行政院國家科學委員會補助專題研究計畫 ☑ 成 果 報 告 □期中進度報告

計畫名稱:以限制理論建構 U-Port 資訊系統及其行銷策略研擬

計畫類別：☑ 個別型計畫　　□ 整合型計畫
計畫編號：NSC 96－2415－H－019－007－SSS
執行期間：　96　年　8　月　01　日至　97　年　10　月　31　日

計畫主持人：陳秀育 助理教授
共同主持人：
計畫參與人員：李宗儒 教授

成果報告類型(依經費核定清單規定繳交)：☑精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
☑出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立臺灣海洋大學航運管理學系暨研究所

中　華　民　國　97　年　10　月　28　日

以限制理論建構 U-Port 資訊系統及其行銷策略研擬

Using TOC to Develop U- Port Information System and to Formulate Its Marketing Strategy

計畫編號：NSC 96－2415－H－019－007－SSS
執行期限：96 年 08 月 01 日至 97 年 10 月 31 日

主持人：陳秀育 助理教授 國立臺灣海洋大學航運管理學系暨研究所
主持人電子郵件：shiouyu@mail.ntou.edu.tw

摘 要

近年來亞太地區已成為目前全球貨櫃裝卸量發展最為快速的地區，然而台灣的國際港口卻都呈現貨櫃量成長緩慢，國際排名每況愈下。加上大陸及香港港口莫不致力於港埠建設，已對台灣港口之未來經營及發展形成重大威脅。台灣一向以科技島的美稱聞名世界，台灣政府對於資通訊科技(information communication Technology，ICT)的推廣更是不遺餘力。因此資通訊科技提供港埠經營業者在資源有限下另一套持續改善以達成預定目標的新契機。因此本研究利用限制理論結合資通訊科技管理為出發點，分析基隆港港埠管理的現況，找出瓶頸問題與提供改善方案。藉此建構資訊無所不在之安全智慧化優質航港區(U-Port)，以及其對應行銷策略之研擬。本研究發現目前基隆港推動U-Port的瓶頸有「法令限制」、「外部經濟環境不佳」、「腹地不足」、「港區基礎設施未盡完善以及各單位整合未達理想」；針對瓶頸提出之行動準則包括：內部行銷及技術的強化、政府主導、使用者付費、薪資結構的重新設計與引進新血等。最後在U-Port環境下，運用資通迅科技所形成之行銷組合分別為全球資訊網，無線射頻辨識技術與船舶交通系統以達成浸沒行銷之目標，行動通訊系統以達成轉換行銷與同步行銷之目標，而電子資料交換系統，無線區域網路，無線廣域網路，船舶交通系統以達成關聯行銷之目標。

關鍵字：資通訊科技，限制理論，U化港口，U化行銷

Abstract

Recently the rapid increase in container volume make the Western Pacific Region becomes the most rapid development region in the world. However, almost all Taiwan's international port container volume grows up slowly, and lost the competitive advantage gradually. Moreover, Mainland China and Hong Kong Governments devoted to port construction has put Taiwan ports into even worse position.

The Taiwan is famous as “Technology Island”; therefore the Government has put lots efforts on promoting ICT (information communication Technology). Therefore, the Information communication technology offers Port authorities another opportunity to continue improving to achieve “the goal”--- regain the sustainable competitive advantage in Asia-Pacific Region.

This study used the theory of constraint and combined the concepts of the valued-added port characterized with safety, intelligence, and omnipresent port. Then focus on the needs of port users, analyze the current situation of ports, identify the bottlenecks and then provide the solutions. Through these processes, this study found the main bottlenecks are “legal restrictions”, “economic depression”, “insufficient hinterland”, “inadequate port infrastructure”, and “ short of smooth integrations”. Corresponding to these bottlenecks, this study proposes workable solutions are “ enforcing internal marketing”, “ upgrading the IT capabilities”, “ Government take charge of integration”, “users pay”, “redesign the compensation and reward system”, and “recruiting new employees” etc. Finally, this study formulate U-port’s marketing strategies by using ICT applications in U-Space, that is World Wide Web, RFID and VTS/ATS in immersion marketing, mobile communications both in transformation and sync marketing, and WLAN, WWAN, EDI in

nexus marketing.

Keywords: ICT, Theory of constraint, Ubiquitous Port, Ubiquitous Marketing

一、前 言

近幾年來，由於西太平洋地區經濟快速成長，貨櫃量增加迅速，使得亞太地區港口成為目前全球貨櫃裝卸量發展最為快速的地區，故目前貨櫃裝卸量排名全球十大貨櫃港中，亞太地區即佔了六個港。然而在亞太地區主要貨櫃港埠中，台灣各國際港口大都呈現貨櫃量成長緩慢，未能到達其他亞太地區主要競爭港埠的水準，排名每況愈下。基隆港近年來持續面臨轉型的議題（蕭丁訓等人，2007）；對外面對中國大陸港口快速崛起的威脅（游振明，2003）、對內則有台北港未來加入營運的衝擊（王鐘雄等人，2004），裡裡外外實則對於基隆港的貨運吞吐量及港埠競爭力產生莫大的影響。因而本研究試圖在基隆港被迫轉型之際，利用持續改善的限制理論為基隆港尋求可能的因應策略方案，進而藉建構資訊無所不在之安全智慧化優質航港區(U-Port)，以及其對應行銷策略之研擬，期望能找出提升基隆港附加價值優勢之轉型方向供有關當局參考。

二、文獻探討

2.1 加值港區

隨著時代的演進，港埠功能隨之演進，承如上節文獻當中所描述之各年代港埠功能的變化。因而我們可以得知，站在託運人或是航商等各式運送人的立場上來看，今日港埠使用者所選擇的港埠重視因素，已非昔日貨物處理能力之效率優劣，而更加重視的是港埠當局所能傳遞給港埠使用者的價值與利益來加以考量。否則僅止於港埠生產力（港埠營運效率）之高低來與其他港埠競爭者做為區別，最終還是會落於價格上的競爭，因此如何創造自身港埠的價值而形成與對手的差異化，是現今港埠當局所要頭痛的問題。

以下茲以聯合國報告書中（Economic and Social Commission or Asia and the Pacific, 2002）所研究之相關港口加值議題加以論述，此報告書中將港口加值議題主要區分為兩大塊：一是港區物流中心；二則為自由貿易港區的探究。

2.1.1 國際港區物流中心

相對於處理單一國家境內物流作業的國內物流中心，港區物流中心必須處理多國間的物流業務，其作業上的複雜性與困難度相對較高，所需具備的設施及提供的功能亦較國內物流中心繁多。另外，交通部運輸研究所（1993）提出國際港埠物流中心 (International Port Cargo Distribution Center, IPCD)之概念，認為「國際港埠物流中心」除了一般海運貨載之進出口作業外，尚可在港埠中進行分類倉儲、銷售推廣等工作。經濟部加工出口區管理處（1996），對港埠型物流中心之定義為：對港埠中流通的貨載提供加工、分類、整理、倉儲、配銷或推廣等功能性服務，並結合內陸運輸公能將貨物配送至消費市場，或以海運進行再出口（或轉運）至其他區域，以形成一結合貿易、港埠、運輸唯一貫作業的物流中心。丁吉峰與梁金樹（2002）也提出，港埠以國際港埠物流中心為其策略性發展的服務要項，進而吸引其他國際相關聯物流產業駐留本地，因而形成緊密結合的上、中、下游的「國際物流群」（International Logistics Cluster）之產業關係，稱之為「國際港埠物流中心」。

回顧台灣的港埠物流中心之發展概況，根據交通部針對海運轉運中心的規劃，台灣地區國際港埠的發展策略之一係以境外航運中心為先導，進而由運輸型的轉運作業帶動加工型的轉運作業，以期促成高附加價值的區域型物流，以及加工再出口新興生產和服務業之發展。自九十年代開始，國際港埠物流中心已成為國際物流發展中相當重要的一環，而傳

統的海洋運輸只提供貨主港到港（port to port）的運送服務，已無法有效滿足大多數要求戶到戶（door to door）的貨主需求。有鑑於此，加強傳統內陸運輸與海運整合及未來接合陸、海、空整體運輸服務是必然的趨勢。又由於各國的內外環境與條件不同，故其設置的國際物流港埠中心的類型也都各有不同，但其主要設置理由不外乎為降低物流總成本與創造更多的附加價值。

2.2.2 港區自由貿易中心

目前主導國際貿易流通樞紐、集散和交易中心者，是分布在全球的六百多個自由貿易港。跨國公司更是廣泛利用「自由貿易港」來佈局，以推動全球化的生產網路和內部貿易。就自由貿易港區一詞，國際間因其不同的設立目的與功能而有不同之命名稱，包括自由港市（Free Port City）、自由港（Free Port）、自由港區(Free Port Zone)、自由貿易區（Free Trade Zone）、加工出口區（Export Processing Zone）、保稅區（Bonded Area）、對外貿易區（Foreign Trade Zone）、關稅自由區（Customs Free Zone）等（交通部運研所，2006），但其背後精神皆是一致的，即泛指由政府港區附近劃定一特定範圍，區內貨物與人員可自由進出不受海關的管制，可免除種種繁複之行政手續，且企業可於區內進行裝卸、儲存、製造、加工、組裝等各種物流活動，是希望創造自由流通的貿易環境，以吸引外商與促進貿易發展。

2.2 國內三大國際商港加值現況

依據我國「自由貿易港區設置管理條例」第三條規定，其所謂自由港區事業：「指經核准在自由港區內從事貿易、倉儲、物流、貨櫃（物）之集散、轉口、轉運、承攬運送、報關服務、組裝、重整、包裝、修配、加工、製造、展覽或技術服務之事業。」自民國 92 年 7 月 10 日通過「自由貿易港區設置管理條例」之立法，交通部遂積極推動基隆港、台北港、台中港、高雄港、花蓮港及桃園航空貨運園區等海空港「自由貿易港區」相關設置規劃作業，目前績效如下表一：

表一 國內自由貿易港區實際營運效益表

統計年月：96 年 1-12 月　　單位：新台幣千元

指標 / 各港區	進出口貿易值			
	進口	出口	合計	佔百分比
基隆港自由貿易港區	713,186	1,104,368	1,817,554	3.05%
台北港自由貿易港區	1,918,893	2,857,834	4,776,727	8.01%
台中港自由貿易港區	7,992,256	4,722,480	12,714,736	21.32%
高雄港自由貿易港區	1,778,762	1,334,914	3,113,676	5.22%
桃園航空自由貿易港區	20,492,782	16,709,715	37,202,497	62.39%
總計	32,895,879	26,729,311	59,625,190	100.00%

資料來源：基隆港務局

2.3 U 化之資通訊科技

Park (2003)曾探討資訊無所不在之商務型態(U-Commerce)所應用的資通訊科技，包括：行動通訊中的 3G，也就是全球無線通信系統(Universal Mobile Telecommunications System，UMTS)；而作動器科技乃是能夠根據感受器所接收資訊而有具體行動，其所應用之範圍十分廣泛，比如在晚上因為感應到行人而忽然亮起的燈也是作動器科技的應用；此外，Adhoc Networking 是區域無線網路的一種，其功能為通信器材間可以互相溝通而形成

網絡，而不需固定的硬體設施；最後，還有可收集生理與行為等資料並加以辨識的生物測定科技(biometrics)等。Gersham(2002)認為資通訊科技讓遠端服務提供者能夠透過隨時隨地的網路連結作為服務提供的管道，可以透過感測網絡(Sensor Network)收集當地消費者的資訊，並且可以透過作動器科技(Actuator)與區域通訊聯繫來影響使用者環境中的事物，這些技術包含全球定位系統 GPS、無線射頻辨識技術 RFID、3G 行動通訊、生物測定技術 Biometrics 等。Acquisti(2005)則指出無所不在運算能力(Ubiquitous Computing)的應用科技包括自動辨識技術(Auto-ID)，如：無線射頻辨識技術(Radio Frequency Identification, RFID)；通訊系統，如：全球行動通信系統(Global Standard for Mobile Communication, GSM)，還必須有感測網絡(Sensor Networks)與全球定位系統(Global Positioning System, GPS)相互搭配，才能精確地判讀出目標物所在的位置。Hwang(2005)也指出，傳統供應鏈的資訊系統並不能滿足其作業流程中對於資訊的需求，而未來各種自動運算技術、無線網絡環境、RFID 等資通訊科技的發展將改變供應鏈與運籌管理，在 U 化的供應鏈(U-SCM)之下，間接成本、直接人力成本、總存貨成本、作業錯誤成本等各種成本將平均下降 30%，而各種運送、存貨的資訊準確度也將有所提昇。

除了廣泛地探討未來將應用在生活與商業行為中的資通訊科技之外，也有文獻專門針對港埠所能應用之資通訊科技，茲回顧如下。張雅富等人（2005）對新世代碼頭之經營規劃與設計，將貨櫃碼頭系統所用到的管理系統茲分如下：無線射頻技術、網際網路與企業網路、自動音效回報系統、光學字元辨識系統、電子資料交換系統、遠端閘口作業系統、自動堆疊系統、衛星追蹤與全球定位監視鏡頭等。而在現在物流技術與戰略雜誌（2006）中也提出港區企業用動態指派倉儲管理系統，該系統對於接單與進貨驗收作業、入庫上架作業、出庫理貨作業、儲位移轉作業以及盤點作業等皆有其一定之效益。另外張雅富（2003）以新加坡資訊流為例，探究港埠 EDI 整合之狀況，文中提及新加坡所發展之 TRADENET 係同時整合了貿易業、銀行保險業、港務局、貿易發展局、海關以及區域主機等，有關海運產業之整合，直接影響了簡化表件的效益以及船舶滯港的時間，並且對於自由貿易港區內貨物流通最有效率管理。李國良（2000）所提出台灣地區發展智慧型港埠運輸系統之初步探討研究中，構建出台灣智慧型港埠運輸系統包含了以下兩個主要系統：智慧型港埠運輸系統平台、智慧型港埠交通系統。而其中所應用之技術涵蓋衛星定位系統（GPS）、差分定位校正系統（DGPS）、無線通訊系統、地理資訊系統（GIS）、電子地圖資料庫、車輛導航系統、車輛追蹤系統（AVL）等相關資通訊科技運用於港口領域上。

2.4 U 化的行銷模式

資通訊科技的發展不僅促進了商務模式的進化，同時也帶動了市場形態的演變。傳統面對面交易的實體市集(Marketplace) 逐漸被虛擬市場(Marketspace)所取代(Rayport & Sviokla,1994)，顧客可以透過電腦網絡在虛擬市場進行產品或服務的資訊交易，U-Space (Watson et al，2002)則整合且超越了傳統實體市集與虛擬市場空間，擴展了行銷的理性界限，也將行銷帶進了新的領域空間。 隨著服務的傳遞是在特定時空或是隨時隨地進行，以及顧客接受服務時是否具有知覺感受等，在行銷的重點將有所不同，Watson 等人(2002)以這兩個構面為基礎，將未來U 化的行銷模式劃分為四種，包含浸沒行銷、轉換行銷、關聯行銷、同步行銷。

三、研究方法與問卷分析

本研究即同時運用質化與量化之研究方法，探討港區之核心問題與解決方案，並利用量化的數據調查港區使用者之需求並將其需求做重要性之排序動作，進一步透過資通訊業者訪問，加以導入合適之資通訊科技與對應於 U-port 的行銷戰略以迎合港區使用者需求，追求港區的改革創新。研究方法主要為限制理論，灰關聯分析及使用者與資通訊業者問卷。

3.1 限制理論

限制理論是 Eliyahu Goldratt 在 1992 年提出,該套理論主要是以邏輯推演的方法歸納出組織流程的核心問題，並找出管理方案來達成預定之目標，並對過程中所面臨之限制（或稱為弱環節）加以逐一突破，以提昇整體效率與績效。限制理論的運用已經被各個領域廣為接受，儼然成為當代具代表性的管理思想之一。因此，本研究將運用限制理論之思維及邏輯推演工具樹圖，以建構資訊無所不在的資通訊 U 化港區。

3.2 灰關聯分析

灰色系統理論(Grey System Theory)是鄧聚龍教授（1999）所提出，在灰關聯分析中，灰關聯度是表示兩個序列的關聯程度，其數值多少並非是關鍵，各關聯度的前後排序才是最重要的訊息，灰關聯分析法可以用來處理各種不確定及資訊不完全的問題，因此被廣泛地運用在許多領域，用以處理優先順序排列的問題。本研究也擬將灰關聯分析法應用在本研究的問卷分析，以找出 U 化港區使用者所重視、能提高其在從事港區加值活動時興致之因素。

3.3 U-port 使用者重視因素之問卷

本研究是透過問卷調查方式進行，取得 U-port 使用者端的重視因素，以便順利建構先決條件樹的成立。在此所指之加值 U-port 活動乃針對業者（港埠使用者）在基隆港區內投資自由貿易港區事業或設立港區物流中心而定，因而所帶來一連串附加價值的產生。

經由以上影響加值 U-port 進駐業者之因素整理後，為求其效度，故在發放問卷之前，委託學術界在港埠相關研究領域之專家、港埠使用者等航運公司內部高階人員以及港埠當局之內部高層人員此三方立場來為本問卷做專家效度之審核，經由面談或電子郵件填寫的方式，刪除或增加了一些問項上的描述，而形成本研究，本研究問卷以李克特 5 點尺度量表進行因素重要性之調查，其中,「1」代表「最不重要」; 反之,「5」代表的則是「最重要」。本問卷以實有進駐基隆港並從事加值 U-port 活動（投資自由貿易港區事業或是從事港區物流活動）之事業體為施測對象，發放時間乃自 2007 年 10 月 1 日至 2008 年 3 月 21 日，共歷時五個月收集問卷。而在發放管道方面，主要是透過本研究者親自拜訪該基隆港區從事加值活動事業體以及透過電子郵件以夾帶表單問卷填寫的方式進行，並且收得有效紙本問卷 70 份、無效問卷紙本問卷 11 份、電子郵件回覆問卷 3 份，共計 73 份。經過灰關聯分析演算後所得的數值，茲以表二列出本問卷影響業者從事港區加值 U-Port 活動時之滿意程度因素的演算結果。

表二 影響業者從事港區 U-Port 活動時之滿意程度因素之重要性關聯度和排序

構面	分類排序	整體排序	關連度	因素
降低成本面	2	2	0.8222	港埠的作業效率
	3	3	0.7550	各項港區事業主管機關之行政效率
	4	6	0.7088	文件的傳輸效率
	5	7	0.6893	勞工的作業效率
	6	9	0.6708	單一窗口辦理相關業務
	1	1	0.8412	通關的便利性
提升附加價值面	3	8	0.6855	港區資訊系統整合
	5	11	0.6116	港務當局所提供的相關資訊服務平台
	7	13	0.5794	通訊設施
	1	4	0.7259	航港電子交換 EDI
	8	14	0.5675	先進的港區資訊作業系統
	4	10	0.6196	貨物的資訊管理
	6	12	0.6083	船舶交通系統 VTS 及 AIS
	2	5	0.7222	港埠作業整合

根據 Daniel（1961）指出，「組織的資訊系統必須集中於關鍵成功因素，而大部分產業的關鍵成功因素數目在 3 到 6 個之間」。因此，在因素項目數目的挑選上，本研究挑選前 3 群共 6 個因素作為港區創新改革所必須優先達成的關鍵因素。分別為灰關聯度最高的第一群有「通關便利行性」及「港埠作業效率」兩個因素，且與其他因素間的差距十分明顯，代表著受訪者在從事港區加值 U-Port 活動時，對於「通關便利行性」及「港埠作業效率」此兩因素的重視程度，遠遠超過其他項目。灰關聯度最高的第二群所包含的有 1 個因素為「各港區事業主管機關之行政效率」，表示港區使用者對於該從事 U-Port 活動時，不僅重視外在作業效率因素，也同時考量內部的行政效率因素。灰關聯度排序下的第三群所包含的有 3 個因素分別為「航港電子交換 EDI」、「港埠作業整合」以及「文件傳輸效率」。以上 6 個因素將作為後續限制理論邏輯推導中，港區創新之優先項目。

3.4 資通訊科技應用之問卷

根據使用者問卷共整理出 14 項影響業者從事港區加值 U-Port 活動時之滿意程度因素，並且排列出重要順序。而本節將接續進行資通訊科技應用問卷之設計與調查，透過訪問資通訊科技領域的專業人員，找出可以應用在滿足上述業者在從事港區加值 U-Port 活動時之需求因素的資通訊科技。

本研究之資通訊科技問卷主要分為三大部分，其一為列舉進駐港區從事加值 U-Port 活動等相關業者之重視因素，便於讓資通訊業者知悉從事港區加值 U-Port 活動業者之需求因素；其二為則整理出適用於港區的各項資通訊選項，便於讓資通訊業者在填寫該份問卷時，一方面能快速憑藉其專業經歷選出合適的資通訊科技，第三部份則針對 U-port 情境下四種行銷情境之對應之行銷戰略工具提出建議。本問卷填答的方式採用半開放式。亦即受測者（資通訊科技領域人員）除了能透過本研究所提供之相關適用於港區資通訊科技的彙整表以便填答；也為求研究之完整性受測者能藉由其專業來做加註說明（例如：有些科技具備相互替代性，而有些科技則有互補性，因此本研究要求受訪者必須從替代性科技中選出最佳科技，若有些科技具要互補才能發揮最佳作用，則需要加以註明），本研究問卷主要以「目前從事資通訊科技相關領域工作」之人員作為發放對象，但鑑於對於港口所採用之資通訊科技相關係屬較為特殊領域科技，因故問卷發放對象乃採用專家問卷的訪談方式進行，透過基隆港務局資訊部內部人員提供相關資通訊科技領域專家，以求其問卷施測對象之準確性。發放時間乃自 2008 年 5 月 1 日至 2008 年 5 月 30 日，共歷時 1 個月發放及回收問卷。而在發放管道方面，主要以透過一對一電話訪談，方便讓受測者以透過本研究者之解說立刻知悉本問卷主要調查內容，共得有效問卷 15 份。

四、分析結果

經由基隆港務局內部相關高階人士所提供之意見，先行列出 U 化港埠所面臨的困擾，以及相關所不願看到的結果(Undesired Effects, UDEs)：包含煩惱、焦慮的問題點、一些相關議題以及關心的問題等（Richard A. Reid＆Thomas E. Shoemaker, 2006）。在接觸四個相關部門最初所列出一共大約 62 個問題點，透過分類、整理意思相近之問題點，歸納為港區路域面積以及後線腹地不足、行政管制過多或繁雜，法令未鬆綁、外部經濟環境不佳、基礎設施的不足、港口所能提供的服務不足、組織內員工行銷能力不足、貨櫃作業量不足、貨櫃航線不足、港區土地面積不足、作業流程繁瑣、作業環境不確定感、轉運業務未臻發達、租金偏高與租稅優惠不具吸引力、貨物通關、保稅及管制作業開放度不夠、自由貿易中心無一定的法權來行使統整之力、無一個直接授權及管理的主管機關、經常受到自屬單位的行政規定之牽絆、自由貿易中心並無一套完善的推動措施、招商面積不足等、招商活動只能常處於被動的狀態、法令產生競合，常常產生雙重規範的窘境、港區設廠之物流業者不具經濟規模,綜合以上描述，描繪出基隆港自由貿易港區之現況樹，撥雲見日圖，未來狀況樹，先決條件與轉換樹，因篇幅限制，故省略限制理論相關圖形之推論過程，僅以文字說明之。

五、結論與建議

本研究以限制理論出發，從當中的三大思維模式：什麼需要改變、改變成為什麼、如何導致改變，來探討港區欲推行加值 U-Port 活動之相關議題，並根據限制理論的五個工具圖：現況樹、撥雲見日圖、未來狀況樹、先決條件樹、轉換樹等，重新檢視存在港區加值 U-Port 活動議題現況中的問題，並予以擬定理想目標，最終以港區使用者需求作為建構 U 化港區的考量基礎。以下分述下列五大工具圖當中，各個推演圖當中之發現：

從現況樹當中發現，存在基隆港發展 U 化港埠理想的當中，有五大瓶頸點：法令限制、外部經濟環境不佳、腹地不足、港區基礎設施未盡完善以及各單位整合未達理想。進一步排除外在瓶頸點，僅針對基隆港務當局有能力改變之問題點進行改善。因此，最終要突破目前基隆港在面臨「加值活動未興盛」的不良循環，必須從「港區基礎設施未盡完善」及「各單位整合未達理想」此兩大內部核心環節著手。

撥雲見日圖，本研究分別以「基礎設施需充分滿足使用者需求」及「有效率的服務程序」作為創新改革的理想目標，來作為港務當局內各部門產業的共識與努力，本研究發現，增加必要的的資源投入以及建立良好的溝通管道都可以為港區使用者帶來價值，因此探討「資通訊科技」如何解決資源利用上的矛盾。

未來狀況樹描繪出「資通訊科技加值 U-Port」的未來狀況，並從韓國釜山港推行 U–Port 計畫以及文獻當中發現「港區 U 化」可以解決港區在資源利用上的矛盾，而能同時兼顧增加資源投入及建立溝通管道等必要條件。港區的 U 化，也會直接與間接地帶動進駐廠商在從事加值 U-Port 活動時的利潤，更近一步帶動整體產業的港區磁吸效應，進而改善「港區加值活動未興盛」此一關鍵環節，有效突-Port 並非一蹴可幾，因此本研究建構「資通訊科技 U-Port 之先決條件樹」，以港區使用者重視的需求，即能滿足該需求的資通訊科技作為「加值 U-Port」所應優先達成的中間目標，這些需求包括：通關便利性、港埠的作業效率、各項主管機關的行政效率、航港電子交換系統、港埠作業整合以及文件的傳輸效率等；而根據相關資通訊科技人員的意見表示，能夠有效迎合上述需求的資通訊科技包括：全球資訊網、全球定位系統、船舶交通系統、地理資訊系統、最佳化裝載系統、行動通訊、無線射頻辨識系統、車輛導航系統、最佳化儲位管理系統、貨櫃堆放規劃系統、電子封條、無線區域網路、電子交換系統以及單一簽入系統等。然而，本研究也透過基隆港內部資訊室人員之訪談，發現在上述資通訊科技導入的過程中，可能會遭遇到的阻礙，整理成下列五大阻礙：安全層面的阻礙、整合層面的阻礙、技術層面的阻礙、成本面的阻礙以及人員層面的阻礙等，必須進行探討來解決這些阻礙。

轉換樹：因此，本研究建構「資通訊加值 U-Port」，針對上述五大阻礙提出各種行動準則，以求能順利將基隆港區轉換成應用資通訊的加值 U-Port。這些行動準則包括：在安全層面的阻礙，主要分為心理層面的不安全疑慮及實際的不安全顧慮，則分別透過著重內部行銷及技術的強化來加以突破；而在整合層面的阻礙，則主要擬從政府出面主導來整合各方所遭遇問題，另外港埠系統開發的程序係為考量依據；在成本面阻礙部分，係擬從使用者付費以及引航商加入來共同分擔；最後在人員阻礙層面部分，主要分為直接誘因及間皆誘因效果，直接誘因係從薪資上的增加來突破、間接誘因係從新血引進及教育訓練來突破。最後利用專家問卷針對U 化下的四種行銷模式，包含浸沒行銷、轉換行銷、關聯行銷、同步行銷提出應對的資通訊應用組合以有效執行U化之行銷策略。具體之行銷工具為全球資訊網，無線射頻辨識技術與船舶交通系統以達成浸沒行銷之目標，行動通訊系統以達成轉換行銷與同步行銷之目標，而電子資料交換系統，無線區域網路，無線廣域網路，船舶交通系統以達成關聯行銷之目標。

透過本研究的一連串研究過程，試圖為基隆港的未來提供一個可行的轉型方向。近幾年來台灣港埠面臨成長瓶頸，而在各界的解套方案與措施也都層出不窮，本研究期待能為基隆港再創新的契機，再現港埠興盛之榮景。

5.2 建議

本研究針對研究結果給予基隆港務局相關單位之建議如下:

►先行診視內部組織狀況，從自身利基點出發，並可嘗試從本研究所列之兩大內部核心問題進行改善，尋求轉型之契機。

►外部環境及限制係屬較為無法改變之瓶頸，建議可以從國際上找尋與基隆港條件相仿之港口，並對於該港口進行轉型之路深入調查。本研究僅提出韓國釜山港給予一個參考目標與方向，也許可以透過蒐集多方港口之轉型成功案例，給予自身一個學習之標的。

►台灣係屬一資訊強國，而本研究亦試圖從資通訊科技的導入來強化加值 U-Port 之競爭力，期望提供一個策略方針，利用本國資訊強項來帶動港口產業的發展。

►利用資通迅科技加值 U-Port 策略也許將所費不貲，本研究試擬從大方向進行考量，在基隆港考慮推動該項策略之同時，可從某一畫定區域當作一試行的作業港區當成是一個短程目標，以及用來評估其可行性的試行區域。未來，若推行能順利進行並能受到該區使用者的廣泛迴響，則可進一步規劃接下來的中、長期計畫來達成整體港埠 U 化之夢想。

六、成果自評

本計畫研究內容與原定預計達成之研究目標相符，研究結果對學術研究及港埠實務方面，均有具體成果與貢獻，曾與高雄與基隆港港務局局長分享，且獲得相對的實質建議。本研究之部分研究成果已發表於 2007 兩岸三地研討會與 2008 航海節航運學術研討會。也完成了二份初稿，將於近期內將投稿至「運輸學刊」或「運輸計劃季刊」之 TSSCI 學術期刊或 Transportation 或 Marine Policy 等 SSCI 英文期刊。

七、參考文獻

一、中文部份

1. 丁吉峰、梁金樹（2002），「台灣地區發展國際港埠物流中心之探討：整合供應鏈之觀點」，海運學報，第十期，頁 99-119。
2. 王鐘雄、盧展猷、林資源、陳榮聰、曹至宏、楊太郎（2004），台北港貨櫃碼頭營運後對基隆港營運所產生之影響及因應策略之探討，*2004兩岸三地航運與物流研討會*，中華海運研究協會，中華民國，頁227-241。
3. 交通部基隆港務局（2006），基隆港與臺北港自由貿易港區招商推動情形簡報。
4. 行政院經濟建設委員會（2002），自由貿易港區規劃簡報。
5. 李國良（2000），「臺灣地區發展智慧型港埠運輸系統之初步探討」，*中國海事商業專科學校學報*，第八十九期，頁75-94。
6. 張雅富、郭佩玲、葉乃妏（2005），「新世代貨櫃碼頭經營規劃與設計」，*港灣報導*，第七十二卷，頁34-40。
7. 游振明（2003），「中國大陸航運及港埠經營競爭力之提升對基隆港港埠經營之衝擊與因應之道」，運籌研究集刊，第三期，頁 113-132。
8. 鄧聚龍（2001），*灰色系統理論與應用*，台北：高立圖書有限公司。
9. 蕭丁訓、張志清、林光、陳基國（2007），「台灣港埠再現風華：發展加值型服務港埠之省思」，*航運季刊*，第十三卷，第二期，頁 43-54。

二、英文部分

1. Acquisti, A. (2005) ‘Ubiquitous Computing, Customer Tracking, and Price Discrimination’. In Roussos, G. (ed), Ubiquitous Commerce, Springer Verlag.
2. Daniel, D.R. (1961), “Management Information Crisis”, Harvard Business Review.
3. Gersham, A. (2002) ‘Ubiquitous Commerce - Always On, Always Aware, Always Pro-Active’. Proc. The 2002 Symposium on Applications and the Internet (SAINT’02), IEEE
4. Goldratt, E. M. (1992), *The Goal*. North River Press.
5. Hwang, H. S. (2005) ‘E-logistics/SCM Based on Ubiquitous Technology’. Proc. Conf.

Supply Chain Management and Information System (SCMIS 2005), Taichung.
6. Park, J. D. (2003), "Co-evolution in u-Commerce: Emerging Business Strategies and Technologies". Telecommunications Review, Vol. 13, No.1, pp. 48-56.
7. Rayport, Jeffrey F. and Sviokla, John J. (1994), "Managing in the Marketspace". Harvard Business Review, November –December.
8. Richard A. R. and Thomas E. S. (2006), "Using the Theory of Constraints to Focus organizational improvement efforts：PART 1－Defining the Problem", *American Water Works Association Journal*, Vol. 98, No. 7, pp. 63-75.
9. UNCTAD, (1997), "International Investment Trends Towards the 2001," pp. 8-9.
10. Watson, R. T., Pitt, L. F., Berthon, P. and Zinkhan, G. M. (2002), "U-commerce: Expanding the universe of marketing". Journal of the Academy of Marketing Science, Vol. 30, No.4, pp. 29-43.

附件一出席國際學術會議心得報告

計畫編號	NSC 96-2415-H-019-007-SSS
計畫名稱	以限制理論建構 U-Port 資訊系統及其行銷策略研擬
出國人員姓名 服務機關及職稱	陳秀育 國立台灣海洋大學航運管理學系助理教授
會議時間地點	中國大連市,2008.4.1-2008.4.4
會議名稱	International Association Of Maritime Economists 2008 Annual Conference 國際海運經濟學人協會 2008 年年會
發表論文題目	Developing Higher Maritimes Security Quality for US-Bound Trade

IAME 2008 programme

i) Organizers: University of Plymouth, UK and Dalian Maritime University, China

ii) Conference Programme

Tuesday 1 April '08

Afternoon Registration

Wednesday 2 April '08

Morning Official Opening and Plenary Session

Six keynote speakers discuss the contemporary maritime essential issues, including: seaport and beyond, sustainability, environmental protection, and corporate social responsibility in shipping industry, maritime security and port governance etc.

Afternoon Concurrent Sessions

Thursday 3 April '08

1. Editors Panel "Insights from Journal Editors"
2. Concurrent Sections

Friday 4 April '08

一、參加會議經過

本次 IAME 2008 年會由英國 University of Plymouth 與大連海事大學合辦。

1. 4 月 1 日　下午辦理報到。
2. 4 月 2 日　上午開幕式，旋即由國際知名學者對海運研究重要主題作 keynote Speech，目前較重視之研究主題包括安全、保全、環保及企業社會責任等等。
3. 4 月 2 日　論文發表。在三間研討廳同時舉行，與會者可擇其一聆聽研討。
   4 月 4 日　本人與張志清教授、林光教授合著之論文在下午 16:00-17:40 之場次發表，由本人上台發表。
4. 4 月 4 日　中午舉行閉幕式，並宣布明年年會在丹麥哥本哈根舉行。
5. 4 月 4 日　下午參觀大連港口貨櫃碼頭，運煤碼頭及油品碼頭。
6. 4 月 5 日　上午 11 時由大連搭機返台。

二、與會心得

1. 本次會議參與之學者，大都為國際知名學者，包括 Professor Wayne Talley (Transportation Research Port E 主編)；Professor John Liu (Hong Kong Polytechnic University 國際海運研究中心主任)；Dr. Derek. Styles（Maritime Policy and Management 行政主編）；Professor Jose Tongzon（Inha University）等在會場中之討論，往往能針對重點提問，其思維方式及研究領域之廣泛程度，有值得請益學習之處。

2. 職所發表之論文亦被詢及為何政府對保安之支持不足。雖當下予以回覆，認為政府與港務局對保安重要性之認知不一，但亦省思是否有以實證方式，進一步確認本論文之初步成果，再發表於國際期刊中。
3. 本次發現歐洲地區學者所發表論文題目及研究方法與台灣學術界略有不同。我們比較重視實證研究（包括以問卷調查及訪談）。歐洲學者在經濟、財務上之推論，較常使用現成數據（由管理顧問公司，例如 Clarksons 提供）。二者各有其背景及優劣。Clarksons Consultants 所提供者，亦經過精心調查。但學者必須以重金購買；並非國內一般研究學者所能負擔。而國內學者自行作問卷調查，大都限於台灣，且回收率不高，在全球觀點上及信度上往往有缺憾。

附件二出席國際學術會議發表之論文一份

請見檔案如下

DEVELOPING HIGHER MARITIME SECURITY QUALITY FOR US-BOUND TRADES

Chih-Ching CHANG
Professor, Department of Shipping and Transportation Management, National Taiwan Ocean University
2 Pei-Ning Road, Keelung, Taiwan, cchang@mail.ntou.edu.tw
Tel: 886-2-24622192, Fax: 886-2-24631903
Shiou-Yu CHEN
Assistant Professor, Department of Shipping and Transportation Management, National Taiwan Ocean University
2 Pei-Ning Road, Keelung, Taiwan, shiouyu@mail.ntou.edu.tw
Tel: 886-2-24622192, Fax: 886-2-24631903
Kuang LIN
Professor, Department of Shipping and Transportation Management, National Taiwan Ocean University
2 Pei-Ning Road, Keelung, Taiwan, b0031@mail.ntou.edu.tw
Tel: 886-2-24622192, Fax: 886-2-24631903
S.T. LIU
Ph.D. Student, Department of Shipping and Transportation Management, National Taiwan Ocean University
2 Pei-Ning Road, Keelung, Taiwan, stl@motc.gov.tw

ABSTRACT

Since the 911 terrorist-attack, those shipping companies and port operators, which are engaging in shipping service for US-bound trades, are required to pay more attention to implement various maritime security measures according to the US regulations, such as the US Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiatives (CSI) and Security and Accountability for Every Port Act (SAFE Port Act) 2006, as well as international conventions, such as the International Code for the Security of Ships and Port Facilities (the ISPS Code). However, the adoption of these security measures might hinder cargo flows, incur extra costs, and result in potential liabilities. It is necessary to develop effective and efficient ways for adopting preventive actions.

Many private sectors in shipping industry may aim to meet the minimum security requirement as imposed on by mandatory regulations. It would mainly rely on governments' efforts to provide infrastructure for effective implementation. This paper discusses the challenges for implementing those security regulations. It adopts risk management concept to provide higher quality security measures with the minimum impact on ship and port operations. This paper considers those mandatory regulations

provided by the IMO and the US government, the challenges faced by ships, port facilities, and government efforts to enforce security regulations. It aims to provide a reference to the government agencies while implementing maritime security policy.
Keywords: Maritime security measures, ISPS Code, Anti-terrorist attack, Risk Management, US-bound Trade, CSI, C-TPAT

DEVELOPING HIGHER MARITIME SECURITY QUALITY FOR US-BOUND TRADES

1. INTRODUCTION

Ship and port operations are closely connected with the efficiency of global supply chain. If a port is shut down by a terrorist attack, its economic impact will be tremendous (GAO, 2007a; Martin Associates 2001; Anderson 2002). To facilitate ship and port operations and upgrade their service quality, it is necessary to ensure port and ship security, and thus to avoid damage to those industries, such as shipping and manufacturing, while a port is closed (Chang and Chiu 2003). A number of international conventions and national regulations have promulgated, including the International Code for the Security of Ships and Port Facilities (the ISPS Code) and the US Security and Accountability For Every Port Act (SAFE Port Act) 2006, aiming to coordinate the efforts and resources of government authorities, shipping companies, port facility operators, and port authorities. These regulations require parties concerned to discover security threat and adopt preventive measures to safeguard the ship, their crew or passengers, the cargoes, port facilities and relevant properties from terrorist attacks. It is especially true for those ships and port facility operators, which handle US-bound cargoes. They have been required to meet high security standards provided by the US laws and international conventions.

On the other hand, the adoption of these security measures faces certain challenges. For example, it may hinder cargo flows, incur extra costs, and result in potential liabilities if a security threat causes loss of life or damage to the goods or properties. There arise the issues of how to effectively and efficiently implement the security measures in order to provide high service quality in maritime transportation.

By reviewing relevant laws, regulations and documents, and interviewing company security officers of several shipping companies, this article analyzes the challenges for implementing security measures, especially those required by the US laws or regulations. It adopts risk management concept in order to provide solutions and suggestions parties concerned.

2. CHALLENGES FOR IMPLEMENTING MANDATORY SECURITY REGULATIONS

It needs to examine the contents of mandatory requirements provided either by the International Maritime Organization (IMO) or by the US government in order to discuss challenges and solutions relating to the compliance with the requirements.

2.1 Security Measures Required by the ISPS Code

IMO has promulgated the ISPS Code, which aims to establish an international framework involving co-operation between governments, administrations, shipping companies and port authorities to detect a security threat early and to take preventive measures against a security threat or terrorist attacks. The ISPS Code provides the following functional requirements (Chang and Chiu 2003):

(1) Gathering and assessing information with respect to security threats and exchanging such information with appropriate governments;
(2) Requiring the maintenance of communication protocols for ships and port facilities;
(3) Preventing unauthorized access to ships, port facilities and their restricted areas;
(4) Preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;
(5) Providing means for raising the alarm in reaction to security threats or security incidents;
(6) Requiring ship and port facility security plans based on security assessments; and,
(7) Requiring training drills and exercises to ensure familiarity with security plans and procedures.

Because each country has its own legislative procedure, lawmaking priorities, security and financial background, the degree of implementation of the ISPS Code differs in countries. Also, national regulations may change from time to time aiming to prevent security threat in different circumstances. Shipping companies and ship's crew usually face confusion while calling at different ports, or different port authorities require them to meet the requirements of new laws or regulations. Moreover, in lack of applicable legal framework, government and the port authorities may face difficulty in exercising their public power to check the identity of suspected terrorists, inspect transportation equipment, and detain a suspected property or cargo.

In some areas, terrorist attacks are often connected with local politics and social order. Some countries may not allocate significant resources to implement the ISPS Code. Also, the problems of piracy may attract more concerns from shipowners or ship operators than security threat, although ships are vulnerable to security threat in those waters where pirates dominate. The problems of security and piracy may have close connection.

The framework and process of adopting security measures as provided by the ISPS Code are shown by Figures 1(Chang and Chiu 2003) and Figure 2 (Chang 2005).

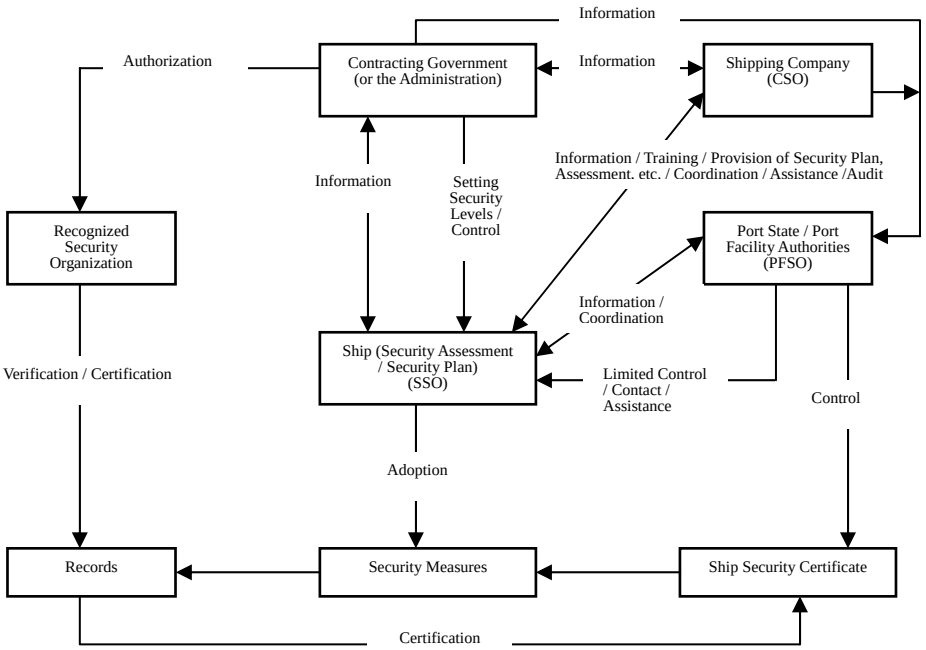

Figure 1 Framework and process for implementing ship security

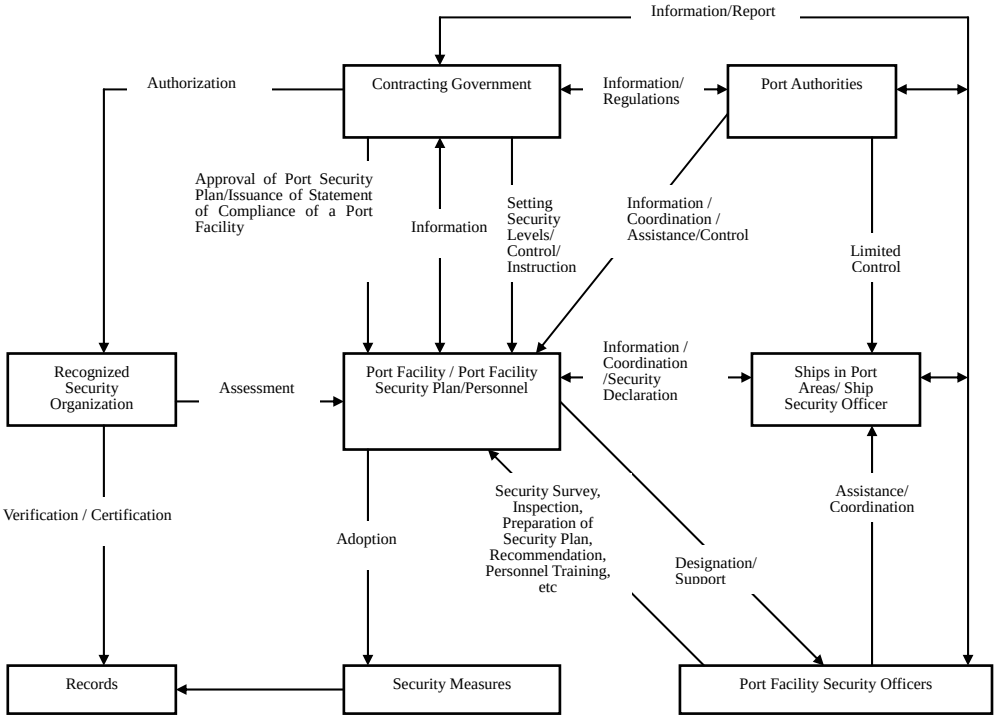

Figure 2 Framework and process for implementing port security

2.2 Security Measures Required by the US Government

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

The C-TPAT is a voluntary program that enables CBP officials to work in partnership with private companies to review the security of their international supply chains and improve the security of their shipments to the US. The program directs to establish uniform standards for secure facilities, assets and equipment, procedures, and personnel

throughout the supply chain, including the importers, carriers, and third parties. Nevertheless, the implementation of the C-TPAT needs to improve its effectiveness and management (GAO 2007b).

2.2.2 The Container Security Initiatives (CSI)

Under the CSI, foreign governments sign bilateral agreements with the US CBP to allow teams of US Customs officials to station at foreign seaports in order to identify cargo container shipments at risk of containing weapon of mass destruction. This program aims to extend the US zone of security by pre-screening containers posing a potential security risk before they leaves foreign ports for US ports. It will enhance container handling efficiency through the supply chain at the US side, while carriers and shippers have to invest huge capital on system development at loading ports to comply with the CSI.

The CSI program faces the following challenges:

1. To ensure sufficient and qualified staff for targeting high risk containers.
2. To develop an international consensus on sovereignty concerns and technical requirements (GAO 2007).
3. To ensure that designed high-risk containers are inspected by continuously refining the performance measures, and to track the effectiveness of CSI program by streamlining the number of measures it uses.
4. To continuously refine its automated targeting system (ATS), which has been designed to analyze shipping information and identify suspicious containers, based on shipping information (manifest, bills of lading, and entry data).

2.2.3 24-Hour Advance Cargo Reporting

Under 24-hour Rule, each carrier, including Non-Vessel Operating Common Carrier (NVOCC), is requested to file manifest data with the US CBP, 24 hours before loading containerized cargoes at a foreign port aboard a ship bound for the US. This practice might cause a serious disruption of the information flow and documentation procedures for the international shipping trade, especially for NVOCCs. However, merely filing and examining manifest may not provide sufficient information for detecting high-risk containers. It needs much more information, including transshipment information through a foreign port. Furthermore, it would be difficult to inspect those cargoes while they remain on board the ship within a foreign transshipment port.

2.2.4 SAFE Port Act 2006

The US Security and Accountability for Every Port Act (SAFE Port Act) 2006 was enacted to provide a comprehensive legislative measures to the US government. It includes the following provisions:

1. It codifies the CSI and the C-TPAT. Two programs are administered by US CBP to help reduce threats associated with cargo shipped in containers. It also established the Domestic Nuclear Detection Office (DNDO), which is responsible for conducting research, development, testing, and evaluation of radiation detection equipment;
2. It requires interagency operational centers where agencies organize to fit the security needs of the port area at selected ports;
3. It sets an implementation schedule and fee restriction for Transport Worker Identification Credentials (TWIC);
4. It requires all containers entering high-volume the US ports to be scanned for radiation sources by December 31 2007 (but, it appears that the government agencies failed to meet the scheduled deadline);
5. It requires additional data be made available to the US CBP for targeting cargo containers for inspection;
6. It contains possible changes to the 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.

3. CHALLENGES FOR SHIP'S ADOPTION OF SECURITY MEASURES

Ships may face the following challenges while adopting security measures:

3.1 Gathering, exchange and judgment of information

The collection and judgment of security-related information might be beyond the level which company security officers or ship security officers can deal with. Such a burden will be mainly on government authorities. It would be difficult to require shipping companies to allocate significant resources in the collection of security-related information. Also, the information collected by governments may be treated as confidential and may not be circulated widely among commercial circles enabling shipping companies to inform their fleet for taking appropriate measures. Nevertheless, a shipping company must carry out background checks for its current and future employees, and provide its shipmasters updated security-related information, including:

(1) Who is responsible for appointing the member of the crew or other persons currently employed or engaged on board the ship, especially when the employment of the crew are arranged through a ship management company.
(2) Who is responsible for deciding the employment of the ship, especially when the ship is chartered out, and the charterer is entitled to decide the employment of the ship.
(3) Who are the parties to charterparties, especially when the ship is employed under the time charter, including the identity of the sub-charterer, and relevant information for

keeping awareness and taking preventive measures, if necessary.

3.2 Time-consuming problems

It would consume much time in the following issues:

(1) It takes time to cultivate skilled staff, including company security officers and ship security officers, in order to require him to possess security knowledge, and take appropriate responses or measures. It would be difficult to require a chief officer to undertake complicated security task, and to be familiar with the assigned security duties at all security levels, if he only accepts several training courses.

(2) It also needs a long period of time to ensure all security-related personnel in shipping companies to aware the full contents of their security duties, and effectively adopt appropriate measures.

(3) Each government needs sufficient time to enact relevant laws and regulations, as well as administrative procedures, for implementing the maritime security measures.

3.3 Coordination and cooperation

The ISPS Code and certain US laws and regulations require coordination and cooperation among those parties concerned while implementing security measures. There exist challenges if one of the parties fails to meet the following requirements:

(1) The shipping company or the company security officer must ensure all personnel capable of responding to a security threat or breach of security. And, the shipmaster shall liaise at the earliest opportunity with the port facility security officer of the port the ship intending to visit.

(2) A ship security officer shall coordinate various personnel while the ship is handling cargoes, stores, or bunkers. He must report to the company security officer any deficiencies and non-conformities identified and record all security incidents. It becomes crucial to maintain ship-to-ship or ship-to-facility interface operations for each security level in a successful preventive action.

(3) Government agencies should establish the best methods and procedures in order to provide information to those ships flying its flag or intending to enter into its ports or staying at its ports. In the case of an imminent attack, the flag state should recommend certain security measures to be adopted by the ships, e.g. searching for assistance from nearby coastal states, and procedures for liaison between port facility officers and ship security officers. Nevertheless, for those ships flying flag of convenience, their flag state is usually unable to provide the above support effectively and timely.

3.4 Ships' abilities to implement the required measures

Except for those routine works in navigating their ship, Ship's crew have to meet various requirements demanded by the IMO Conventions, including the on-duty training and

requirements provided by the International Safety Management Code (ISM Code), and those security measures according to the mandatory regulations. Ships or shipping companies may face the following difficulties in implementing security measures:

(1) Since the ship security officers are trained by the company security officers of the same company, it is doubtful whether the result of the training is satisfied.

(2) Small or medium shipping companies may be difficult to develop its ship security plans by themselves for lack of resources. Shipping companies have to bear extra costs, including the training and the certification costs for company or ship security officers, the costs for installing, maintaining security equipment, and the costs for the assessment of ship security plan, etc. Such accrued costs may not be fully shifted to cargo owners by assessing a surcharge.

(3) There exist certain problems of heavy working load imposed on seafarers. Their overloaded burden might result in less effectiveness while implementing security measures (Lin and Jeng). If the number of seafarers has to be increased in order to carry out the above tasks effectively, it would inevitably increase the ship's operating costs.

4. CHALLENGES FOR PORTS' ADOPTION OF SECURITY MEASURES

While implementing security measures, ports and port facility operators may face the following challenges:

4.1 Personnel abilities and awareness

While port authority and port facility operators are ensuring their employees have competence, and the ability to deal with security threats, they may face the following difficulties:

(1) Port facility security officers have to coordinate among ships, shipping companies, port authorities, governments, local administrations, and any other entities connected with security. To deal with port facility security matters, they should remain in the port authority facility organization. However, their command and coordination systems shall not be limited to the port organization structure. For the purpose of achieving better performance, port facility security officers, including those working for privatized ports, shall be authorized to undertake their duties independently.

(2) Maritime security exercises would benefit from timely and complete after-action reports, increased collaboration across government agencies, and broader port-level coordination. Comprehensive security training, drill and exercises will ensure those people whose job is to maintain security to perform their job properly (Hawkes 1989). However, a port security exercise improvement plan has to overcome the following difficulties: (a) how to set the scope of the program; (b) how to complete after-action

reports in a timely and thorough manner; and (c) how to ensure that all relevant agencies participate,

(3) The faster growth rate of container throughput at Far East ports will result in lack of experienced personnel, who are required to possess security knowledge, maintain awareness of all personnel, facilities or cargoes, collect and judge security-related information, and take appropriate responses or measures. The ports need to continuously hire and train new staff, and the re-assess compliance with security standards. While the US government promote some programs to upgrade security standards in foreign ports, its officials do not have sufficient resources to directly assist countries they visit with more in-depth training or technical assistance. They can only provide opportunities to identify potential areas to improve or help sustain the security measures put in place, other than sharing best practice or providing presentations on security practices (GAO 2007b).

4.2 Lack of sufficient supports

Port facility operators may not effectively implement the ISPS Code for lack of sufficient resources, for example:

(1) Lack of security information. Many developing countries might not be able to establish their own security information-gathering system and anti-terrorist strike forces by themselves for lack of know-how and sufficient financial resource. Also, certain information is deemed confidential so that how to share such information enabling port facility operators to response would be important for achieving higher quality security standard. It needs to refine security sharing procedures in order to coordinate with government agencies and other operators. Moreover, it would be doubtable whether or not every port facility can be well equipped with security alert system and fully meet the requirements.

(2) Lack of sufficient finance support. The installation of physical security measures mandated by the security plan could be an expensive matter if extensive infrastructure or modifications must be developed in port areas, such as security fencing, barriers, as well as safety guards (Hidehiro 2003). It therefore needs to determine the criteria of choosing how many measures to be performed with priority, how far or extent to be implemented, and what their performance indexes are.

(3) It would be difficult to ask a private port facility operator to allocate significant budget to improve its security facilities. Even if the port facility is run by public sectors, there still exist commercial considerations of operational efficiency.

5. GOVERNMENTS' EFFORTS TO ENFORCE MARITIME SECURITY

MEASURES

For developing higher quality security measures with resources constraints, it would mainly rely on governments' efforts, since governments are able to promulgate regulations, enforce, and control the performance of the implementation. It is suggested that governments adopt risk management approach, proper information collection and sharing, and international cooperation to achieve the above goals (GAO 2003).

5.1 Risk Management Approach

5.1.1 Risk Management Concept

Based on the security challenges discussed above, risk management approach for higher security quality can be divided into the following elements (as shown by Figure 3):

1. Threat assessment, to identify adverse events that may affect any entity, such as transportation staff, passengers, conveyances, access control, cargo and baggage, port facilities and ships.
2. Vulnerability assessment, to identify weaknesses in physical structures, personnel protection systems, processes or other areas that may be exploited by terrorists.
3. Criticality assessment, to identify and evaluate an entity's assets or operations based on a variety of factors, including importance of an asset or function.
4. Risk assessment, to qualitatively and/or quantitatively determine the likelihood of an adverse event occurring and the severity, or impact, of its consequences. Risk assessment plays a vital role in risk management approach because it links vulnerability/criticality assessments and risk mitigation.
5. Risk characterization, to involve designing risk on a scale (low, medium or high).
6. Risk mitigation, to adopt certain responsive actions by considering risk, costs, and other implementation factors. Governments have to consider an efficient way to allocate resources available, and estimate the relative impact of mitigation alternative and determine the optimal investments in these alternatives based on cost and benefit analysis. A system approach to risk management can enhance the efficiency of security efforts. It encompasses actions taken in all organizational areas, including personnel, processes, technology, infrastructure, and governance. It also integrates the capabilities of governments and commercial interests throughout the world.
7. Monitoring and evaluation, to keep risk management current and relevant, by continuous repetitive assessment process.

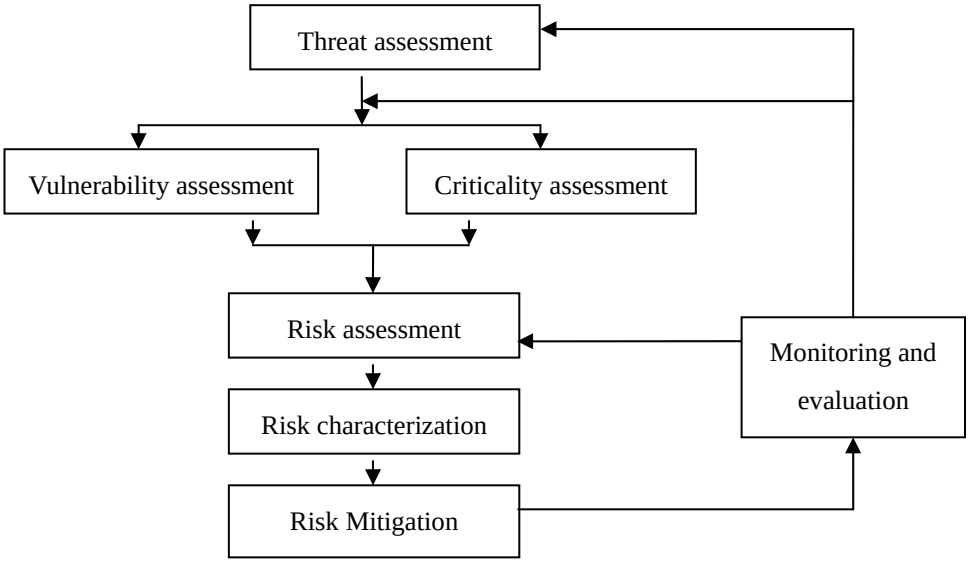

Figure 3 Elements and Process of Risk Management Approach

5.1.2 Interactive Risk Assessment Process

An interactive risk assessment process is suggested to substitute a static risk assessment process. The latter is often used to assess security threat through manifest or other information provided by carriers and cargo owners. But, the interactive risk assessment makes use of internet, satellite and biometric technologies to communicate with each other. It will determine not only specific pre-arrival information about the ship, its cargo, and its crew, but also audit those information relating to their ship managers, their owners (financial backing for the ship), their commercial charter, and the associated marine terminal operator. It will also allow those stakeholders, including arriving ships, their crews, cargo owners and terminal operators, to voluntarily link with port officials via a world-wide-web application to text communications. Such a process will accumulate an assortment of information and establish a more comprehensive database about the marine industry enterprise, and thus provide effective and efficient information for adopt anti-terrorism action.

The interactive risk assessment will also allow legitimate shipping and chartering companies and marine terminals with access to the maritime green lane, and provide the opportunities to improve port security and simultaneously enhance maritime commerce. Therefore, it would encourage those legitimate ship owners, cargo consignees or charterers, and terminal operators to voluntarily participate and answer any and all port official questions, especially while the ship is at sea, and avoid unnecessary delay.

5.2 Information Collection and Sharing

Another key component of risk management is to have relevant, reliable, and timely information available to assess performance over time and to correct deficiencies as they occur. It requires different entities to communicate effectively, including sharing information. Through information sharing, different entities and participants in a security operation can enhance the partnership and improve the allocation of resources across jurisdictional boundaries for deterring, preventing, or responding to a possible terrorist attack at the nation's ports. Nevertheless, the following measures can be adopted to further enhance security quality:

1. Domestic and international cooperation for gathering, identifying, analyzing, and disseminating key information within and among government entities. It needs to address potential overlapping responsibility for clear and coordinated actions across the agencies, such as leadership roles for Coast Guard of each country and its interagency partners.
2. Better resource allocation for investment in information system, sensor network, and facilities upgrades and expansions.
3. Establishment of new structure and procedures for effectively sharing information. It needs to develop formal procedure so that government agencies and their officials can use common databases as management tool to monitor. Also, the ability to share classified information can improve the ability to deter, prevent, and respond to a potential terrorist attack. The way information to be shared varies depending on their purpose and mission, leadership and organization, membership, and resources. It needs to raise the awareness of relevant government agencies and shipping circles about the process of applying for security clearance for information sharing

5.3 International Cooperation

The growing interdependence of nations requires policymakers to recognize the need to work in partnerships across international boundaries to achieve vital national goals. This involves all nations that have an interest in maritime security, as well as the ability and willingness to take steps to defeat terrorism and maritime crime. While enforcing those security initiatives, the US government needs to specify details of how participating countries' customs officials will implement the mutual recognition arrangement, and what benefits, if any, can be allotted to members of other countries.

The following initiatives have been suggested to be coordinated by the US Department of State (GAO 2005):

(1) Implementing standardized international security and World Customs Organization (WCO) frameworks for customs practices and standards to ensure that goods and people entering a country do not pose a threat,

(2) Expanding the use of modernized and automated systems, processes, and trade-data

information to make vessel registration, ownership, and operation, as well as crew and cargo identification, more transparent and readily available in a timely manner,

(3) Developing, funding, and implementing effective measures for interdicting suspected terrorists or criminals,

(4) Developing and expanding means for rapid exchange among governments of relevant intelligence and law enforcement information concerning suspected terrorist or criminal activity in the maritime domain,

(5) Adopting streamlined procedures to verify nationality and take appropriate and verifiable enforcement action against vessels, in a timely manner and consistent with the doctrine of exclusive flag state jurisdiction,

(6) Expanding the US Government's capacities to prescreen international cargo prior to loading,

(7) Adopting procedures for enforcement action against vessels entering or leaving a nation's ports, internal waters, or territorial seas when they are reasonably suspected of carrying terrorists or criminals or supporting a terrorist or criminal endeavor, and

(8) Adopting streamlined procedures for inspecting vessel reasonably suspected of carrying suspicious cargo and seizing such cargo when it is identified as subject to confiscation.

6. CONCLUSIONS AND SUGGESTIONS

6.1 Conclusions

Maritime security is closely connected with the maintenance of supply chains and thus significantly contributes to a country's economics. It may also directly or indirectly benefit marine transportation, port security, and public interests. For long-term success, it requires the following structures to fight against terrorism and help ensure higher quality security standards:

(1) To establish and maintain international standards of accountability. The international community has developed a compelling body of international obligations relating to counterterrorism.

(2) To strengthen coalitions and partnerships.

(3) To enhance government architecture and interagency collaboration.

(4) To foster intellectual and human capital

For ships and shipping companies, high security quality will provide a safe operational environment for ships, cargoes and personnel in the port areas although it may cause certain inconvenience and incur extra costs while implementing security measures. Shipping companies must deem the implementation of security measures as giving positive benefits and not simply as a matter of burden.

For port authorities and port facility operators, port security relies on adequate information on any change of security level, and timely reaction as required by the port facility security plan (Hawkes 1989). If a port facility operator is willing to commit the time, budget and other resources to develop and implement a security plan, it will insulate itself as much as possible from negligence liability, and achieve certain commercial advantages, e.g. to prevent the port from becoming an unsafe port, which will prevent ships from using that port.

For government agencies, as the cost of physical protective measures in terms of money and manpower might be high, maximum security measures can not be achieved under all circumstances. By means of risk management approach, government agencies can specify areas of vulnerability in order to allocate resources for adopting security measures in an ideal situation: effectiveness and efficiency. The following criteria can be applied for determining the scope of security measures (Hawkes 1989):

(1) Vulnerability of potential risks, such as the nature and sensitivity of cargoes, equipment or location, as well as evaluation of the risk by considering the capacity of potential attackers, the economic and political situation of the area involved, and the geographical location, etc.
(2) Criticality of security measures on business and operational efficiency. Alternative measures need to be considered as well as evaluation of the port facility's security requirements, the priority of protective measures, and decisions concerning the allocation of resources to better protection of the port facility.
(3) Practical limitations, such as the physical characteristics of the vessel, facility, or installation, as well as the availability of security equipment or infrastructure.
(4) Evaluation of the security capacities of all available external resources, funds, external support, and the nature of that support.

While implementing security measures, governments need to consider the benefit resulting from the balance among: (1) the competing goals of providing port security; (2) facilitating trade; (3) collecting trade revenues. The strategic objectives of government maritime security plan would focus on:

(1) preserving the freedom of the seas;
(2) facilitating and defending commerce to ensure this uninterrupted flow of shipping;
(3) facilitating the movement of desirable goods and people across US borders, while screening out dangerous people and material.

6.2 Suggestions

To overcome the above challenges, it needs to develop strategic plan, plan their better use of human capital, establish risk assessment process, and improve the operations of those

Initiatives in order to enhance the effectiveness and efficiency of the implementation of ship security. It is suggested that:

(1) For those US bound ships, which are imposed on duties of implementing CSI, C-TPAT programs, etc., shipowners and ship operators shall endeavor their efforts to adopt advanced technology for containerized cargo, such as electronic sealing system to record the movement of containers. It is necessary to embed security into commercial practices to reduce vulnerabilities and facilitate commerce**,** including the adoption of CSI, C-TPAT, 24-hour Rule. It needs to encourage the private sectors, by means of outcome-based security standards, incentives, and market mechanisms, to conduct comprehensive self-assessments of their supply chain security practices; adhere voluntarily to baseline security criteria; and implement other regulatory security measures as deemed necessary by the US Department of Homeland Security. Verification and compliance procedures by the private sector, as well as the use of technology to allow greater visibility into the supply chain, will enable the government agencies to develop more accurate processes for detecting high-risk cargo. In short, security measures must:
   a. be aligned and embedded with supply chain information flows and business processes;
   b. keep pace with supply chain developments;
   c. optimize the use of exiting databases; and
   d. be implemented with the minimum essential impact on commercial and trade-flow costs and operations.

(2) It would be helpful to adopt risk management approach to develop an effective and efficient security system, including vulnerability and criticality assessment, risk assessment, and the adoption of mitigation actions.

(3) The enactment of relevant laws and regulations is essential to implement the security measures. These laws and regulations must include those rules and procedures to inspect and detain a ship, the administrative penalties and criminal penalties for the violation, etc.

(4) It is suggested to develop a national maritime security plan, providing the following matters:
   a. Collection and exchange of security-related information;
   b. Co-operation of personnel training;
   c. Allocation of sufficient resources for the purpose of providing financial supports to port facility operators and shipping companies;
   d. Unified definition of terrorists in local laws in order to extradite them to a right jurisdiction or try the case;
   e. Implementation of port state control and port facility security measures.
   f. Promotion of international cooperation and assistance.

REFERENCES

1. Alexander, Yonah (1992) *International Terrorism: Political and Legal Documents*, Martinus Nijhoff Publishers.
2. Anderson, P. (2002) Lost Earnings Due to West Coast Port Shutdown — Preliminary Estimate (Oct. 7. 2002), http://www.AndersonEconomicGroup.com.
3. C.S. Chiu (2003) *Knowledge of Ship Security*, Jacksoon Shipping Safety Management Consultant Co., Taipei.
4. Chang, Chih-Ching (2005) *Port's Preventive Measures and Civil Liabilities in connection with Terrorist Attacks*, International Association of Airport and Seaport Police 36th Annual Conference, Section 4: pp. 1-15
5. Chang, Chih-Ching, and Chiu, C.S. (2003) Certain Problems Concerning Ship's Implementation of the ISPS Code, in L. Lan (ed) *The New Challenge of International Transportation Security*, International Symposium on Aviation and Maritime Security, pp.43-56.
6. Combs, Cindy C. (1997) *Terrorism in the Twenty-First Century*, Prentice Hall.
7. GAO (2003) *Homeland Security Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*, Testimony before the subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, United States Government Accountability Office.
8. GAO (2005) The National Strategy for Maritime Security, September 2005.
9. GAO (2007a) *Transportation Security: TSA Has Made Progress in Implementation the Transportation Worker Identification Credential Program, But Challenges Remain*, Testimony before the United States Senate Committee on Commerce, Science, and Transportation, United States Government Accountability Office.
10. GAO (2007b) *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later*, Testimony before the Subcommittee on Border, Maritime and Global Counterterrorism; Committee on Homeland Security; House of Representatives, United States Government Accountability Office.
11. Hawkes, Kenneth G. (1989) *Maritime Security*, Cornell Maritime Press.
12. Hidehiro, Okayama (2003) Trade Facilitation and Security, *15th PECC General Meeting*, September 2003, Ministry of Land, Infrastructure and Transport of Japan.
13. Krieken, Peter J. van, ed. (2002) *Terrorism and the International Legal Order*, T.M.C. Asser Press.
14. Lin, Bin, and Jeng, Yi. (2003) Impacts and Effects of the ISPS Code on Merchant Ships, *The New Challenge of International Transportation Security*, International Symposium on Aviation and Maritime Security, Taipei, p.127.
15. Martin Associates (2001) *An Assessment of the Impacts of West Coast Container*

Operations and the Potential Impacts of an Interruption of Port Operations, Pacific Maritime Association.
16. Ronzitti, N., ed. (1990) *Maritime Terrorism and International Law*, Martinus Nijhoff Publishers.
17. US Department of State (2003) *Patterns of Global Terrorism*, http://www.state.gov/s/ct/rls/pgtrpt/2003/c12153.htm.

ACKNOWLEDGEMENTS

This article is based on a research project (NSC-93-2415-H-019-003-SSS) sponsored by National Science Council in Taiwan.