a lot of human factors, so as to affect the effectiveness. The small shipping company may face challenges in developing its ship security plans and the certification for lack of any security background. There arise the issues of how to effectively and efficiently implement relevant laws and regulations to ensure establishing a quality approach for efficiently and effectively implementing said rules.

In addition, strong requirements from buyers make suppliers and carriers have no choice but comply with said rules. American retailers strongly support security initiatives to safeguard the US from the introduction of dangerous weapons and persons while also protecting retailers' supply chains and brand names. In the meantime, most of them are located in the USA. Developed countries think any large port would require a number of scanning devices capable of detecting nuclear

or other weapons inside shipping containers to upgrade security without impinging on the international supply chain of goods. It's workable to address the development and delivery of integrated in-transit visibility, cargo security and mobile asset management solutions for the government, as well as other government agencies, port and terminal operators, and commercial customers by using the supply chains system with RFID based data collection and management capabilities. However, neither RFID nor smart container could be afforded by carriers. Obviously, not every port could afford to pay such a price. 911 was a significant and tragic event but it should not establish the paradigm to shape considerations for maritime security and the momentum of trade.

The worse one relates to customer satisfaction. Relevant regulations may change from time to time aiming to prevent security threat in different circumstances. To strictly and effectively implement the relevant laws and regulations will provide a safe operational environment for ships, cargoes and personnel. However, it may impede the efficiency of cargo flow that's caused the complaints from customers since they might expect a service with smooth cargo flows, short transit time, lower transport cost, safety, convenience, and transparent information systems, etc. Meanwhile, the additional workload and the charge of AMS filing per bill of lading that's assessed on customers are also the reasons of complaints. In other words, the more rules are required, the lower satisfaction is going to be reflected from customers.

5.2 Suggestions

Based on the results of this study, some recommendations could be concluded to maritime management.

1) SOPs

To cope with security requirements and achieve service standards, shipping companies and port facility operators shall establish their companies' security and service policy as well as the procedure for the performance of such a policy.

2) The Just In Time (JIT) system

Under the influence of new security measures, greater restrictions on public access and greater trace-ability of goods can be expected. This implies more fences and gates, more security networks. The effect of this will not stop terrorist activity but shift it to other areas of the transport chain. Any disruption can inflict severe costs. What we need is agile systems encompassing flexible security measures that easily adapt to a particular threat. The final objective of any security measure must be to protect the commercial core of society.

3) A 100% screening of all containers is not yet feasible

The approach to maritime security has to be different from that of aviation security. The issue of a container loaded with destructive capability being used to penetrate

deep into a country before being activated is credible scenario but a 100% screening of all containers is not yet feasible. Fences, gates, walls, etc are only good if they work 100% of the time. If they do not, they only create a belief of security, which can be dangerous because it can lead to reduce alertness.

4) Total Quality Management (TQM)

TQM can be very powerful to address supply chain security concerns. Quality movement emphasizes prevention, source inspection, process control, and a continues improvement cycle. These are all ingredients for successful and effective ways to manage and mitigate the risks of supply chain security.

5) EDI transmission between customers, ports, terminals, truckers and rails

All containers can be controlled from making the booking to final delivery in the integration system. The site is equipped with comprehensive monitoring and control systems which interface with instantaneous evaluation for booking system of alarms at the precise commodities which danger occurs. The integration system can make the cost down. Trying to mirror the scenarios faced by users/customers and emulate what other carriers testing personnel do, in terms of how the user is staged and the factors being tested. The leading-edge perimeter detection systems are capable of detect security problem. The establishment of a new organization can provide integrated real-time information solutions and services for securing and managing global supply chains to make their supply chains more efficient, dynamically responsive and secure.

Global collaboration in support of maritime security with information exchange, shared intelligence and trans-national cooperation in R&D are some of the areas in which the foundations of maritime security should be anchored. Sharing common interest which removes the element of conflict at the interfaces of several self interests. To build a more comprehensive system for scanning cargo containers rather than jumping immediately into a 100 percent scanning mandate that would have snarled retail supply chains and possibly increased security problems rather than minimizing risks. One hundred percent scanning is currently operationally infeasible, technically unreliable and would cause unacceptably high economic costs and disruptions to the economy while offering no real improvement to the nation's cargo security system.

Offering customers complete, integrated solutions, including powerful analysis tools that will enhance their situational awareness, security, and decision making in tracking and managing shipments every step along the way as they move through global supply chains from point of origin to destination to meet these significant challenges.

References

1. Barry Mawn, 1996, $38 Million in Stolen Goods Recovered, *FBI Special Agent as quoted in the Philadelphia Inquirer article*.
2. Campbell Roy, 1991, Study in Crime, *Cargo Systems*
3. Chang Chih-Ching, 2005, Port Preventive Measures and Cicil Liabilities in Connection with Terrorist Attacks, *International Association of Airport and Seaport Police 36th Annual Conference*.
4. Chang et al., 2003, Problems Concerning Ship's Implementation of the ISPS Code, *The new Challenge of International Transportation Security*
5. Chin K.L., 1999, Smuggled Chinese, *Clandestine Immigration to the United States*
6. Gilmour T.H., 2003, A letter to Liberia, *US Coast Guard, Ref 5500/MTSA*.
7. Hickey K., 1999, NATC introduces intermodal transportation simulation system that is clearly not a game, *Journal of Commerce Inc*.
8. Hoaglund Robert F CPP, 1990, The Making of a High Security System, *A Presentation at American Defense Preparedness Association*.
9. Hough R., 2003, Maritime security – a summary of the ISPS code, Britannia News, http://www.britanniapandi.com/publications/britnews/pdf/britnewsmay03-3.pdf, 6-9.
10. International Chamber of Shipping, Guidance for Shipowners, Ship Operators and Masters on the Protection of Ships from Terrorism and Sabotage. MSC 75/ISWG/INF.1, Nov. 2001.
11. International Maritime Organization, 2002, International Ship and Port Facility Security Regulations and Codes, Chapter XI-2 of SOLAS and its Codes.
12. Korkuch MaryrLu, 1996, *High Tech Cargo Theft*, A Presentation at the U.S. Capitol, Executive Director, Technology Theft Prevention Foundation.
13. Leeds Jeff, 1997, Special Report: Cargo Theft, *Los Angeles Times*.
14. Lloyd's Register, 2003, International Ship and Port Facility Security Code – Practical Pack, 6-8.
15. Ministry of Mercantile Marine, 2003, Sea Borders and Illegal Immigration, Greece, http://www.mmm.gov.gr/mmm/politics/immigration/illegal/en/index.asp.
16. Morganelli J. M., 2003, The Subcommittee on Immigration, Border, Security and Claims, Testimony of Northampton County, Pennsylvania, http://usinfo.state.gov/regional/ea/chinaaliens/morganelli.htm.
17. NEP&I, 2001, Stowaways, Signals Special Edition, No.6, *North of England P&I Association, Newcastle, England*.
18. Orient Overseas, 2003, http://www.oocl.com/logistics/.
19. GAO/NSIAD-97-95, 1997, Terrorism and Drug Trafficking: Responsibilities for Developing Explosives and Narcotics Detection Technologies (Briefing Report),.

20. The Transportation Equity Act for the 21st Century. Public Law 105-178. TEA-21. http://www.fhwa.dot.gov/tea21/.
21. U.S. Customs Press Release, 2002, http://www.customs.ustreas.gov/csif.htm.
22. United Nations, 2001, Protocol Against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention Against Transnational Crime, United Nations.
23. United Stated Department of Transportation, 1980, "A Report to the President on the National Cargo Security Program, "Washington, DC.
24. US Department of Homeland Security, 2003, Final Rule, Federal Register, Vol. 68, No. 204, pp. 60483-60515.
25. US Department of Transportation, 2003, SAFETEA Safely Moving America, www.dot.gov/affairs/dot04003.htm.