LLOYD'S PRACTICAL SHIPPING GUIDES

RISK MANAGEMENT IN PORT OPERATIONS, LOGISTICS AND SUPPLY CHAIN SECURITY

General Editors: **KHALID BICHOU, MIKE G.H. BELL AND ANDREW EVANS**

informa law
from Routledge

RISK MANAGEMENT IN PORT OPERATIONS, LOGISTICS AND SUPPLY-CHAIN SECURITY

LLOYD'S PRACTICAL SHIPPING GUIDES

Other titles in this series are:

Port Management and Operations
2nd edition
by Professor Patrick M. Alderton

ISM Code: A Practical Guide
to the Legal Insurance Implications
2nd edition
by Philip Anderson

The Handbook of Maritime Economics and Business
by Costas Th. Grammenos

Maritime Law
6th edition
by Chris Hill

RISK MANAGEMENT IN PORT OPERATIONS, LOGISTICS AND SUPPLY-CHAIN SECURITY

BY

KHALID BICHOU
MICHAEL G.H. BELL
AND
ANDREW EVANS

informa law
from Routledge

First published 2007 by Informa Law

Published 2014
by Informa Law from Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Informa Law from Routledge
711 Third Avenue, New York, NY, 10017, USA

Informa Law is an imprint of the Taylor & Francis Group, an informa business

Whilst every effort has been made to ensure that the information contained in this work is correct, neither the authors nor Informa Law from Routledge can accept any responsibility for any errors or omissions or for any consequences arising therefrom.

Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

[Lloyd's is the registered trade mark of the society incorporated by the Lloyd's Act 1871 by the name of Lloyd's]

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 13: 978-1-843-11655-4 (hbk)

Text set in 9/11pt Plantin by Interactive Sciences Ltd, Gloucester

PREFACE

The 9/11 attacks and other subsequent events have fostered further dimensions to port, maritime and supply-chain security with a raft of compulsory and voluntary measures being put in place at both domestic and global levels. However, while much of the academic and the industry's attention was paid to the deadlines and prescriptive mechanisms for compliance, few or no attempt(s) was made to analyse the frameworks, models and applications of port and supply-chain security regulations and the interplay relationships between the regulatory framework, the risk element and the appropriate operational and management systems.

This book, based on the papers presented at a workshop on risk management in port operations, logistics, and supply-chain security at Imperial College London in 2006, offers a first and unique insight into the complex world of port and supply-chain security by combining selected peer-reviewed contributions from an international line-up of top-tier academic and professional experts in the field. In particular, the book addresses operational and management challenges that port, international logistics and supply-chain operators face today in view of the new security regulations and the requirements of increased visibility throughout the supply chain.

The book also offers a rare blend of academic and practitioner contributions covering a wide collection of security models and applications ranging from operational and functional subjects to management and policy issues. Both the structure and content of the book were carefully planned and drafted to encompass the multi-faceted nature and components of the global port and supply-chain security system, including the international maritime and trading systems.

This page intentionally left blank

INTRODUCTION

Khalid Bichou, Michael G.H. Bell and Andrew Evans

PORT AND SUPPLY-CHAIN SECURITY, RISK AND RELIABILITY

The events and aftermath of 9/11 have not only fostered further dimensions to global port, logistics and supply-chain security but have also triggered a fundamental shift in the way policy and regulatory instruments are drafted, managed and implemented. On the one hand, the interplay of relationships between trans(port), logistics and supply-chain networks has led to a system of layered security whereby a combination of multi-level/multi-layer contractual and voluntary arrangements is being operated for each pattern of port, logistics, trade and supply-chain configurations. On the other hand, the complexity and multi-dimensionality of the security-risk factor may require new models and frameworks of risk assessment and management. This is because probabilistic models for the analysis of safety presume that accidents are unwanted unintentional events, and that data on past accidents and precursors provide useful information about future accidents. In the case of security, the unwanted events are intentional. In that case, the past may be a poorer guide to the future, and the characteristics of the events may be very different.

In advocating a shift (i) from facility security to supply-chain security and (ii) from safety-based to security-based risk models, both operational and strategic decisions across port, logistics and supply-chain settings must be adjusted. Operational challenges stemming from the new security framework involve far-reaching issues ranging from operational planning and execution, ICT and technology applications, quality standards and processes, cost and performance models, and reliability and recovery options. Strategic challenges brought about by the new security regime include such aspects as strategic management and competitive models, policy making and implementation, information reporting and co-operation arrangements, economic evaluation and impact analysis, and financing mechanisms and cost recovery schemes.

This book addresses operational and management challenges that port, international logistics and supply-chain operators face today in view of the new security regulations and the requirements of increased visibility throughout the supply chain. The book provides a structured selection of contributions covering a wide collection of security models and applications ranging from operational and functional subjects to management and policy issues. The focus on ports in this book is rightly justified because although security measures have targeted a variety of entities and facilities across the international logistics and supply-chain community, ports stand as the only node/link that can bring together all these institutions, functions, assets, processes and flow-type elements.

AN OVERVIEW

The focus of this book is on security, risk and reliability in supply chains which are having a major impact on the port and logistics industries. The chapters can be grouped into four sets, reflecting different issues associating risk and reliability with port, logistics and supply-chain security.

The first set reviews current security programmes and initiatives in port, logistics, and trade settings, highlighting in particular the increasing shift from physical and facility security to the wider supply-chain security. The first chapter thoroughly discusses the interface between marine reporting and maritime and port security, highlighting in particular the lack of information available for both cargo and passenger manifests, as well as the ability of both maritime and port stakeholders to report and share such details with maritime authorities throughout the world. The second chapter reports on the global trade system, an industry initiative that seeks to meet both the need to improve the logistics processes to handle increasing global trade and the requirement to enhance global trade security both to and from all participating nations. This concept has, since it was first presented to the United Nations in 2003, progressed to the implementation and review phase. The third chapter analyses different systems of container security from box standardization and packaging to container loading and unloading, including while in-transit or on delivery processes. It goes on to show how container security is a complex system of interrelated activities in information and data capture and controlled re-distribution, physical surveillance of the container, and inquiries into the various actors in the supply chain.

The second set suggests different methods and applications for enhancing port security and operational efficiency. The fourth chapter investigates the use of RFID systems to enhance port operations security and uses process modelling to analyse the implementation of RFID technology in yard operations. The fifth chapter uses discrete-event simulation to investigate port recoverability from security incidents. The results from a hypothetical scenario show an increase in the number of chassis and containers in the yard, as there were not enough trucks to pick them up, as well as a large increase in the gate queue. The sixth chapter examines the security and reliability of the global container-line shipping network through simulation and mathematical modelling. The study goes on to illustrate a case study of shipping networks plying the West European and North American continents and shows how a disruption in a regional network could have wider cascading effects in global shipping networks. The seventh chapter deals with the stability and reliability of container-line schedules in the context of random events and successive ports of calls. Throughout the study, mathematical models supported by hypothetical case studies are developed to show the variability of schedule stability as the number of port calls increases. Chapter eight applies artificial neural networks to predict and test the efficiency of container-port operations. Using Hong Kong container terminals as a case study, the results show small prediction error, hence the suitability of the method in reducing operational risks and increasing reliability. The ninth chapter discusses the links between shipping alliances and terminal operations and examines how such strategic alliances could reduce operational and performance risks of port operations.

The third set of chapters provides several empirical frameworks for managing the security of global trading and supply-chain systems. The tenth chapter empirically investigates how the Business Alliance for Secure Commerce (BASC) programme, a privately-driven voluntary security initiative created in Latin America in 1996 to initially prevent legal cargo from being used to smuggle drugs, has evolved towards an integrated security management system. The eleventh chapter presents trade disruption insurance (TDI), a risk management framework, and evaluates its effectiveness along with other complementary programmes such as C-TPAT and the ISO/PAS 28000 to tackle the risk management of external security threats to supply chains. Chapter twelve uses a combination of primary and secondary data sources from maritime and related industries in Europe and the Asia-Pacific region to look at the requirements for designing, developing and implementing safety and crisis management cultures that enhance vulnerability analysis in maritime trading systems and the security assurances of supply chains. Chapter thirteen presents, through a survey of senior US executives in manufacturing and retail operations, the cargo-interest perspective of the maritime container security framework. Chapters fourteen and fifteen both provide quality management frameworks to ensure regulatory compliance and quality assurance for new security initiatives, and present case studies for implementing and managing the 24-hour rule and the ISO 28000 programme, respectively.

The final set of chapters presents different models for analysing the security risk element with a policy perspective. The sixteenth chapter reviews and critically analyses current maritime security and regulatory-based models and highlights the limitations of the current framework in providing an integrated approach to risk assessment and management, including supply-chain security. The seventeenth chapter presents the full and detailed results of the UNCTAD global survey on the implementation costs and financing mechanisms of the ISPS code in ports, including such aspects as cost-factor distribution and cost-recovery schemes. Chapter eighteen analyses the implications of the enactment of EU policy measures for European ports, and discusses several related issues including such aspects as the distribution of responsibilities among port stakeholders, the search for a balance between risk and regulatory policies, and the emerging cost and financial implications. Chapter nineteen discusses the wider topic of strategic risk management in ports and presents a case study that associates strategic risk management with port security. Finally, the last chapter, chapter twenty, analyses the implications of port security on the competitiveness of short sea shipping (SSS) in Europe, which appears to be an overlooked and forgotten issue in the current EC policy framework, and mechanisms for implementing and enhancing SSS networks.

LIST OF CONTRIBUTORS

EDITORS

Khalid Bichou is the co-founder and Managing Associate of the Port Operations, Research and Technology Centre (PORTeC) at Imperial College London, where he manages a number of research and consultancy projects in port operations and maritime logistics, alongside his involvement with other projects in freight logistics, transport economics, supply-chain planning and operations strategy. Having graduated with a first class BSc in public economics and administration from the École Nationale d'Administration (ENA), he also holds an MSc in port management (Distinction) from the World Maritime University (WMU), an MSc in international logistics (Distinction) from the University of Plymouth, and a DIC in transport operations from Imperial College London. He has a broad knowledge of the transport, infrastructure and logistics sector, in particular the port and maritime transport industry, with over 14 years' international experience in the industry, including periods in senior positions and as a consultant and adviser to private operators, governments and international agencies. He is a Chartered Member of the Institute of Transport and Logistics, an Associate of the Institute of Management Consultancy, and a member of many other professional and academic associations in the field. He has published on a number of aspects of port operations, maritime and transport logistics, and he is the author of several research and policy reports on the subject. His research interests span various aspects of port operations and freight logistics, in particular the association of ports with logistics operations and supply-chain management.

Michael Bell is Professor of Transport Operations at Imperial College London. Having graduated in 1975 from Cambridge University with a BA in economics, he obtained an MSc in transport planning in 1976 and a PhD in 1981 (both from Leeds University). Between 1979 and 1982 he worked as a Research Associate at University College London, before moving to the Institut für Verkehrswesen at the Technical University of Karlsruhe as an Alexander von Humboldt post-doctoral Research Fellow. He returned to the UK in 1984 as a New Blood lecturer at the University of Newcastle. In 1992 he became the deputy director of the Transport Operations Research Group (TORG), becoming its director in 1996. He was promoted to a Personal Readership in 1994 and to a Personal Chair in 1996. In January 2002, he moved to Imperial College London and in 2005 established the Port Operations Research and Technology Centre (PORTeC). His research and teaching interests have spanned travel demand forecasting, network modelling, traffic engineering and control, transport telematics and, and most recently, port operations and logistics. Recent projects include multi-objective traffic signal control (for the Department for Transport), road network monitoring (a European Union project), a Swiss national traffic model (for ETH, Zurich), the impact of congestion charging in London (for John Lewis Partnership and Transport for London), robust and adaptive navigation for road vehicles (for BMW), congested transit assignment (for the Department of Transport), road network reliability and door-to-door transport for elderly and disabled people (Transport for London). His team currently consists of 11 research students and two research assistants.

Andrew Evans has been Lloyd's Register Professor of Transport Risk Management at Imperial College London since January 2004, and was Professor of Transport Safety at University College London between 1991 and 2003. He is an economist and statistician by background and he regularly advises on safety risk assessment and on the economic appraisal of safety projects and regulations. His safety interests are in risk estimation, risk appraisal, the economics of safety and safety regulation. Andrew is a chartered statistician and Fellow of the Institute of Transport and Logistics.

AUTHORS

Panagiotis Angeloudis is a PhD student at CTS, Imperial College London, where he also obtained an MEng in civil and environmental engineering. He has past research and work experience in the engineering and maritime sectors. Since the beginning of his research at Imperial, he has worked in the areas of port automation, next generation container terminals and maritime security. In close co-operation with the industry he is developing new efficient control algorithms for automated guided vehicles for ports, as well as a simulation model for the analysis of the global container shipping network.

Dr Jean-Paul Arnaout is an Assistant Professor at the Industrial and Mechanical Engineering Department, Lebanese American University, Byblos, Lebanon. He received his MSc and PhD from the Department of Engineering Management and Systems Engineering at Old Dominion University, Norfolk, Virginia in 2003 and 2006 respectively. He received his bachelor's degree in mechanical engineering from the University of Balamand, Lebanon. Dr Arnaout has developed several simulation and optimization models including port operation simulations. His research interests include optimization techniques, modelling and simulation and scheduling. He can be reached at jeanpaularnaout@gmail.com.

Dr Regina Asariotis is Chief of the Policy and Legislation Section in the Trade Logistics Branch of UNCTAD. She is involved in all aspects of the

Secretariat's work on transport law issues, including international regulation to enhance maritime and supply-chain security. Before joining UNCTAD in 2001, she was senior lecturer in law at the University of Southampton where she taught international maritime and commercial law at undergraduate and postgraduate level. She holds degrees from universities in Germany and the UK and is a qualified barrister (England and Wales) and attorney at law (Athens). Regina has authored and co-authored numerous publications in the field of maritime and transport law and is specialist editor for the *International Journal of Maritime Law.*

Giovanni Luca Barletta is a PhD student at the Centre for Transport Studies, Imperial College London. He obtained his MSc in business engineering at the Politecnico of Bari and worked afterwards as a consultant focusing mainly on port security and ro-ro shipping in the Mediterranean. He later obtained his MSc in transport and business management from Imperial College in 2006. He also collaborated with the Politecnico of Bari in the study of RFID applications for supply-chain management. His current research interests are on the influence of smart technologies in port security and the management of supply-chain uncertainty in the container shipping industry.

Dr Paul Barnes is a Senior Lecturer specializing in risk and crisis management within the School of Management at the Queensland University of Technology, Brisbane, Australia. He has made presentations in China on risk and emergency management planning, and elsewhere in Asia, the United States and Europe on risk and crisis management applied to critical infrastructure protection, organizational vulnerability and supply-chain security. He is an active member of the Research Network for a Secure Australia and a European Commission Expert Evaluator: Risk Management & Governance Systems (FP 6 & 7). Before returning to academia he held senior public sector positions in emergency management, including chairing the National Community Education Sub-group of the Australasian Fire Authorities Council, and corporate risk management in government portfolios dealing with animal and plant health and agriculture. Most recently he was Director of Security Policy Development within the Defence Security Authority, Australian Department of Defence. Dr Barnes received undergraduate qualifications in Environmental Science and a PhD in Risk and Organizational Analysis from Griffith University, Australia.

Hassiba Benamara is an economic affairs officer at United's Trade Logistics Branch. She is currently working on transport and supply-chain security, WTO transport and logistics services trade negotiations and the Review of Maritime Transport. Hassiba holds an MA in economics and has worked for the Canadian Ministry of Transportation for several years. During that time she was a policy analyst in both the shipping and trade divisions and represented the Ministry at the IMO Legal Committee meetings, as well as the

WTO and the bilateral and regional trade negotiations. Areas of work included marine insurance and liability, maritime security, arrest of ships, cabotage as well as transport and logistics services trade liberalization.

Dr Mary R. Brooks is the William A. Black Chair of Commerce at Dalhousie University, Halifax, Canada. She was Membership Secretary and Treasurer of the International Association of Maritime Economists from 1994 to 1998 and a director of the Halifax International Airport Authority from 1995 to 2004. She currently chairs the Committee on International Trade and Transportation, Transportation Research Board, Washington DC. She is a member of the Chartered Institute of Logistics and Transport. She was the co-editor of the *Canadian Journal of Administrative Sciences* from 2003 to 2005. In 2005, she was a Canada–US Fulbright Scholar based at George Mason University in Fairfax, VA. She is best known for her books, *Sea Change in Liner Shipping: Regulation and Managerial Decision-Making in a Global Industry* (Pergamon Press, 2000) and *Maritime Transport* (with Button and Nijkamp by Edward Elgar, 2002). Dr Brooks received her undergraduate degree from McGill University, her MBA from Dalhousie University (1979) and her PhD in maritime studies from the University of Wales in 1983

Dr Kenneth J. Button is Professor of Public Policy and Director, Center for Transportation Policy and Logistics at the School of Public Policy, George Mason University, Fairfax, VA. He is a world-renowned expert on transportation policy and has published, or has in press, some 80 books and over 400 academic papers in the field of transport economics, transport planning, environmental analysis and industrial organization. Before coming to the School of Public Policy, Dr Button was an adviser to the Secretary General of the Organization for Economic Cooperation and Development where he headed up the OECD work on international aviation (which produced *The Future of International Air Transport Policy: Responding to Global Change*). Dr Button received his undergraduate degree from the University of East Anglia, his MA from the University of Leeds and his PhD from Loughborough University.

Professor T.C.E. Cheng is Chair Professor of Management in the Department of Logistics, Hong Kong Polytechnic University. He has obtained bachelors, masters and doctoral degrees from the Universities of Hong Kong, Birmingham and Cambridge, respectively. He has previously taught in Canada, England and Singapore. His expertise is in operations management; in particular, quality management, business process re-engineering and logistics and supply chain management. An active researcher, he has published two books and over 250 academic papers in these areas. He has secured over HK$20 million in research grants from different funding bodies and business and government organizations to support his research programme. A registered professional engineer and a seasoned management consultant, Professor

Cheng regularly advises business and industry and provides management training and executive development to public and private corporations

Francis D'Addario is Vice President, Partner & Asset Protection, Starbucks Coffee Company. He has more than twenty years experience in law enforcement and corporate security management, and is a Certified Protection Professional, Fraud Examiner and Community Emergency Team Responder. His teams have provided private sector benchmarks for violence reduction and bottom line profit contribution. His publications include *Loss Prevention through Crime Analysis* (Butterworths 1989) and *The Managers Violence Survival Guide* (CPA 1995). He designed LossVision, a copyrighted loss reporting, investigations, and asset recovery software program; and Safe and Sound, an interactive, multimedia workplace violence training curriculum marketed by Learning Dynamics. D'Addario currently serves as a board member of the West Seattle Food Bank. He co-chairs the business committee for Three Projects/One Community, a US$29 million capital campaign to provide West Seattle with permanently affordable facilities for food, social services, low income housing and the arts. He is also an advisory board member for CSO magazine and a project team member for the International Standardization Organization (ISO) that drafted an international supply-chain security standard.

Kevin Feldman is a management consultant in transport and supply chain systems. After successfully passing his French scientific baccalaureate, he went into the selective *classes préparatoires aux grandes ecoles* where he had intensive maths, physics, chemistry and engineering science courses. He then passed the entrance exam to ESTP (*École Spéciale des Travaux Publics*), one of the leading French civil engineering schools. In 2006, he obtained an MSc in transport and business management from Imperial College as well as a *Diplome d'Ingénieur* in civil engineering from ESTP as part of a double curriculum. He has been working on the impacts of uncertainty on supply chain performance and his career interests lie in supply-chain management and logistics.

Ximena Gutiérrez is a PhD student at the College of Management of Technology, École Polytechnique Fédérale de Lausanne (EPFL). She obtained an MSc in industrial engineering from Universidad de Los Andes (Colombia) and later an Executive Master in management of logistical systems from EPFL (Switzerland). She has been conducting research in the fields of logistics, supply-chain security and cross-border operations.

Juha Hintsa holds an MSc (Eng.) degree from Helsinki University of Technology in industrial management and artificial intelligence (1994). After working for eight years in steel manufacturing and supply-chain software industries, he started a global cross-border operations and supply-chain security management research programne (Cross-border Research Association, CBRA:

www.cross-border.org) in close collaboration with DHL, World Customs Organization and HEC University of Lausanne (summer 2001). He became a full-time research assistant and doctoral candidate at HEC Lausanne in 2003, and he is aiming to complete his doctoral thesis by the end of 2007.

Dr Kee-hung Lai is an Assistant Professor specializing in logistics and maritime studies in the Department of Logistics, Hong Kong Polytechnic University. He obtained his PhD from the same university. His research in logistics and shipping management practices has resulted in over 10 published papers in reputable international academic journals. He has also undertaken consultancy and executive training work for private and public organizations in Hong Kong and on the Chinese mainland.

Dean L. Kothmann is a senior industry consultant at Electronic Data Systems (EDS), USA, where he develops solutions for the advancement of the global trade system by assisting regional development corporations, governments and Fortune 1000 companies. Prior to EDS, Mr Kothmann held the position of chief enterprise officer at BV Solutions Group from 1999 to 2005, where he developed strategies and architectures for a global trade system. His experience also includes the role of general manager/general partner of the Power Division for Black & Veatch (1986–99). As a founding board member of the Chemical, Biological, Radiological Technology Alliance (CBRTA) and the Innovative Trade Network (ITN), Mr Kothmann has been closely involved in supply-chain security and efficiency efforts. At CBRTA, he was the team lead for the alliance's solution to global trade security. He draws upon his wealth of experience in trade lane and supply-chain logistics to develop innovative architectures for improving the supply-chain efficiencies while securing logistics worldwide. In addition to his CBRTA and ITN memberships, he is also a member of the ISO 28000/28001 Trade Lane Security Working Group and the ISPS ISO standards development committee. He is a technical adviser to the American National Standards Institute on trade lane security standards for the United States and is a member of the US Chamber of Commerce Homeland Security Task Force.

Dr Richard Linn is an industrial engineer with the Boeing 787 Program, Everett, Washington. He received his PhD in industrial engineering from Pennsylvania State University. Production control, operation management and logistics are his areas of specialty. He has taught in Florida International University, Hong Kong University of Science and Technology and Iowa State University, and worked with General Instruments Corp., E.I. DuPont and IBM and consulted for companies such as Hong Kong International Terminal Limited, Gold Peak Electronics and Wong's Printed Circuits. He was an ONR Senior Research Follow (Logistics) at the Naval Air Warfare Center, Aircraft Division between 2001 and 2003 and is serving on the editorial board of the *International Journal of Production Economics*.

Dr Jiyin Liu is Professor of Operations Management in the Business School at Loughborough University. He previously taught at Hong Kong University of Science and Technology and Northeast University of Technology, China. He received his PhD in manufacturing engineering and operations management from the University of Nottingham. His research interests are operations planning and scheduling problems in production and logistics systems. For many years he worked with colleagues in Hong Kong on a logistics initiative and with local industry there on operations problems of container terminals, air cargo terminals, freight forwarders, distributors as well as manufacturers. He has also worked on planning and scheduling problems in iron and steel industry.

Dr Y.H. Venus Lun is a lecturer in shipping operations and management at the Department of Logistics, Hong Kong Polytechnic University. She holds postgraduate degrees in business management and has worked for more than 10 years in the shipping industry in both Hong Kong and Canada. Her research interests in the field focus on the interplay between maritime business and logistics transportation.

Dr Koi Yu Adolf Ng is an Assistant Professor at the Centre for Maritime Economics and Logistics (MEL), Erasmus University, Rotterdam, The Netherlands. His research interests include port competition, reform and governance (especially East Asia and Europe), short-sea shipping and supply-chain development. Apart from academic research, he has had recent experience in preparing consulting reports, e.g. for Europe Container Terminals BV (ECT) and European Investment Bank analysing the competitiveness of the port of Rotterdam in transhipment traffic and the economic eligibility of introducing short sea shipping in Europe, respectively. Between 2004 and 2005 he was invited to provide professional advice to the Port of Felixstowe Ltd in their business plans and has been a referee in peer-reviewing papers for the *Journal of Transport Policy* since 2003. Dr Ng received his BA (First Class Honours) and MPhil from the University of Hong Kong and DPhil in Maritime Studies from the University of Oxford.

Richard Oloruntoba has more than 10 years international experience in the shipping and freight forwarding industry in the Europe/West Africa general cargo and container trades, as well as in cross-border haulage in West Africa. His research interests include supply-chain risk and security, logistics in developing economies and the logistics of disaster relief. Richard received an Advanced Diploma in shipping and ports administration (Distinction) from the University of Lagos, a BSc (hons) zoology degree and a Masters in business administration (operations) degree from the University of Ilorin, as well as an MSc in international shipping and an MSc in international logistics from the University of Plymouth. He won the 2001 Charles Gee Centenary Award from the Institute of Chartered Shipbrokers, London, and he is an active member of several logistics and maritime professional associations such as the Logistics Association of Australia, Queensland and the Chartered Institute of Logistics and Transport Australia, Queensland. He is the co-author of the pioneering report *Humanitarian Organizations and Logistics* resulting from a research project funded by a research grant from the Institute of Logistics and Transport UK (2003, ISBN 1-904564-01-1). He has presented research findings at several international conferences and published in several international journals including the *Journal of International Management* and *Supply Chain Management*. Richard is currently undertaking PhD research in international logistics at the Queensland University of Technology, Brisbane, Australia, while lecturing on export management, logistics management, supply-chain management and international marketing.

Dr Athanasios A. Pallis (PhD, Bath, UK) is Assistant Professor in the Department of Shipping, Trade and Transport, University of the Aegean, Greece. He is the author of books and journal papers examining the economics and politics of the European port policy and the common EU maritime transport policy. He is the holder of a Jean Monnet grant on European port policy, and is also involved in research projects examining the structures of the European port industry and maritime markets monitoring. His work has been acknowledged, among others, by the European Parliament and by reviews of the most important studies in the field of port economics and policy. He has won the ‘Best European Study 1999’ Competition, organized by the Foundation for the Advancement of European Studies (FAES).

Dr C. Ariel Pinto is an Assistant Professor of Engineering Management and Systems Engineering at Old Dominion University, Norfolk, Virginia, USA, where he was recently awarded a research grant to study the continuity of operation of maritime ports after the occurrence of security disruptions. His works focus on risk management in engineered systems and systems engineering. He has worked at Carnegie Mellon University’s Software Industry Center on software security and quality. He also worked at the Center for Risk Management of Engineering Systems at the University of Virginia on various projects with the US Army Corps of Engineers, Virginia Department of Transportation, and Comdial Corporation. He received his PhD from the University of Virginia and his MSc and BSc from the University of the Philippines.

Dr Ghaith Rabadi is an Assistant Professor and has been the Graduate Program Director at the Department of Engineering Management and Systems Engineering at Old Dominion University since 2002. Prior to that, he was a visiting assistant professor at the Department of Industrial Engineering and Management Systems at the University of Central Florida, Orlando, FL, where he received his MSc and PhD in industrial engineering. He received a BSc in industrial engineering from the University of Jordan, Amman, Jordan.

He has been involved in research projects funded by various agencies including NASA, Department of Homeland Security (DHS), Virginia Port Authority (VPA) and MITRE Corporation. He was awarded the NASA Faculty Fellowship in summer 2003 and Lucent Technologies Industrial Fellowship in 1996. He teaches graduate courses (MSc and PhD) in supply-chain management, simulation and optimization at the Engineering Management and Systems Engineering Department. His research interests include simulation modelling and analysis, operations research, scheduling, optimization and machine learning, and he has numerous peer-reviewed journal and conference publications. For more information visit *http://www.odu.edu~grabadi* or e-mail grabadi@odu.edu

Mark Rowbotham is an independent consultant in customs and marine security, safety and control issues, and has spent a considerable length of time working in both the government and commercial sectors. He deals primarily with compliance, control and procedural issues in both customs and marine matters. He was originally an officer in HM Customs & Excise, where his responsibilities involved import and export controls over maritime freight traffic into and out of UK ports. Upon leaving HM Customs & Excise, he became customs and seafreight operations analyst at one of the London branches of Nippon Express, a large Japanese freight company, and was largely responsible for setting up a new branch of the company at the port of Felixstowe. Following this, he spent some time on contract assignments designing and implementing sea freight operations systems, including Leyland-DAF Vehicles near Preston, Lancashire. Following graduation in export management, he gained a Masters' degree in international relations and political economy in 1995, and became an independent consultant in customs and marine matters three years later. His clients range from SMEs to multinational enterprises, and are located throughout northern England, Scotland and Northern Ireland, with further connections in Europe. He has written extensively on the subjects of customs, VAT and international supply-chain compliance issues for a wide variety of publications, including international trade and logistics magazines and journals of the universities of Cranfield and Glasgow. He advises several chambers of commerce on customs, international trade and marine issues throughout Scotland and northern England, and frequently delivers training courses and seminars on these issues. He is also an adviser to UK Trade & Investment on customs procedures pertaining to trade with North America. In his capacity as a member of the Chartered Institute of Logistics and Transport, he is chair of their Maritime Forum, and has presented marine seminars to a variety of organizations.

Dr Christoph Seidelmann is the president of the International Container Security Organization (ICSO) based in Brussels, Belgium. He is also the managing director of the Centre for Intermodal Transport (Studiengesellschaft für den kombinieten Verkehr e.V.) in Frankfurt, Germany, where he deals with a wide range of national and international studies mainly in the field of intermodal transport and logistics such as feasibility studies for various new technologies of intermodal transport including road-railer, height-capacity automatic transfer systems, fleet management, automatic identification, tracking and tracing, EDI, container design and operations, and container security systems He also provides consultancy to the European Commission and the German Government on issues related to intermodal transport, terminal investment and public-private partnership in intermodal infrastructure investment.

Xiaoning Shi is a PhD candidate jointly affiliated with the Institute of Information Systems at the University of Hamburg, Germany, and the Department of Management at the Shanghai Jiao Tong University, People's Republic of China. Her position in Hamburg is supported by the DAAD (Deutscher Akademischer Austausch Dienst) and CSC (China Scholarship Council). Formerly, she worked as a teaching assistant and later as a lecturer at the Institute of International Shipping, Department of Navel Architecture Ocean and Civil Engineering, Shanghai Jiao Tong Univeristy. In 2005, she was a visiting research assistant at the University of Hong Kong and in 2002 she was working at Maersk-Sealand Shipping Corporation, Shanghai. She holds Bachelor and Master degrees in engineering from Dalian Maritime University (China). Her current research interests are in economitrical and game theoretical applications in the shipping/port industry and optimization of logistics networks.

S.N. Srikanth is founder and senior partner of Hauer Associates, India's highly acclaimed maritime and port consultancy. He works extensively in the areas of maritime policy, port development and privatization and shipping commerce. Mr Srikanth currently specializes in providing strategic guidance to international investors and terminal operators seeking to invest in India's booming port industry. His firm, Hauer Associates, identifies investment opportunities, carries out technical, commercial and financial assessments of projects and assists investors through the bid process. The firm also advises port authorities on privatization and development strategies and risk management. Mr Srikanth served as adviser for a landmark study on short sea shipping for the Government of India in 2003. The effort led to the formulation of a national policy on short-sea shipping and the diversion of freight from India's congested road and rail networks on to coastal waterways. Mr Srikanth also led a first of its kind study on container shipment economics for the government of the state of Kerala, India in 2004. The experience Mr Srikanth has acquired over the last 25 years is wide ranging. He has served as managing director of Hauers Lines (shipowners and operators) and as director on the board of the Chennai Port, India's eastern gateway. He has been nominated to a number of policy-making bodies including the National Shipping Board, a statutorily created body to advise the Government of India on shipping policy.

Mr Srikanth has also presented papers on port and shipping dynamics at a number of international conferences.

Risto Talas started his career in Lloyd's of London in 1992 with Octavian Syndicate Management, first as an assistant and then as a war, terrorism and political risks underwriter. He served on the Lloyd's Market Joint War Committee from 1998 until 2000 when he left Lloyd's to join British Marine Managers. After completing his MBA at Cass Business School he joined Maritime & Underwater Security Consultants and was involved in much of the ISPS Code-related work throughout 2003 and 2004. In 2004 he was appointed Visiting Lecturer in Maritime Security Studies at City University, London and has recently completed a secondment to the British Government as the export promoter in the ports and logistics unit of UK Trade & Investment. In July 2006 he was appointed chair of the Ports and Terminals Group's Port and Maritime Security Working Group.

Dr Wayne K. Talley is Professor of Economics at Old Dominion University, Norfolk, Virginia, USA, where he is the executive director of the Maritime Institute and holds the designations of Eminent Scholar and the Frederick W. Beazley Professor of Economics. He has published over 120 academic papers and six books. He is an internationally recognized transportation economist. He has held visiting domestic positions at the Woods Hole Oceanographic Institution, US Department of Transportation, the Interstate Commerce Commission and the National Aeronautics and Space Administration and international positions at Oxford University (England), the University of Sydney (Australia), University of Wollongong (Australia), University of Antwerp (Belgium) and City University (England). He is the editor-in-chief of *Transportation Research E: Logistics and Transportation Review.*

George K. Vaggelas is a Research Fellow and PhD student in the Department of Shipping, Trade and Transport, University of the Aegean, Greece. His research interests include port and maritime economics and management. His fellowship on the examination of the relationship between the public and private sector in the port sector is sponsored by the Ministry of Development and the port of Piraeus. He has participated in the authoring of journal papers, as well as a number of papers that examine issues of port economics that have been presented in international and national conferences. He is also involved in European and national projects examining the port and maritime industries.

Ramesh Venkataraman is a management consultant. He heads the Asian operations of CurAlea, an international management consulting firm specializing in the areas of corporate governance, risk management and internal auditing. His primary focus is on entity level assessment and COSO, enterprise risk management, risk management for Asian markets, code of ethics related services and internal audit methodology and training. Ramesh has been a guest speaker at INSEAD Singapore and is one of the pioneers in teaching of corporate governance and business ethics in India. He has been conducting for the past three years a comprehensive 11-session programme on this subject for a leading B-school in Bangalore. Ramesh's most recent work experience was with Unilever PLC as Director—Corporate Audit, Asia. In this role he has had experience of providing reassurance on major risks for the company's operations in over 15 large countries in the Asia Pacific region, with intensive exposure to China, India and Southeast Asia. He has worked closely on implementation of enterprise risk management initiatives over the last 10 years. He has also held controllership and senior management positions with Pond's India and Unilever India over the last 25 years. Ramesh is a chartered accountant from India.

Professor Stefan Voß is professor and director of the Institute of Information Systems at the University of Hamburg. Previous positions include full professor and head of the Department of Business Administration, Information Systems and Information Management at the University of Technology Braunschweig (Germany) from 1995 up to 2002. He holds degrees in mathematics (diploma) and economics from the University of Hamburg and a PhD from the University of Technology, Darmstadt. His current research interests are in quantitative/information systems approaches to supply-chain management and logistics including public mass transit and telecommunications. He is author and co-author of several books and numerous papers in various journals. Stefan Voß serves on the editorial board of some journals including being editor of *Netnomics*, editor of *Annals of Information Systems*, associate editor of *INFORMS Journal on Computing* and area editor of *Journal of Heuristics*. He frequently organizes workshops and conferences and works as a consultant for several companies.

Dr Yat-wah Wan is an Associate Professor and the Director of Graduate Institute of Global Operations Strategy and Logistics Management at the National Dong Hwa University in Taiwan. He previously taught at the Hong Kong University of Science and Technology and City University of Hong Kong. He received his PhD in industrial engineering and operations research from the University of California at Berkeley. His research interests are transportation logistics management, applied stochastic models and stochastic scheduling. For many years he worked with colleagues in Hong Kong on a logistics initiative and with local industry there on operations problems of container terminals, air cargo terminals, freight forwarders, distributors and manufacturers.

Dr Phillipe Wieser obtained his diploma of engineering in mechanics at the EPFL in 1977 and he got his PhD in 1981. After a few years working in an engineering consulting company, he joined the EPFL as lecturer. His fields of research and teaching deal with logistics and information systems and integrated logistics. Since May 2000, Dr Wieser has been the executive director of International Institute for the Management of Logistics (IML) (EPFL—Lausanne and ENPC—Paris). Dr Wieser teaches in EPFL—Lausanne (Master and Executive Master MSL) and ENPC—Paris (Executive Master). He is author and co-author of more than 60 publications.

Dr Chuqian Zhang is currently a senior system analyst at Columbia University. She received her PhD in industrial engineering and engineering management from the Hong Kong University of Science and Technology. Her research in Hong Kong included optimizing various operations decision problems in container terminals. She is now working in the area of information technology.

This page intentionally left blank

CONTENTS

PART I BACKGROUND

PART II SYSTEMS FOR ENHANCING PORT SECURITY AND OPERATIONAL EFFICIENCY

PART III FRAMEWORKS FOR MANAGING THE SECURITY OF GLOBAL TRADING AND SUPPLY-CHAIN SYSTEMS

PART IV MODELS FOR ANALYSING SECURITY RISKS AND POLICY IMPLICATIONS

LIST OF FIGURES

Chapter 2

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 13

Chapter 14

Chapter 15

Chapter 16

Chapter 17

Chapter 18

Chapter 19

Chapter 20

LIST OF TABLES

References are to page number

Chapter 1

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 13

Chapter 14

Chapter 15

Chapter 16

Chapter 17

Chapter 18

Chapter 19

This page intentionally left blank

PART I

BACKGROUND

This page intentionally left blank

CHAPTER 1

MARINE REPORTING AND MARITIME SECURITY

Mark Rowbotham

Portcullis ISC Marine, UK

Abstract:
Much is being studied about the prevalent issue of maritime security, especially from the point of view of landside operations at sea ports. However, although the issues concerning the overall security of port operations and how these relate to the security of vessels entering, berthed at and leaving port have been investigated, less has been studied concerning the actual security of those vessels at sea, especially in relation to their complements, such as cargo or passengers. The US maritime security issues in the wake of 9/11 imposed significant compliances upon overseas traders sending goods to US shores. These security issues highlighted the lack of information available in many cases concerning both cargo and passenger manifests, as well as the ability of the vessel and its crew to effectively report their details to the US national authorities. How much less, therefore, is the ability of the same or similar vessels to report the same kind of information to other national maritime authorities throughout the world. This study, part of a larger study into the issues of maritime reporting and territorial controls, seeks to address some of the issues at stake, and to shed some light on the overall subject of marine reporting and how it could be better managed and developed.

1 A VIEW FROM THE BRIDGE

The state-of-the-art marine freighter or passenger liner bears little relationship to its forebears in terms of the technology of its control systems. Gone are the telegraphs between bridge and engine room, as are the conventional wheelhouses with their huge steering wheels. Everything is controlled by complex on-board computer systems, from steering and navigation to engine control and position monitoring. Even the marine propulsion systems have changed, from the combinations of conventional stern-mounted screws linked to huge marine engines and bow-thrust mechanisms, to azymuth propulsion systems, where the propulsion systems can revolve through 360 degrees and are connected to smaller, more efficient diesel engines by an adjustable link mechanism, which eliminates the need for a conventional rudder steering mechanism. The one main link with more traditional times is the vast array of Admiralty charts ranged across the available desk space, although even this is giving way to a large extent to the ECDIS computerized charts. Today's control systems rely heavily on a mixture of GPS, VTS, AIS and conventional radar systems. From port of departure to port of destination, the vessel monitoring process from a navigation point of view revolves around the following systems:

- Leaving port—VTS/AIS;
- Open sea—AIS/GPS;
- Entering port approaches—AIS/VTS;
- Port arrival—VTS.

The VTS systems allow for the close monitoring of vessels within port approaches and port areas themselves, while AIS allows for the monitoring of vessels throughout their voyage, and indeed while the vessel is in port as long as the AIS transponder is switched on. The drawback with any of these systems is that they identify the ship, but not its crew or its cargo or complement of passengers. Equally, the AIS system is still subject to a slight delay between the time the transponder emits the signal and the time this registers on the system and thus registers the ship's position. All this may be good insofar as it exists, but it does not tell the full story. There are considerable gaps in the whole process, mainly because of the issue of cargo reporting, and these gaps are the issues of the greatest importance owing to the risks posed by unreported cargo and other security considerations. Other risks also prevail, in particular the lack of monitoring of vessels outside the remit of the VTS and AIS systems, which could have an adverse effect on the security and safety of vessels covered by these systems. Despite the evident technological tools available to the ship's master and his crew, the view from the bridge may still be obscured by many external factors beyond the master's control.

The synopsis of procedures concerning the voyage of a cargo vessel may be loosely categorized as follows:

1. the ship's agent and the freight forwarders verify specific documentation (e.g. dangerous goods notes etc.) to ensure compliance with IMO requirements;
2. the cargoes destined for loading aboard vessel are declared to Customs by electronic input;
3. Customs clearance is given for the consignments to be loaded aboard vessel;
4. the ship is loaded at port with the cargoes (e.g. containers);
5. bills of lading are issued for all cargoes loaded aboard vessel, and the cargo information is also entered on the cargo manifest;
6. a copy of the ship's manifest is given to the ship's master by the ship's agent (the port agent) and a further copy of the manifest is also submitted to Customs;
7. the ship's master notifies the port and the Customs authority that all cargoes are loaded aboard vessel;
8. the ship is given clearance to sail;

9. the master maintains contact with the port VTS concerning the ship's movement out of the port, through the channel and into the open sea;
10. the ship maintains electronic contact with other vessels and land through the use of the AIS system;
11. the ship sails across the ocean to its destination. Upon the approach to the port of destination, the following action is undertaken:
12. the vessel's agent notifies the port of destination of the arrival of the vessel;
13. the ship notifies the port of destination 24 hours in advance with details of the ship, its crew and any hazardous or dangerous cargoes aboard vessel in accordance with the IMDG Code, and its intention to dock;
14. the ship enters national territorial limits and notifies the port of details of its crew, its stores and any other information required by the national authorities;
15. the ship maintains contact with the port through the VTS system from the time it enters the port approaches, and proceeds to enter the port;
16. a copy of the cargo manifest is submitted by the port agent to the port authority and the Customs authority prior to the ship's arrival at port;
17. the ship's master submits a FAL Declaration to Customs of all details of crew and stores on board; and
18. the ship's master gives a detailed report to the port authority complying with the regulations set down by the ISPS Code.

Although details of cargo reporting may have been covered earlier in this section of the study, they still have an overall bearing upon the safety and wellbeing of both the vessel and its crew. It should be noted that the ship's master can only report details of the cargo if he is fully aware of that cargo aboard the vessel according to the cargo manifest. In many cases, the cargo may only be known by its groupage description, i.e. a generic description of the consolidated cargo in a LCL container load, and not by details of each individual consignment within that consolidated cargo. This absence of information may not yield vital information, such as the hazardous nature of an individual cargo, or whether such a cargo was (in)correctly stowed aboard vessel. It is this lack of information which may mask a much greater risk to the ship, its crew and its location depending upon the location of other vessels close by, e.g. within the confines of port approaches, or where adverse weather conditions such as fog may be prevalent. It is this anomaly which may prejudice or compromise the safety and security of not only the ship and its crew, but also the safety of the surrounding environment including the port itself. There is a further risk prevalent if the exact nature of the crew is not fully known, concerning their professional competence to crew the vessel or their nationality or even their motives for being aboard the vessel at the time of the voyage.

A major problem arises where the buyer (i.e. the importer) arranges groupage shipments and has the cargo consolidated at a point in the country of departure under an ex works (EXW) basis. Given that the buyer initiated the transport of the various consignments, the shipping line will still issue both a master bill of lading for the LCL groupage shipment as well as a set of house bills of lading, but may not necessarily issue the house bills to the buyer unless specifically requested. Thus, the exporter may never receive a copy of the house bills of lading relating to their consignment since they did not arrange the shipment. Nor will the exporter receive a copy of the export Customs declaration for that consignment, assuming that an individual export declaration has been physically raised by the freight forwarder, which may not be the case in the event of a consolidated consignment. In many cases, this does not happen. There is thus no audit trail available to the exporter to show that their particular consignment was shipped. Furthermore, where a groupage consignment simply shows "freight of all kinds" (FAK) or a generic description such as "cosmetic products" or "automotive equipment", there is no specific means of verifying the individual consignments grouped within the container in question, as there may be the risk that no specific house bills of lading were raised for each individual consignment as far as the exporter is concerned. Furthermore, this lack of detailed information will also reflect on the cargo manifest issued to the ship's master and to Customs at the point of export.

The problem is compounded by the fact that the forwarding agent notifies the port agents about the cargo once the shipment has been arranged for loading aboard the vessel. The freight forwarder is responsible for sending full details of the cargo to the port agent for the latter to incorporate the details of the consignment and the container in which it is loaded on the cargo manifest. The port agents are responsible for dealing with all affairs relating to the vessel while it is berthed at port, including the loading and unloading of the vessel, and the liability for conservancy and port handling charges. It is thus the responsibility of the port agent to ensure that the ship's master is made aware of all cargoes loaded aboard the vessel, and that all hazardous or dangerous cargoes are notified in advance to the master of the vessel in order to ensure compliance with port regulations, SOLAS regulations and the general regulations concerning the correct stowage of all cargoes aboard the vessel. If a freight forwarder does not submit the correct information concerning cargoes, especially those of a groupage or consolidated nature, to the port agent, the freight forwarder could be made liable for any accident or damage which could occur as a result of the failure to inform the port agents or the ship's master or even the port itself of the nature of the cargo being loaded aboard the vessel. In reality, the responsibility for correctly divulging information pertaining to the cargo lies with the exporter. If the exporter does not inform the freight forwarder of the true nature of the consignment, the rest of the chain of reporting is severely prejudiced, including the ramifications for insurance of the cargo in question.

In short, the neither the ship's master nor the shipping line nor the port authority may be entirely knowledgeable about the crew of the vessel or its cargo. Although the ISPS Code goes a long way towards tightening up security measures aboard vessels as well as providing information about the crew, it only covers that which is known or is divulged in the company's interests. In the case of the ISPS Code, there are, however, likely to be cases where although the crew's nationality may be known, other information about each crew member may not be known because of the withholding of personal information by certain crew members for personal or other reasons. Furthermore, there is no internationally-binding code obliging the exporter or the freight agent to correctly declare all freight being loaded into a container, and in this way the cargo considerations are completely divorced from the issues of the nature of the vessel's crew. Even the recently introduced ISO 28000 and 28001 standards allow the trader to compile and implement their own set of checklists and procedures concerning cargo security, and do not dictate the exact details of such procedures. The underlying principle is still one of *uberrimae fidei*. Thus, in an age of information technology and access to information, the data held by the shipping line pertinent to the cargo on any of its vessels may only be as accurate as the organization inputting that information to the shipping line, such as a freight agent. With large-scale cargo consolidations, the risk of inaccuracy and heightened risk on this basis is greatly increased. A ship will not report in either to a sea port or a control centre overlooking a narrow strait concerning the nature of its cargo if it is not aware of any hazardous or dangerous cargo on board, especially since the 24-hour reporting mechanisms in place at many ports, particularly those in the UK, are still voluntary and not fully mandatory. The ship is entirely at the mercy of the shipping line's agents and the freight agents responsible for shipping cargo consignments. This level of uncertainty only adds to the risk of accidents or catastrophes occurring as a result of marine accidents, and thus severely compromises marine safety for the vessel, its crew and other cargoes aboard the vessel.

2 A VIEW FROM THE SHORE

The aspect of maritime reporting is naturally important from the onboard vessel perspective. However, from the port perspective, there are many issues which beset port and landward activity which need to be addressed on a long-term basis, mainly as a result of recent maritime legislation which affects worldwide maritime activities.

The EU Directives covering vessel monitoring and tracking have meant that more sea lanes must be covered by some form of VTS system. The waters around southern Scandinavia are being increasingly brought under some form of VTS activity, with the most recent being the Storebaelt (Great Belt) within Danish territorial limits. Invitations to tender have also been submitted for the purpose of the provision of a VTS system to cover the Öresund, between Denmark and Sweden. And yet, there are still many sea areas, including much of the coastal waters surrounding the UK, which are not yet covered by an interactive VTS system similar to that at the Strait of Dover. Only the AIS system is being actively used around all UK waters, and even this is only effective if the vessels have their AIS transponders switched on. There are various AIS websites for public use, and these are in some ways the only way in which many organizations can monitor maritime activity around the UK coast. However, there is no fully-integrated VTS system for the whole of the UK, and every port manages its own affairs concerning vessel control activity. Indeed, there are still major ports in the UK which are not yet equipped with a VTS system, inferring that they have little, if any, monitoring or control facility over inward and outward vessel movements, despite the incidence of marine accidents close to their domains. Ports do not divulge information to other ports for a variety of reasons, and there is therefore no way of knowing a vessel's circumstances without being located at the port of arrival or departure. In short, the UK system of vessel control is severely fragmented, with information concerning a vessel's movements restricted to the authorities located at the vessel's port of arrival, unless it is passing through the Strait of Dover, in which case that information is also known to the MCA's CNIS operations. Other than this, only the vessel's agents will retain information concerning a particular vessel, its cargo and movements, and they will only convey that information to the port of destination.

Such information concerning the vessel's cargo is also becoming less manageable because of the increasing sizes of vessels. The latest vessels entering service with shipping lines such as Maersk, CMA CGM and COSCO are well in excess of 100,000 grt and can carry some 9,000–10,000+ TEUs (twenty-foot equivalent units). The increasing number of containers carried aboard vessels inevitably results in a greater difficulty in managing such information as the compilation and transmission cargo manifests, as well as the problems associated with the loading and unloading of containers at any port visited. This additional burden of loading and unloading will also result in increased pressure on the ports to manage their infrastructural facilities, which inevitably leads to increased congestion of land-based traffic entering and exiting the ports.

Another area of concern stems from the fact that in the UK the Maritime & Coastguard Agency (MCA) has already rationalized its structure to the point where it no longer maintains the number of coastguard stations around the UK coastline that it once did. Many of the MCA operations are not even controlled from coast-based stations, but are managed from inland-based centres. Even MCA operations concerning the North Channel, the Firth of Clyde and the Scottish West Coast are controlled from one building based at

Gourock, on the upper reaches of the Firth of Clyde, far removed from such sea areas. It is assumed that in the event of a maritime emergency or incident, all operations can be controlled from this one centre. It has been confirmed by the MCA office on the Clyde that it does not use a VTS system for these areas, but relies on the AIS systems and information available. This approach is hardly contributing to compliance with the VTMS Directives issued by the EU Commission.

It is appreciated that legislation is designed to formalize and direct activities in a variety of sectors, but there are occasions where such legislation has led to increasing burdens being placed upon those activities leading to questions being asked concerning the efficiency of those operations. The ISPS Code has been introduced by the IMO, and is being implemented by all ports worldwide. However, the smaller the port, the more difficult it is to incorporate the Code's requirements within an already stretched scope of resources. Larger ports find it less difficult to comply with the regulations as they already have a security-based system within which to operate. Small ports have to find the resources to incorporate such changes to their operating structures, and this inevitably leads to greater expenditure and other strains on such resources, as well as the burden of added levels of bureaucracy required to administer such changes and activities. Add to this any port-based activities associated with the impact of the IMDG Code on HAZMAT movements and VTS requirements, and the system moves closer to overload. Additional burdens may now be placed on the system by the introduction of ISO 28000 and ISO 28001 standards, and this will inevitably stretch already limited resources yet further.

In summary, the main codes, regulations and standards which a port must adhere to include the following:

- VTS (seaward);
- AIS (seaward);
- ISPS (landward and seaward);
- IMDG (landward and seaward);
- SOLAS (seaward);
- FAL (landward);
- ISO 28000/28001 (landward).

Other issues, such as port state controls and the presence of both MCA and Customs are also prime issues in port management, as these controls refer equally to both vessel and cargo security. The port authorities are now so enmeshed in such regulations that they appear to need to spend more time complying with them than in actually managing maritime activities. However, despite such regulations and controls it is often the case that the port's harbourmaster is the last point of contact concerning the arrival of a vessel, as the shipping agents will already have arranged berthing formalities with the port authorities in advance, and the vessel does not necessarily report its arrival until it passes through the breakwaters and enters port, thus negating in part the whole rationale behind the reason for many of the regulations concerning vessel movements and port controls.

The question must ultimately be asked as to whether the smaller ports will be able to maintain their operations for much longer in the light of the implementation of such regulations and the costs associated with such changes. As the threat of terrorism and the general concerns over maritime security increase, so too does the requirement for increasing levels of security at the ports. This inevitably costs time, effort and money and many of the smaller ports are finding it difficult to keep up with the necessary changes imposed as a result of such requirements. Even the larger ports are required to adopt more stringent measures with regard to port, vessel and cargo security, and this is creating an atmosphere of radical change within the port environment from both a landward and a seaward perspective.

3 CUSTOMS MARITIME CARGO REPORTING AND CONTROLS

In the UK, HM Customs & Excise, the Government department responsible for indirect taxation, merged with HM Inland Revenue in May 2005 to form an expanded revenue department called HM Revenue & Customs. Although the main activity of the newly-merged department is the levying of national taxes, both direct and indirect, the other primary function still paramount in the department's role is that of the economic defence of the realm from a maritime point of view.

Customs controls are those controls exercised over the process of international trade with relation to specific control over the following areas:

- imports of goods (personal or commercial);
- exports of goods (personal or commercial);
- illicit trade, i.e. smuggling;
- prohibitions and restrictions of the import and export of certain commodities and products;
- trade statistics; and
- duties and indirect taxes.

Customs controls are defined to start at the baseline defining the area of internal sea, and also pertain to control over ports, harbours and wharves which may serve the purpose of international trade. Every sea port must seek the approval of the national Customs authority prior to becoming operational, and thus becomes a Customs port. The Commissioners of Customs & Excise are empowered by section 19 of the Customs & Excise Management Act 1979 to appoint any area of the UK as a Customs port, and to appoint boarding stations for Customs officers to board ships (originally known as the waterguard), although with the changes in import and export procedures to allow for more electronic-based regimes, the facility for boarding ships has decreased to a bare minimum, if not zero, thus allowing for little or no waterborne Customs control over inward or outward shipping movements.

The ports comprise the "internal and territorial waters of Her Majesty's dominions" and extend inland up to the "mean high water line". The Commissioners also appoint "approved wharves" for the loading or unloading of cargoes (section 20 of the Customs & Excise Management Act 1979).

Customs officers have a general power to board ships inside the limits of a Customs port (section 27). They may have access to every part of a ship, and any goods found concealed or undeclared are liable to seizure and forfeiture, along with the ship itself on certain occasions, especially where the illicit trade in drugs is concerned (section 28). A ship which is constructed or adapted or simply used for the purposes of concealing or smuggling goods may itself be forfeit and seized by Customs officers in UK waters (section 88), generally by way of securing the "writ of assistance" to the ship's mast.

A report must be made by every ship, other than authorized regular shipping services such as cross-Channel or North Sea ferry services, arriving at a Customs port from any place outside the UK, or vessels carrying uncleared goods (i.e. goods not in UK/EU free circulation and thus duty-paid) brought in that vessel from any place outside the United Kingdom (section 35), including third-country (i.e. non-EU) goods which have crossed the European Union under Community Transit (CT) conditions (i.e. undeclared up to the point of entry into the UK). The Ship's Report, Importation and Exportation by Sea Regulations 1981, SI 1981/1260, amended by SI 1986/1819, specify that a report (the Customs Cargo Report—CUSCAR, generally comprising the ship's cargo manifest) must be made immediately to a boarding officer if he requests it. Otherwise, the report must be made within three hours of the ship reaching her place of unloading or loading, or within 24 hours after entering the limits of the Customs port if she has not then reached that place. There must be no interference with goods after the ship has come within UK internal waters until a report is made. On arrival, a ship must be immediately brought to the boarding station, unless public health regulations require her to be taken to a mooring station pending examination and clearance to dock. Goods imported by sea must be landed at an approved wharf. If chargeable or dutiable goods are unloaded from a ship without payment of the appropriate duties and taxes, or prohibited goods are imported, or imported goods are concealed or otherwise not correctly declared, they are liable to seizure and forfeiture (section 49). With the move from manual to electronic import declarations, however, there is little evidence of Customs landing or import controls at the port, as there is intense pressure on the port authorities to ensure that containerized consignments are moved from the port to an inland destination as quickly as possible following unloading from the ship, especially given the limited space available at the port for the detention or storage of goods.

No ship may depart from a port on a voyage to an eventual destination outside the UK unless clearance has been obtained. A Customs officer may board a cleared ship while the vessel is still in UK waters and require documentary production of her clearance. A ship departing from a Customs port must bring to at a boarding station if required (section 64). Consignments for exportation and stores must be loaded at an approved wharf and must be correctly declared, using the new export system (NES) electronic procedures. The ship can only be cleared for departure once the Customs CHIEF (Customs Handling of Import & Export Freight) computer has given clearance for all goods declared for export to be loaded aboard vessel and those goods correctly loaded and recorded on the ship's cargo manifest, including manifests concerning the shipment of consignments to the North Sea continental shelf.

Although it is accepted that a regime exists for Customs cargo reporting in line with the requirements laid down by the 1979 Customs & Excise Management Act, the information contained in such reports may not necessarily be sufficient to satisfy the Customs CHIEF computer or officers perusing such details. Containers unloaded from aboard ship will be classified in either of two categories—FCL (full container load) containing cargoes pertaining to one single importer—or LCL (less-than-full container load) containing a variety of consolidated or grouped cargoes pertaining to a variety of importers. Whereas an FCL will define the exact nature of the cargo contained therein, which can then be easily defined and declared by the clearing agent, an LCL will simply be defined to HM Customs & Excise as "groupage" or FAK. At the point of reporting, it will thus be impossible for the examining officer, or the CHIEF computer, to define exactly the nature of each consignment carried within the container until such time as the clearing agent makes the individual Customs import entry declaration for each deconsolidated consignment. By this time, the container may well have left the port for a determined inland destination, and will not have been examined by an HM Customs & Excise officer other than if it has been subjected to an x-ray examination at the port, in which case a full out-turn of all consignments may be required by a Customs officer. Given this lack of control, there is no certainty that an officer would pick up any irregular details pertaining to cargoes such as the illegal import of drugs, firearms, weapons of mass destruction or even illegal immigrants.

The issue of the exemption of authorized regular shipping services from Customs reporting regimes (JCCC Papers (04)10 and (04)27, HM Customs & Excise 2004) gives rise to anomalies in the reporting of cargoes, as it is very likely that such vessels are not only carrying goods of EU origin but also consignments under Community transit (CT) Customs control, i.e. goods which are not in EU free circulation and are hence uncleared. They may also be carrying consignments on a consolidated basis, i.e. consignments grouped together in one consolidated trailer load, and for which there is only brief summary details referring to the consolidation, and not necessarily for each individual grouped consignment. There is a clear need for Customs to know what such consignments are and where they are to be cleared through Customs controls, as national revenue is at stake. There is a significant risk that since vessels pertaining to authorized regular shipping services (including ferry services from Norway such as the sailings of DFDS and Fjord Line into the River Tyne) are not required to report into Customs prior to or upon arrival at a UK Customs port, such cargoes will not themselves be reported to Customs in an adequate form to enable Customs to establish the nature and status of such consignments. In one case, however, an anomaly exists concerning the DFDS sailings between Gothenburg (Sweden) and the UK via Kristiansand (Norway), as the voyage is essentially an intra-EU sailing with a non-EU intermediate stop added in. The rules applying to such authorized services also apply to those sailings between Norway and Denmark, also operated by DFDS and Fjord Line. Indeed, there could also be the risk that if the vessel concerned were carrying consignments or passengers of a nature deemed a threat to national security or the economic security of the nation, these contents could pass unnoticed into national territory without any form of verification or checks given the nature of the voyage within EU waters.

However, the fact that because a vessel sails within EU territorial waters between ports of two member states does not imply that the information pertaining to its cargoes is automatically passed from the despatching party to the receiving party. Although electronic facilities enable a seller to communicate with a buyer concerning the consignment of goods to be shipped, as far as commercial documents such as invoices or packing lists are concerned, this information does not necessarily correspond with that contained on loading lists or ship's manifests, or even bills of lading or waybills, which generally reflect upon the information contained in the former sets of documents. Indeed, it is very likely that the information contained on either of these latter documents exists only in abbreviated form, and may prevail in a greater sense with the advent of electronic bills of lading presently being introduced under the revisions to the Carriage of Goods at Sea Acts and the Hague-Visby and Hamburg Rules. Hence the inability of HM Customs & Excise to maintain full controls over the information submitted by shipping agents or shipowners pertaining to Customs cargo reporting, despite the requirements for vessels other than those operating on authorized regular services to submit reports to the Customs authority prior to or upon arrival in a UK port. This scenario shows that although information pertaining to cargoes may be known by the trader, be it import or export, it is not necessarily known or communicated by either freight agents, NVOCCs (non-vessel-owning common carriers), port agents, liner agents, shipowners or Customs officials, despite the rules laid down by the Carriage of Goods at Sea Acts of 1971 and 1992 pertaining to the responsibilities of shipowners, shipping agents and the masters of vessels. This would also suggest the possibility of a vacuum in information transparency and accessibility as far as the carriage of goods on the high seas is concerned. Hence, the urgent need to review the level and detail of cargo information pertaining to any vessel sailing into or within the confines of EU territorial waters, especially as such information may pertain not only to the insurance principle of *uberrimae fidei* (utmost good faith) but also to issues of national security which could be prejudicial to the wellbeing or security of the national state.

Given the freedoms enjoyed by the member states of the European Union in moving goods within the Community as long as consignments originate within the EU there are no controls concerning their movement. This implies that an EU-registered ship sailing from, for example, a port on the Baltic bound for a UK port will require no Customs controls given the assumption that its cargoes originate within the EU and are thus not subject to Customs declarations. However, it should be noted that the vessel concerned may carry cargoes originating outwith the EU, e.g. from Russia or elsewhere. Unless that cargo is individually reported as being in separate containers or trailers, or the vessel itself is registered outwith the EU, the cargo may not be declared to the CHIEF Customs computer when it arrives at the UK port. The underlying risk is that undeclared cargo may "slip through the net" on arrival in the UK and may either be misdeclared or not declared at all, thus posing a substantial risk to not only the national revenue and hence the economic wellbeing of the nation but also may pose a threat to national security if it were subsequently discovered that the cargo was made up of weapons or was of a chemical nature. As the level of Customs presence at UK ports has diminished, so the risk and threat to national security of unsolicited and undeclared imports has increased.

Only if cargoes are declared at the point of entry into the distant EU state under CT status, and are then shipped via the EU port of despatch to the relevant UK port, will the consignment be declared on the ship's manifest to HM Customs & Excise at the point of arrival at the UK port. In this way, a full import declaration can be made, and the consignment properly discharged out of Customs control.

The export element of Customs control, especially with regard to maritime movements, has become more automated and electronic with the implementation in 2002 of the NES means of export declarations, although there is still the requirement for the submission of the full cargo manifest to Customs by the ship's agents prior to the vessel being cleared by Customs for sailing. In this respect, the cargo manifest is based on the issuing of marine bills of lading for each consignment, coupled with the raising of NES export declarations by the clearing agent/freight forwarder. However, the submission of each set of documents rests with different parties, as the following summary shows:

- The cargo manifest is submitted to Customs by the ship's agents or the port agents;

- the NES declarations are submitted by the freight agents;
- the bills of lading are raised by the carrier (the shipping line).

The bills of lading are submitted by the shipping line to the freight forwarder responsible for arranging the shipment, and copies may also be held by the ship's agent, who submits the cargo manifest on behalf of the line to Customs. Cases arise where there is uncertainty over who is responsible for the loading of cargo aboard a vessel, owing to the absence of a specific INCOTERM in the contract of delivery, with the result that in some cases bills of lading are not submitted to a freight agent, and consequently no cargo manifest is submitted concerning the specific consignment to Customs. Customs are therefore unaware that the consignment in question has been loaded aboard the vessel, and consequently has not been correctly declared. In the case of hazardous or dangerous cargoes, this failure to correctly record and declare a consignment could prove disastrous in the event of an accident aboard the vessel or a collision, as a trader, i.e. the exporter or importer, could ultimately be held liable for the consequences of such an accident. A further consequence of a failure to correctly declare a consignment to Customs is that the trader is liable for VAT on the value of the consignment and equally a civil penalty on the grounds of a false declaration being made to Customs.

In all instances of loading aboard a vessel, it is imperative that all steps are taken to ensure that all cargoes are correctly entered on shipping documentation so that correct export declarations can be raised and submitted to Customs in advance of the cargo being loaded aboard the vessel, as well as the cargo manifest being submitted to Customs prior to the vessel's departure. Theoretically, failure to correctly declare a cargo to Customs could result in the refusal by Customs to allow the loading of the cargo aboard the vessel, although in reality there are few physical checks of export cargoes made at the port owing to a lack of physical resources and manpower on the part of Customs, thus allowing the port authority to carry out loading formalities without physical Customs checks on the consignment concerned.

With the transfer of most reporting mechanisms to electronic means, the structure of the maritime reporting regime with regard to Customs controls has also changed. Although Customs still maintain control over all sea ports, there is no longer the same degree of physical presence of Customs officers at many sea ports. The CHIEF Customs computer relies on the details of the export consignment in the form of the DUCR to ensure that the correct details of each consignment have been entered into the computer by the exporter or, more likely, the freight agent. However, in cases where the consignment is shipped EXW and especially in a groupage arrangement, the exporter is very unlikely to see a copy of the export declaration, and in many cases a DUCR may not be raised by the clearing agent as the consignment is part of a larger consolidated consignment arranged by the overseas buyer, and thus the only declaration raised at export will be the master UCR which covers the whole LCL groupage container load. In this respect, the details shown on the declaration will show the agent/consolidator as the exporter, and hence their VAT details will be entered, rather than those of the individual exporters whose consignments are contained in the consolidation. In this respect, there is no compliance for each exporter, and this not only distorts statistical information pertaining to export consolidations, given that the Customs authority places full responsibility for an export at the door of the exporter, but also masks and distorts information concerning the true contents of the container at the time of export. Such omissions contravene US Customs regulations under the CT-PAT initiative, and also compromize safety regulations concerning the carriage of cargoes by sea, especially concerning the nature of the FAL 2 cargo manifest and its requirements under the IMO FAL Convention.

As previously mentioned, most of the administrative and documentary control activity is conducted from distant entry processing units and centralized control functions elsewhere in the country. Actual port-related activities are conducted on the basis of officers travelling to a port when required, for example, in cases of random checks made on passengers disembarking from cruise liners or container scans. Otherwise, all declarations for cargoes, ship's stores, passengers and crews are being transferred to electronic facilities, and the procedures for these declarations are detailed as follows.

3.1 Imports/Arrivals

The vessel notifies the port of its impending arrival. The cargo manifest (in its IMO electronic UN/EDIFACT CUSCAR format) is submitted electronically by the port agents representing the shipping line to the CHIEF computer. The port agents also submit the IMO FAL forms detailing the following information:

- ship's stores still on board vessel (INVRPT);
- crew lists and Effects; and
- passenger lists.

Based on this information submitted electronically, an officer may decide to travel to the port to board a vessel and examine the details pertaining to the crew. One system which has facilitated the electronic submission of the cargo manifest is FCPS, an electronic cargo processing system originally developed by the port of Felixstowe in the 1980s under the maritime cargo processing (MCP) banner. It facilitates the submission of the cargo manifest to the port authority and Customs to enable Customs to select in advance containers which require examination or scrutiny on unloading from the vessel. It also enables the port authority to move containers from the vessel in a short space of time and facilitate Customs and port clearance by the freight forwarders or clearing agents by streamlined means, as the system also facilitates electronic import clearance direct to the CHIEF Customs computer. However, the system still relies upon the accuracy of the information supplied on the cargo manifest, and this information may not be sufficient to show exact details of every cargo contained in any container, especially groupage/consolidated LCLs. Only that information supplied as a result of the information which is also used for the purpose of the issuing of a bill of lading will be found on the cargo manifest. This information may be insufficient for Customs purposes, and may result in greater numbers of containers being selected for scrutiny by Customs at the port of arrival.

The freight agents submit electronic online import declarations directly to the CHIEF computer, which sends back an acknowledgement along with the calculation of import duty and VAT in the form of an entry acceptance advice. Each import declaration represents the cargo in each container which may be detailed on the CUSCAR cargo manifest.

The drawback of the increase in tonnage and size of the new super post-Panamax container vessels (8,000–10,000 TEU) means that the cargo manifest for each vessel becomes larger, with the risk that the computer systems required to analyse the information therein require updating to cover the increased volume of information or may take some time to absorb all the information contained therein. It is also the case that in many cases, the containers listed on the cargo manifest will only be detailed as groupage or consolidated loads, without defining the exact details of each individual cargo within the consolidation. Given the sheer volume of container information in each manifest, it is too cumbersome a task for the Customs computer to analyse each cargo at the time the manifest is submitted, although containers are selected at random for scanning and examination at the port. Any cargo examined as a result of the container scan is only scrutinized based on an individual declaration submitted by the clearing agent, which was identified by the CHIEF computer on a Route 2 (full examination) basis.

In theory, the marine bill of lading issued for every consignment should equate with the details on the cargo manifest, although for consolidations there are two types of bill of lading—the master bill of lading and the house bill of lading. In many cases, especially under EXW consolidation conditions, the master bill of lading is issued for the full consolidation (assuming that the whole container load is destined for the same buyer), but the house bills referring to each individual consignment therein may not necessarily be issued to the buyer as the whole container load is to be delivered to the buyer's premises. The house bills should be issued, however, for the prime purpose of declaration to the Customs authority at the point of import, since a declaration must be submitted to Customs for each consignment within the container.

3.2 Exports/Despatches

In the same way that all import declarations for maritime cargo have been rendered electronic, so too have export declarations for maritime cargo and ship's stores. Electronic initiatives driven by the EU have resulted in many EU countries implementing electronic export declaration procedures, and the UK implemented its own electronic export regime, the NES, in 2002 for all sea freight export declarations. The CUSCAR cargo manifest is submitted electronically by the port agent to Customs in advance of the vessel being loaded, especially in the case of shipments destined for the US, where cargo manifests must be submitted to US Customs officers based in the UK 48 hours prior to the vessel's departure under the US CT-PAT initiative. The NES export declaration is submitted to the Customs CHIEF computer as a pre-shipment advice (PSA) once the cargo is ready for shipment (usually no more than 24 hours before the consignment is due to be loaded aboard the vessel), and this declaration is acknowledged by the computer. Once the consignment has been loaded aboard the container and reaches the port of loading, another message (the arrival message) is entered by the agent into the CHIEF computer stating that the consignment has arrived at the port and awaits clearance instructions. The CHIEF computer issues the appropriate message (Route 6 automatic clearance/Route 1 documentary check, etc.) for the export consignment in question. Once the consignment has been cleared by the CHIEF computer, the consignment is loaded aboard the vessel and a Route 7 departure message is issued by CHIEF. A further Route 8 message clears the vessel to sail, and departure is completed. At this point, the marine bills of lading for each export consignment are issued to the party arranging the shipment.

The same electronic initiative which controls inward IMO FAL declarations is also used for outward movements. The suppliers of ship's stores must also submit electronic declarations based on the UN/EDIFACT inventory report (INVRPT) for all ship's stores loaded aboard a vessel prior to its departure. These declarations can be submitted electronically online in the same manner that inward ship's stores declarations are submitted at the time of the arrival in port of the vessel. Thus, the electronic arrangement of Customs export declarations is as follows:

- NES export declaration (exporter/freight forwarder/port agent);
- IMO FAL Form 2 cargo manifest (CUSCAR); and
- IMO FAL Form 3 ship's stores declaration (ship's master, supplier or agent).

However, given that an IMO ship's stores declaration requires a signature by either the ship's master or the agent, there is still the need for a hard copy to be made available to a Customs officer where required. The same is true of both the FAL Form 2 cargo manifest and the NES declaration. A hard copy of the export declaration plus supporting departure messages must be kept by the exporter for presentation to a Customs officer where and when required for VAT zero-rating or Excise suspension purposes.

Despite the increasing reliance on electronic means of reporting and declarations for Customs purposes, there is still a requirement for documentary evidence supporting any electronic declaration. This means that all parties involved in either import or export maritime activities must maintain a set of documentary records relating to every shipment. These requirements are based on liability for either VAT or Excise duty, and require the supplier of anything loaded aboard a vessel, be it exporters or ship's chandlers, to show proper accurate documentary evidence of everything loaded aboard the vessel for compliance and control purposes.

3.3 Multimodal Information and the International Supply Chain

A key factor in deciding upon the transparency of information submitted through marine channels is the availability of information emanating from the supplier of a consignment of goods, or, in the case of passenger liners, the agency booking the voyage on behalf of individual passengers. If the supplier or the agency concerned does not convey accurate or detailed information to the carrier, then it cannot be expected that the carrier can in turn convey such information to the relevant authorities of the country of destination or even the port of arrival.

In the case of sea cargoes, the information flow within the supply chain commences at the door of the exporter. In order to facilitate such a flow of information, there are 13 recognized international terms of delivery—the INCOTERMS—which are occasionally revised to account for changes in international market conditions or to clarify the varying degrees of risk and responsibility incurred by either the seller or the buyer in each of the stages of any international shipment. The very basic term used by the exporter is EXW, where the exporter does no more than make the consignment ready for collection from the exporter's premises by the buyer. The buyer takes total responsibility for the shipment right up to their own premises. It would be normal practice to expect the exporter to inform the buyer of the nature of the shipment by way of a commercial invoice or a packing list.

However, in cases where the consignment from the exporter is collected by a haulage company on behalf of the buyer and transported to a point of consolidation for loading into a container, such information may well be absorbed into a more general description pertaining to the overall contents of the groupage container on the basis of an LCL shipment. Under such circumstances, it is more common to find the terms "said to contain . . . " or "freight of all kinds" (FAK) used, or even a general term applicable to the purposes of the consignment, e.g. "automotive parts". The fact that within such a consignment there may be a host of different commodities does not figure in the description used on a marine bill of lading. A more radical example is that of a consignment described loosely as "cosmetic products", which may contain commodities ranging from aromatic oils through soaps to lipsticks and nail varnish. However, the consignment may also include items such as nail varnish remover, which is classed as hazardous goods because of its flammable nature, but since the overall groupage consignment description made no mention of this, the specific commodity is overlooked and no specific dangerous goods documentation is issued for the nail varnish remover, despite the evident risk involved in the shipment of the consignment.

Groupage or consolidation is one of the principal enemies of the accuracy of information pertaining to marine cargo reporting. Where the freight agent has accurate detailed knowledge of the consignment to be shipped, that information should be adequately transmitted via the carrier to the port of arrival, and any extra precautions required in the case of the reporting of hazardous goods will be taken. But if such information is not known, then such precautions cannot be taken and the result is a compounding of risks pertaining to both cargo insurance and the provisions for the handling of hazardous goods under the IMO Codes, especially under the IMDG and FAL requirements. In this respect, there is a clear need for the freight agent to be absolutely aware of the nature of the consignment at the time that consignment is loaded into the container, so that the correct information concerning the cargo can be passed to the carrier, i.e. the shipping line, prior to the container being loaded aboard the vessel. Failure to provide such information could result in compromises such as:

- failure to adhere to the requirements of the SOLAS, IMDG and FAL regimes laid down by the IMO; or
- the nullification of the cargo insurance policy under the provisions of the Maritime Insurance Act 1906.

The nullification of the insurance policy would thus also compromise and prejudice the general average principle concerning both the safety of the vessel and the insurance of cargoes and their consequent indemnity if it were found that:

- neither the exporter nor the importer had properly insured the consignment in question;
- neither the insurance company nor the underwriters were made aware of the true nature of the consignment under the principle of *uberrimae fidei*;
- neither the shipowners nor the shipbrokers nor the master of the vessel were correctly informed of the true nature of the consignment; or
- the consignment (or the container in which it was placed) was not correctly stowed in accordance with IMO regulations.

There is therefore the need for a fully transparent system of the transmission of cargo information to the carrier in the multimodal system long before the container or trailer is loaded aboard a vessel. The nature of the international supply chain demands that information pertaining to cargoes is passed down the line from supplier to customer in order to ensure the smooth and efficient despatch and delivery of the consignment, and that all authorities and parties within the supply chain, especially from a transportation and national control perspective, are fully informed as to the nature and risk of the consignment in question. Even where no international frontier controls are involved, such as within the European Union, there is still a significant need for such flows of information, especially where mixed forms of transport are involved, such as road and sea, either from a roll-on/roll-off (ro-ro) perspective or a short sea container perspective. The demands of the short-sea marine motorway require that integrated information flows pertaining to the maritime carriage of goods exist long before the vessel is loaded and sails, as the time scales involved between one part of Europe and another, especially on Baltic Sea or North Sea routes, are minimal. These flows start at the point of the exporter or seller, and progress through the freight agents, the road trucking companies and shipping lines and the port authorities, as well as any Customs authorities, to the importer or buyer. Such information flows should show the full extent of the consignment as well as the risks involved in handling and transporting it between the seller and the buyer.

The timely and efficient arrival of the consignment at the buyer's premises should be reflected in the ability of all relevant parties and authorities to show that they were all party to the same accurate information pertaining to not only the method of transport involved in the movement, but also to the nature of the cargo itself. Any failure in the flow of information could result in at best a delay in the delivery of the consignment to the customer's premises, or at worst the destruction of the consignment and the potential loss of a marine vessel as a result of a severe accident occurring while the vessel was at sea owing to a problem occurring with the consignment itself. This problem could, in turn, attract the attention of not only the Marine Accidents Investigation Board (MAIB) but also those responsible for maintaining the integrity of and compliance with the regulations of the SOLAS Convention, especially in cases where failure to report the true nature of the consignment insofar as its hazardous or dangerous nature was concerned by the exporter or the freight agent resulted in a catastrophe occurring at sea and the safety of the vessel carrying the cargo being compromised or prejudiced. The International Maritime Organization (IMO) is seeking to address the problem of container security in the context of global security initiatives, but this initiative is designed more to fit into the present international ship and port security (ISPS) framework, and does not necessarily address the transparency of cargoes inside a container, especially in the case of consolidated loads where the information contained on a bill of lading or a cargo manifest may be less than explanatory or accurate.

3.4 The Cargo Documentary Approach

Previous sections dealt with the overview of documentation as part of the maritime reporting mechanism. A more detailed approach is now required in order to assess how cargoes in particular are declared, with reference to both the IMO FAL Form 2 and the marine bill of lading, as the two forms relate to each other.

Whereas the IMO FAL Form 2 is an overall cargo declaration (now covered by the CUSCAR regime) as well as being a summary of all cargoes carried aboard a vessel, the marine bill of lading is an individual declaration and a documentary description of a specific cargo consignment, usually in a container, and also represents a specific cargo detailed in the cargo manifest.

There is a clause contained on the bill stating that the goods are "received by the carrier from shipper in apparent good order and condition [unless otherwise noted herein]", i.e. that the carrier bears no responsibility for loss or damage to the consignment prior to receiving it at the appointed place. The bill of lading is issued following the departure of the vessel from the port of loading, thus proving, especially in the case of a shipped on board bill of lading, that the consignment was confirmed as having been loaded aboard the vessel. This confirmation is supported by the evidence of an export declaration to Customs, followed by a series of electronic messages confirming not only loading of the consignment aboard the vessel but also the clearance of the vessel by Customs and its subsequent departure. The cargo manifest in either its manual or electronic format, is produced by the port agents prior to the loading of the vessel. In the case of the US-led CT-PAT initiative, this is a legal requirement for all consignments to be exported to the United States since 2002 for the purposes of the presentation of the cargo manifest to US Customs officials at the port of loading at least 24 hours prior to the vessel being loaded. Thus, for export purposes, a comprehensive reporting system exists, assuming that all consignments within a container are correctly detailed on a bill of lading, although anomalies pertaining to this accuracy of information are detailed in the following section. In the case of an FCL this may be so, whereas in the case of an LCL groupage load, there is every possibility that only a generic description is given on the master bill of lading, which will also refer to and be referred to by the FAL 2 cargo manifest.

A further issue concerning the information supplied on a cargo manifest concerns the mixture of non-EU and EU consignments carried on various vessels. The EU authorities have decreed that the issuers of the cargo manifest may voluntarily include details of EU-originating cargoes alongside details of non-EU cargoes on vessels which are moving between two or more EU member states. Although this can include deep-sea container vessels, it is more likely to refer to short-sea container vessel services where the vessel may be part of a feeder service to link in with a deep-sea container service, or may simply be operating on a service between various EU ports independently of any feeder service. Such services also include authorized regular operators who operate ro-ro ferries in areas such as the North Sea and the Baltic Sea. Although the information they provide is more abbreviated and does not require the same detailed information as that supplied by deep-sea operators or charter services on the grounds of the frequency and regularity of their sailings, there is still the need for a manifest covering all trailer and container loads aboard a vessel for each sailing, as the vessel may carry both EU-originating cargoes, or at least those cargoes deemed to be in EU duty-paid free circulation, as well as non-EU cargoes not in free circulation, i.e. those cargoes under Community transit status on which import duty still has to be paid, or cargoes transiting EU territory en route to a non-EU destination. The EU-originating cargoes should be covered by a T2L document. This document allows the consignments under it EU treatment by the Customs authority when they are unloaded at the EU port of destination. These cases can be represented by the following matrix categorization:

EU-originating consignments Duty paid (T2L)	*Non-EU consignments (free CIR)* Duty paid
Non-EU consignments Duty to be paid on arrival at port	*Non-EU consignments* Community transit—leaving EU

A bill of lading has more distinct functions than does a cargo manifest. Whereas a manifest gives overall details of a set of cargoes, which can then be summarily scrutinized by the Customs authority for the purpose of examination of a specific cargo or the container in which it is located at the port, a bill of lading will be used for the purpose of an import customs declaration, and may be scrutinized by a landing officer of the Customs authority for details with relation to the assessment of import duties and taxes, which cannot be undertaken with a cargo manifest. Furthermore, the bill of lading has three distinct functions which do not relate to a cargo manifest. These functions are:

- document of title (ownership of the consignment);
- evidence of contract of carriage; and
- receipt by the carrier for the consignment.

In these respects, the bill of lading is a legal document and can be used as collateral in the contract of sale, as well as proof of responsibility for the carriage of the shipment. In this respect, it may be used as legal evidence where a cargo manifest cannot. In cases where a NVOCC, i.e. a shipping company which owns or leases containers but does not operate its own maritime vessels, issues bills of lading, the bill will represent a slot charter, i.e. a transaction where the NVOCC has chartered space aboard a vessel owned by another shipping line for the purposes of shipping several containers to an overseas destination. In this case, there will not only be a bill of lading issued by the NVOCC, but also a further bill of lading issued by the carrier with respect to the containers owned by the NVOCC which will be passed from the carrier to the NVOCC. In this respect, it should then be possible to trace every container carried by a container vessel with respect to the owners of the containers and hence the consignments loaded aboard each container. In reality, containers aboard a vessel may be owned by various NVOCC owners, as well as containing varying degrees of information pertaining to their respective loads. Given the increasing size of container vessels along with their capacity to carry larger numbers of containers (>8,000 TEUs), the relative facility to trace each container is becoming more complex and increasingly less straightforward, especially when it is admitted that the sheer quantity and volume of information held on a cargo manifest relating to such vessels is resulting in the manifest becoming more unmanageable, even in its CUSCAR electronic format. Imagine, therefore, that for every container loaded aboard such a vessel, there are even more bills of lading to raise, and that infers more time being spent in raising such documents. Hence the increasing burden of work placed upon the companies, especially shipping agencies, issuing both bills of lading and cargo manifests every time a container vessel sails, and equally the risk of inadequate information being input to complete both a bill of lading and a cargo manifest, resulting in a failure on the part of the vessel's master to be fully aware of the consignments aboard the vessel, let alone the risk of failure to fully report these cargoes to the port of arrival.

3.5 The Role of the Shipping Agency

Much of the mechanism relating to the reporting of the vessel and its cargo revolves around the role of the ship's agent. The agent represents the shipping line in most ports, and deals with all aspects of the ship's entry into port and the time it spends at the berth, as laytime for unloading, loading and maintenance. The agent is also responsible for communication with the port authority concerning the berthing of the vessel, the stevedoring arrangements for unloading and loading activities, the provision of ship's stores and the administration of and documentation for all such activities. It is also the duty of the agency to inform the harbourmaster of the arrival and departure of all vessels they represent, and in so doing, inform the harbourmaster and hence the port of all hazardous cargoes or problems with the vessel. The submission of this information depends upon how much information the master of the vessel holds concerning the cargo. Normally, the cargo manifest and the mate's receipt will give this information, but in cases of consolidations, the information pertaining to a cargo may be less than detailed or at worst inaccurate. The larger the vessel, the greater the cargo and the greater the cargo the greater the amount of documentary information required pertaining to that cargo. With the arrival of 10,000+ TEU container vessels, the greater the risk that this documentary information is less accurate or detailed on the grounds of the sheer volume of information required for the ship's manifest. And with this risk, there is a greater probability of a risk of danger owing to the lack of awareness on the part of both the ship's master and the agent of all hazardous or dangerous cargoes, or any other items potentially deemed as being prejudicial to the safety of the vessel, its crew or the port itself. Indeed, it is becoming evident that certain ports in Europe, including the UK, may not be able to handle such vessels, such is their size as well as the quantity of their containerized cargo.

It is the responsibility of the agent at the port of loading to ensure that the correct information is given to the vessel's master concerning the cargo being loaded aboard the vessel, as the cargo manifest containing such information must agree with both the bills of lading and the mate's receipt, which is duly stamped and signed by the master or the mate. If the information should be lacking in any way, then it is the direct responsibility of the agent at the port of loading to shoulder any liability resulting from loss or damage in the event of an accident or a disaster befalling the vessel during the voyage or on arrival at the port of destination. In this respect, a great degree of professional responsibility is required on the part of the agent, along with a considerable knowledge of the rules and procedures involved in vessel management. In many cases, larger agency companies have offices in a variety of port locations, and deal with a wide range of vessel and freight-related activities, ranging from chartering through port and liner agency to freight forwarding and Customs clearance.

4 ISO 28000/ISO 28001 AND SIX SIGMA

As well as initiatives introduced by organizations such as the IMO and the World Customs Organization (WCO), the International Standards Organization (ISO) has endeavoured to introduce a series of international standards implementing the individual Codes such as ISPS requiring all worldwide port authorities and shipping lines to implement ISO standards in order to maximize their security potential. The ISO 28000 initiative has been introduced to apply a security standard to the international supply chain, by implementing a set of procedures and checklists for all exporters and importers when shipping consignments of goods overseas. The standard requires each exporter to ensure that all consignments being exported are subjected to a series of checks prior to the goods being packed and containerized for security purposes, based on a security risk assessment, and in the form of a security management system. The purpose of the implementation of such a set of procedures is to anticipate any potential risk and reduce or eliminate it at the point of the goods being despatched from the exporter's premises. The drawback in the system is that it refers to the actual goods themselves, and the ability of the exporter to control the shipment. It does not necessarily relate to the documentation accompanying the consignment.

One of the main points of ISO 28000 is the security management system. It states:

- An organization must establish, document, implement, maintain and continually improve an effective security management system for identifying security risks and controlling and mitigating their consequences;
- An organization must define the scope of its security management system;
- Where an organization outsources any processes affecting conformity with these requirements (including Ex Works shipments), the organization must ensure that these processes are controlled, and that the necessary controls and responsibilities of such outsourced are identified within the security management system.

Under the EXW principle this may be a vague area, as the exporter bears no responsibility for the actual shipment. However, within the security management system there are five main action elements:

- policy;
- security risk assessment and planning;
- implementation and operation;
- checking and corrective action; and
- management review.

This implies that a constant self-corrective action plan should be drawn up by the organization and adhered to at all times, suggesting more responsibility being placed on the organization for ensuring that it does have control over all its shipments, both inward and outward. In itself, this is a worthy solution and it can be used effectively. However, the wheel has once again been re-invented, as the whole process defined above bears a similar relationship to that of the Six Sigma process.

The Six Sigma process can be defined as:

- **D**efine;
- **M**easure;
- **A**nalyse Data;
- **I**mplement Changes; and
- **C**ontrol the Process; or, DMAIC, for short.

In reality, the organization content to work within the 3–4 Sigma scale will encounter a problem level of between 25% and 40% or errors requiring addressing in a process. Working towards a Six Sigma level will reduce this to below 0.01% of errors in the system. The actual table used to define the Sigma level (process capability) of any organization is based on the level of defects per million opportunities, i.e. each transaction. It seeks to control the level of allowable defects (if any defective operation can ever be seen to be allowable, as most organizations will seek to reduce their defect acceptance level to zero wherever possible).

SIGMA level (process capability)	*Defects per million opportunities*
2	308,537
3	66,807
4	6210
5	233
6	3.4

Table 1: Probability of Defects of Different Sigma Levels

Although this system is used primarily in production processes to increase quality levels, it can also be used in the service sector equally effectively, especially in terms of the enhancement of security within the supply and logistics chain.

The use of such controls within the Six Sigma process can include:

- the number of correct reports issued in advance of the arrival of all vessels in port per month, compared with the number of actual reports submitted;
- the number of correct reports issued in advance of the arrival of all vessels in port per month, compared with the number of actual arrived vessels; and
- the number of correct cargo reports issued per manifest, compared with the number or actual entries on the manifest.

The analysis of such data will yield the number of successes against the number of actual reports, and will enable the authorities concerned to tighten up their procedures to ensure that all vessels arriving at any port must adhere to the reporting requirements set out at very least by EC Directive 2002/59/EC. It already appears that in many cases, the harbourmaster may not know about all movements of vessels into and out of the port prior to those involved with berthing the vessel and handling its cargo. According to EC Directive 2002/59/EC, the purpose of the exercise is for the vessel to actively submit an advance report to the port of arrival giving all its essential details, including cargo, prior to its arrival. This information must therefore be submitted by the vessel to the harbourmaster as well as to the port VTS operators in advance of its arrival, as well as by the vessel's agents at the port, a situation which does not happen with the required frequency.

This means that any organization maintaining control over the security of its shipments will ensure that it will rarely, if ever, encounter problems relating to those shipments, as it will seek to ensure that all information relating to shipment documentation is correctly completed and recorded, and that it has full access to such information and documentation. This effectively rules out the present principle of EXW, and pushes it more towards free carrier (FCA) or further along the INCOTERMS chain.

It should be pointed out that the Six Sigma process works on the basis of Six Sigma (six standard deviations) from the average calculated as the mathematical mean of any process, and that the closer an analysis comes to Six Sigma, the closer the process comes to perfection, as a Six Sigma measurement allows for virtually zero imperfections in a system. Indeed, the Six Sigma approach may work better than the ISO 28000 approach for a security management system.

ISO 28001 refers to Customs controls and how containers are packed and loaded aboard a vessel. It refers not only to the consignment in terms of physical checks made prior to export, but that the cargo manifest refers to and agrees with the consignments within the container. Again, the information may not be sufficient to satisfy all requirements, in that agents still apply generic terms to consolidations, rather than necessarily recording all exact details of each consignment within the container. Only with the CT-PAT initiative has some attempt been made to itemize in detail all consignments entering the United States and Canada from overseas by maritime means. However, the same rules have yet to be applied to other countries, especially the European Union. The adoption by the WCO of a standard unique consignment reference (UCR) for all imported and exported consignments is only part of the solution. In many cases, the UCR may refer only to a consolidated load, and does not necessarily refer to all consignments within that consolidation. There is still the risk that the information provided on either a cargo manifest or a bill of lading may bear little relation to the cargo actually loaded into the container and aboard the vessel, and this may still emanate from the fact that the party arranging the shipment made the decision to consolidate every cargo loaded aboard the container, and simply instructed the agent to provide a basic set of information, rather than exact details of every load therein. This arrangement of the shipment also depends upon the term of delivery (the INCOTERM) used, and thus is open to considerable interpretation and discretion on the part of either buyer or seller.

The other main reason for Customs involvement is the move away from the examination of consignments at the port, and towards self-regulation by the trader. The authorized economic operator (AEO) initiative is partially designed for this purpose. Any trader wishing to be approved by Customs for such status, namely a privileged fast-track form of clearance of consignments through Customs, will have to ensure strict compliance with a series of regulatory requirements partly based on the ISO 28001 initiative, and aimed at ensuring greater degrees of security and compliance in terms of information supplied by the trader to the Customs authority through electronic means. The electronic form of declaration has taken over from the traditional approach to examinations and clearance internationally, and in turn Customs frontier resources have been reduced, especially with regard to port controls. In the UK, it is expected that the AEO status will be initiated in 2007, and will be fully achieved some time beyond 2010.

Although ISO 28000 and ISO 28001 go a long way towards highlighting risk in the supply chain and attempting to address and reduce this risk, they do not answer all the questions. The increasing size of container vessels and hence the increased amounts of cargo carried inevitably mean that more information for these cargoes is required, especially on an electronic basis, and hence there is a higher risk that such information may not be sufficiently scrutinized in detail to ensure that all cargoes are properly screened prior to entry into another country and cleared through border controls. The emphasis is to move the container through the port as quickly as possible to the trader's premises, with the minimization of delays for examination on the way. Inevitably, there is the risk of corner cutting, and the fact that computers do not always make the correct decision. In this way, the risk of some information passing through the net is increased, and hence the risk of accidents occurring or threats of terrorist attack by exploiting any loopholes in the system, especially where the master of the vessel may still be unaware of the nature of all the cargoes aboard the vessel because of omissions by the agents inputting the original information for each cargo at the time of loading aboard the vessel.

5 PERCEIVED ANOMALIES

In assessing the principle of marine reporting, several anomalies arise which require addressing in the maritime sector. These include:

- requirements of the national maritime authority;
- the reporting of the vessel to the port of destination;
- the reporting of the vessel in restricted international waterways;
- the details included in the report; and
- shared responsibility between the owners of the vessel and the agents.

5.1 Requirements of the National Maritime Authority

Each national maritime authority has its own national or supranational marine reporting requirements, as in the case of the EU. Those requirements are based on the legislation passed by the national government, or, in the case of the EU, Directives issued by the Commission in Brussels. In the case of the EU Vessel Reporting and Monitoring Directives, each member state takes its own action based on its interpretation of the Directive. In the case of Denmark, a VTS system already exists covering the Storebaelt, the strait passing though Danish national territory, but a system has yet to be implemented in the Öresund, the strait separating Denmark and Sweden. Conversely, a mandatory vessel reporting system covering the Strait of Dover is jointly operated by the UK and French authorities, whereas there is no system whatsoever covering the North Channel, the strait separating Scotland and Northern Ireland. All shipping movements through the North Channel are monitored at a distance by the AIS system used by UK coastguards, and even this does not physically control or monitor vessel movements. It merely shows the vessel movements through the Channel on a computer screen at a considerable distance from the strait, in the coastguard building at the other end of the Firth of Clyde. This situation is detailed in a case study at the end of the text.

5.2 The Reporting of the Vessel to the Port of Destination

Unless the vessel's owners have their own representation at a port, it is normal practice for the vessel's agents at the port to report the arrival of the vessel to the port authority, although this practice is not necessarily carried out within the requirements set out in EC Directive 2002/59. This report will give details of the vessel, some general details of its cargo, and the berth, dock or wharf required for the purposes of unloading and loading. To this extent, some general details of the cargo are included, especially as the cargo manifest for the vessel must be submitted to the Customs authority for the purposes of cargo examination by Customs should the need arise. However, with the increase in size of container vessels, the complexity and size of the cargo manifest has also increased. Besides which, although the 24-hour reporting rule applies for all vessels entering port (or at least an inbound report once the vessel has left its port of departure, assuming a voyage of less than 24 hours), the agent does not always report the arrival of the vessel to the harbourmaster, even in the case of the vessel carrying dangerous or hazardous (HAZMAT) cargoes. It is to be expected that as part of any reporting mechanism, the ISPS rules at security level 1 pertaining to the security arrangements for the vessel itself are obeyed when the vessel enters port. The rules pertain to the security plan of the vessel and those responsible for the vessel's security. It is often the case that the harbourmaster only receives information concerning the vessel's arrival via the port authority once the agent has already notified the port authority. In theory, however, the port harbourmaster will have a list of vessels expected to arrive at the port some time before their actual arrival, as the agent will have made arrangements for the docking of the vessel some time in advance of the vessel's arrival, usually some weeks. It is the express duty of the agent to complete a declaration (the agent's declaration) to the port prior to the vessel's arrival, giving all relevant details of the vessel concerned. However, this declaration assumes all known facts are correct; it does not account for any sudden change in the vessel's condition or circumstances, such as accidents aboard a vessel, problems with the vessel itself or its cargo.

In brief, therefore, it is the responsibility of the ship's agent to declare the vessel's arrival to the port authority well in advance of that arrival, and to ensure that all information about the vessel and its crew and cargo is known to the port and other authorities accordingly. However, the normal 24-hour reporting rule is not often obeyed, implying that certain information may not be transmitted to the port authorities in the acceptable manner. There are many instances where the harbourmaster is the last point in the chain of contact to know of the vessel's impending arrival at port. The port authority itself will, however, already be well aware of the vessel's arrival, having been informed by the vessel's agent well in advance of the vessel's arrival.

5.3 The Reporting of the Vessel in Restricted International Waterways

When a vessel is entering restricted international waterways such as the Strait of Dover, the Öresund or the Storebaelt, it is the duty of the master of the vessel to notify the international authorities of each country bordering the strait in question concerning the vessel's passage through the strait, despite the status of the vessel enjoying the rights of innocent passage through the strait, as encompassed in maritime law and stated in the UN Convention of the Law of the Sea. In this case, it is not the task of the vessel's agent to do this, as the vessel may not be calling at a port near the strait in question. It is the direct responsibility of the master of the vessel to carry out this task. However, such reporting may not always be undertaken, as the use of AIS may simply pick up the vessel on radar and monitor it through the strait in question. Only where a mandatory vessel reporting system exists will the master be obliged to report the vessel's presence and intentions as part of its sailing plan, especially where the vessel may be carrying hazardous or dangerous cargoes. In this respect, a more proactive control regime such as vessel traffic systems (VTS) facilitates a greater control over the vessel in question by allowing the constant monitoring of and contact with the vessel while it remains within the domain and scope of the control system. The drawback of the VTS regime is that it does not take account of details of the vessel's cargo or its crew. As with the AIS system, it simply identifies the vessel and its registration details. Because of the VHF radio channel frequencies available for contact between the vessel and the monitoring authority, contact with the vessel's master may be maintained by radio link. However, the purpose of the VTS system is to monitor and track the vessel's movement. Although the VTS operator may issue guidance to the master of the vessel for the purposes of navigation through a channel within a restricted waterway, the system used does not actively intercept that vessel for security purposes, nor does it request details of the contents of the vessel. The information provided will refer to the identification of the vessel and its destination. In this respect, there is a distinct difference in the responsibility for the identification of the vessel depending upon whether the vessel is passing through a strait of international water or whether it is calling at a port in the area. It is this distinction which determines which party, i.e. the vessel or its agents, should declare the vessel's presence to the authorities.

5.4 The Details included in the Report

The reports for the arrival of a vessel at port or its passage through a restricted international waterway differ radically in their content and detail. Details of the vessel's cargo, however general, are required for the vessel's arrival at a port, whereas these are not required at present for the purposes of a vessel's passage through a restricted international waterway. A report for a vessel passing through a strait deals solely with the identification of the vessel, whereas this information is increased to include general details of the vessel's cargo when it arrives at a port, partly as the vessel is entering national Customs territory when it arrives at the port and is therefore required to declare all items it carries, including details of the crew, passengers, stores and cargoes, according to the international IMO FAL regulations. Cargo reports are usually of a more detailed nature, given that the cargo manifest should give full details of all cargoes carried aboard the vessel. This document is also supported by the mate's receipt, which is the document showing that the master of the vessel is certain of all the cargoes carried by that vessel. This set of documents should also be supported by all bills of lading relating to the cargoes aboard the vessel, although in cases of consolidations, FAK or "Said to Contain", this is often not the case. To this extent, cargo manifests and other reports may be scant in the details they provide, which does not give rise to adequate security of cargo or even the safety or security of the vessel itself. Even in an age of increasing tonnages of cargo vessels there is still the need for detailed reports of the cargo of any vessel, and this detail should be known by any relevant authority whether a vessel is passing through a strait or entering a port. In this way, such details can be passed between the authorities concerned in order to allow for the full transparency of any maritime reporting regime.

5.5 Shared Responsibility between the Owners of the Vessel and the Agents

Ultimately, the owner of the vessel is responsible for the safety, security, upkeep and well-being of the vessel at all times, although it devolves a certain degree of that responsibility to the agents when the vessel enters port. However, the owners of the vessel equally devolve the responsibility of the reporting of the vessel to different parties depending upon the circumstances of the vessel at a particular point in its voyage. The sailing plans are the responsibility of the master and the crew, as well as any charterparties using the services of that vessel. The reporting mechanisms required for sailing through restricted international waters are the responsibility of the master of the vessel, while the responsibility for declaring the vessel's arrival at a port are devolved to the ship's agent at the port in question. In this respect, the vessel's owner takes little responsibility for the vessel's activities, other than those basic legal responsibilities required of the owner. The rest is split between the vessel's master, the agents and perhaps the vessel's charterer.

There is a requirement, therefore, for a degree of collective responsibility relating to all parties involved, concerning who should accept responsibility for what function. It is unfortunate that the use of electronics for the purpose of vessel monitoring does not allow for in-depth scrutiny of information relating to both the vessel and its contents. Various rules pertaining to the responsibility for various degrees of reporting functions are often overlooked in the interests of expediency, and often do not account for the complete situation concerning the presence of a vessel in a specific location, especially in an international strait or on the approach to a port. If information is not required or specifically requested, it will not be divulged. A major area of anomaly concerns how much information should be divulged by the operators of a vessel, the vessel's agents or the vessel itself. The net result is that between all these considerations, there is no standardization in the detail or the amount of information available to the maritime authorities from any vessel. It is ultimately this anomaly which needs to be addressed in order to achieve complete control over not only a vessel's movements but also what it carries for overall security purposes.

There are therefore several anomalies in the marine reporting system which can give rise to breakdowns in communication between the vessel and the national authorities. Many of the anomalies refer to the level of basic information required by each of the authorities, but the main concern is to what extent maritime security is being prejudiced by the lack of essential information pertaining to not only the vessel itself, but also the cargo it carries. If such details are not adequately reported, then safety or security issues could be severely compromised. In an age of insecurity and uncertainty, such failure to fully report any information relating to the vessel or its cargo engenders an increasing level of risk, which may in turn compromise the level of national security for any nation concerned.

REFERENCES

Churchill, R.R. and Lowe, A.V., 1999, *The Law of the Sea*, 3rd edn, Manchester University Press.

Wilson, J.F., 2004, *Carriage of Goods by Sea*, Pearson Longman.

Branch, A.E., 2005, *Elements of Shipping*, Routledge.

The International Maritime Organization, 2004, *The ISPS Code*, London: IMO.

The Maritime and Coast Guard Agency On-line, *www.mcga.gov.uk*, accessed 26 September 2006.

This page intentionally left blank

CHAPTER 2

GLOBAL TRADE SYSTEM: DEVELOPMENT UPDATE

Dean L. Kothmann

Electronic Data Systems (EDS), USA

Abstract
In 2003, a global trade system was presented to the United Nations. Industry presented a concept for a global trade system that meets the need to improve the logistics processes to handle improving global trade, and at the same time, enhancing global trade security both to and from all participating nations. This concept has progressed to the implementation phase. This chapter is an up date of the progress made, and the future direction of a global trade system.

1 INTRODUCTION

Today's logistics and supply-chain security challenge is to meet the security needs of a nation while improving logistics and growing commerce. The challenge is not just container security, consolidated shipment security, or bulk shipment security, neither is it the sole creation of safe shipping corridors. It is the ability to engage the world in a global trade, development and security solution that is good for all nations; a solution that does not favour one nation, one port, one vendor, or one individual over another. The challenge is to prepare the world for the near future in which development must occur in third world nations as well. The absence of a robust capacity to filter the illicit from the licit in the face of (a) a heightened terrorist threat environment, and (b) the growing volume of people and goods moving through international trade corridors, places US and global commerce at frequent risk of disruption.

A global trade system demands that more information flows, that it flows faster, and that it becomes more useful as subscribers increase and share information more broadly. In this regard, a global trade system must have the following attributes:

- be available for adoption by all nations;
- apply to all commercial shipments by all modes of transportation;
- be useful to discover all contrabands;

- be structured to secure global acceptance and use, achieving rapid adoption;
- be universally useful, not designed for one user or a single purpose;
- improve commerce without imposing additional cost;
- significantly reduce delays and improve the speed and effectiveness of commerce;
- provide a global response to deal with any transportation incident requiring global intervention or notification;
- increase the system's value and enhance security as the data flow increases when more countries adopt the system;
- provide accurate and reliable data to all stakeholders;
- provide information for verification/validation of manifest;
- provide information on tracking of containers and contents; and
- be capable of incremental, evolutionary growth with no reduction in efficiency or effectiveness, from initial implementation to full utilization.

The challenge is therefore to achieve the business benefits described previously. However, the response to this challenge has been to focus on technology to solve the problem with less emphasis on the business drivers. Essentially, this is a business process innovation requiring realignment of processes and reallocation of people. The technology is in the role of supporting the defined business change.

2 OVERVIEW OF CURRENT GLOBAL TRADE SYSTEMS

Current global trade systems fall into three categories:

- government sponsored or built systems in the highly industrialized nations;
- privately built, profit-making vertical systems; and
- private stakeholder and value added network systems.

The global trade system offers a fourth approach, a shared consortium-based, mutually beneficial, infrastructure approach.

2.1 Nation-Sponsored/Supported Systems

2.1.1 Nation-Centric Systems

The industrialized world has funds to develop their own systems. For example, the United States has adopted the automated commercial environment, or ACE, as a redesign of the systems and processes of US Customs and Border

Protection (CBP). ACE is a key to CBP's long-term vision for trade management, though the results have been slow in coming. ACE was initially envisioned as part of the 1993 Customs Modernization Act, but is only now coming into reality. It will replace the CBP's current import technology, the automated commercial system, which has been in place since 1984. Lack of Congressional funding and other factors led to many delays in ACE realization. According the CBP website, ACE will enable automating time-consuming and labour-intensive transactions and moving goods through the ports and on to markets faster and at lower cost will simplify dealings between CBP, the trade community and other government agencies. Among other capabilities, CBP personnel will have automated tools and better information to decide —before a shipment reaches US borders—what cargo should be targeted because it poses a potential risk, and what cargo should be expedited because it complies with US laws.

The system will have a number of benefits to importers, including further electronic automation, better access to information and, starting last year, the ability to make a single monthly duty payment, rather than on a transaction-by-transaction basis, as in the past. ACE creates for all imports a periodic monthly statement, which must be paid—interest free—by the 15th day of the next month. This will both improve importer cash flow and greatly relieve the administrative burden. The goal is also to make available about 80 reports on-line through the ACE web portal on a wide variety of import and customs data, enabling importers to get much better view of customs compliance and other import activities.

Other countries have developed similar systems at less than the cost or complexity of the United States' ACE system. These systems are country specific. If one were to use a credit card analogy, these are the "house credit cards" analogous to the cards issued by a specific gasoline company or a large consumer retail company. The cards are issued to attract customers, increase market share and improve the bottom line. These systems are designed for the benefit of the country which issues them. Nations develop these systems to increase Customs revenue and to manage the security of their nation. National systems are very expensive, return little if any business value and can impose a burden on the users. Second and third world countries are challenged to adopt these systems because they lack funds and expertise to build, operate and maintain the systems.

2.1.2 Local Community Systems

A second type of government system has been developed by local communities to enhance revenue. Such systems are similar to ACE, but they network the community. The community is likely to be an inter-modal traffic node or a port community. The community develops these systems to make themselves more attractive to the global logistics community and to solve community problems of traffic congestion, regional development and community integration. These systems can be mandatory in some communities. These systems have met with mixed success because they are more difficult to integrate with global logistics stakeholders and many lack a business model attractive to industry.

2.2 Private Vertical Systems

Private vertical global trade systems have emerged because integrating 20 to 30 participants and stakeholders to complete a global transaction challenges the best third and fourth party logistics providers to find the lowest cost and most efficient route. Examples of private vertical systems are Federal Express, United Parcel System and DHL. These systems are similar to American Express in the credit card industry. American Express wished to create an alternative to traveller's cheques. The famous AMEX card was the result of this development. Vertical integrated systems offer unique functions and features that other systems cannot provide since other systems cannot adequately integrate all the participants. Like American Express, the primary barrier to development of these systems is cost. The firms developing and deploying these systems are faced with renewing their technology every five years and the total long-term cost can be huge. These costs must be passed on to users. The users adopt the systems because they must have features and functions that can be offered only by a vertical closed system.

2.3 Private Proprietary and Value-added Networks Systems

Other forms of private stakeholder systems have evolved as well. For instance, SAVI has developed a global system along with partners and owners Hutchinson Whampoa and Lockheed Martin. These proprietary systems are an outgrowth of an existing business. These systems are offered by those already involved in logistics systems and are an outgrowth of that logistics involvement. They are similar to American Express as well. They are proprietary and require adherence to the proprietary system standards. The weakness of these systems is generally high cost and the desire of the owner to lock users into only their system. These systems are not inter-operable across other proprietary or government systems.

Value-added networks have also emerged in parallel with proprietary systems. An example of a value-added network is e-modal and international expediters. These systems are as good as the data providers. The systems have data that is entered multiple times in multiple records and are capable of recording only a limited number of logistics events.

Each of these models have recurring weaknesses of:

- cost control and technology refresh strategies;
- data integration and data quality problems; and

- and the ability of the users to form a mutually beneficial consortium and work together on common governance and common problems.

3 SHORTCOMINGS OF EXISTING SYSTEMS

3.1 Systems Development and Maintenance Costs

The first common problem is cost escalation for operating and maintaining these systems. Private systems are experiencing cost escalation because requirements are changing more rapidly as nations respond to increased concerns with border safety and revenue losses at the border. Security requirements continue to increase, systems must change to accommodate the new requirements. Technology change and escalating security will continue and, therefore, cost escalation to these systems will continue.

3.2 Data Integration

The second common problem is integration of data across disparate systems. The data integration and quality problems occur even for those using electronic data interchanges. Value-added networks address data integration and quality problems, but the solution set is very limited and, therefore, addresses a narrow set of needs.

3.3 Governance Issues

Governance is addressed in national systems with pre-defined stakeholders groups, but the governance and agreements are limited to one country. The World Customs Organization (WCO) is a forum for all nations to address these concerns collectively, but the solutions are focused on the lowest common denominator and are frequently focused on the government requirements and are not business friendly. Further, final decisions on improvements and requirements are decided by the controlling government rather than by consensus of the governance consortium. Last, these systems do not allow for common negotiations between an industry group and government. Governments are reluctant to reach agreement with one company, excluding others giving one company an advantage over another.

These shortcomings present the opportunity for the development and market acceptance of an open, non-proprietary, non-government controlled system. This system would be comparable to Master Card or Visa. Master Card and Visa were developed to allow any bank representing a seller to work with any bank representing a buyer. The banks use a third party to act as an intermediary between the two banks. The banks own this intermediary through a membership programme. Nations allow the member banks to create self-regulating rules which the nation approves. The result is a self-regulating system of credit that does not favour any nation, any community, or any company. All players in the credit system are on an equal footing and use a common shared infrastructure that is controlled by private industry and not the government.

4 THE TRADE DATA EXCHANGE: A GLOBAL TRADE AND OPEN SYSTEM

A fourth system type which recognizes the disadvantages of earlier trade facilitation systems is being developed around the trade data exchange (TDE) and its self-regulating organization (SRO). TDE provides:

- the global infrastructure;
- an "open" non-proprietary model;
- accountability; and
- a consensus-based governance framework that is necessary to create a global trade network.

TDE provides a means for all nations to jointly address global trade, development and security issues. The trade data exchange is the result of the development of a common and shared logistics data solution that is implemented across all nations, all transportation modes, all industries and all participants. The solution is a trade data clearinghouse using the backbone of a common secure virtual private network (VPN). In addition, TDE employs international standards including electronic product code-global and ISO's 28000 series on trade lane security. These standards provide a common naming system as well as common processes developed through interaction of global trade lane participants. TDE business model uses a business approach similar to the credit card and stock exchange industries. The economics of the model are derived from the requirements which include trade lane visibility, trade lane participant accountability and the use of a common shared system to share cost.

In sum, TDE provides industry branded data capture and transactions. It provides commercial industry with a means for single data entry and elimination of handoffs and these alone create benefits and value for commercial industry and governments. The self-funding, self-regulating, and value creation aspects of the model create an attractive solution for industry and government, and also provides the means for joint industry–government involvement and agreement.

4.1 Global Trade System Concepts

Three interlinking infrastructure components are required to achieve a global trade system. These components are inspection, sensing and tracking (IST), profiling, and a business model with a data-sharing mechanism. To be successful, no one component can be effective without its other two partners. Each component supports and supplies answers to the other components.

The sensing and tracking infrastructure is the physical infrastructure that provides the knowledge of where a shipment is, what is in a shipment and all participants involved with the shipment. This infrastructure has four key components:

- visibility of the data in the network provides the shipment's stakeholders with access to IST information that has logistical value;
- a set of auditable inspection standards provides the Customs agency of the importer country with valid information on imported and exported cargo to conduct Customs business;
- the network helps track all people, cargoes and stakeholders and their actions at each stage in the cargo movement. This results in accountability for the cargo at each stage of its movement; and
- sensors allow for the physical verification of cargo location. By design, tomorrow's sensors will use the same infrastructure.

The cargo profiling infrastructure will accommodate data from many locations. The data must be integrated and verified. Profiling is an activity that has three major objectives:

- governments want the data to look for anomalies, determine risk and threat and improve the security of imports arriving in their country;
- buyers of goods want commercial logistics improvement, accountability and predictability of movement and delivery and response in case of a logistics event; and
- stakeholders want valid data. Profiling provides a means to compare data fields throughout the shipping cycle to test the validity of each entry.

The TDE infrastructure flow of commercial shipment data provides stakeholder access for each shipment. Data accumulation for a shipment begins with the buyer of goods. Data will continue to accumulate as each stakeholder accesses, processes and adds to the data for each shipment. Users include all stakeholders including ports, shippers, freight forwarders, insurers, law enforcement, Customs, importers, exporters, third/fourth party logistics providers and security agencies.

4.2 Governance and Ownership—The Unique Solution

The ownership and governance of the system is what creates a unique solution. Based on extensive experience, industry wants to own its global trade system because it is their data that transits the trade system. The data is owned by the firm that creates the data or by the firm that contracted to have the data created. Multiple firms participate retaining ownership of their data but understanding that the trade system is "collectively" owned by all stakeholders.

Once "collective" ownership is established, a number of concerns are resolved, including:

- handling proprietary information;
- distribution of the revenue; and
- decision-making process to deal with emerging issues.

Resolution is achieved by establishing ownership of the data and of the trade system. The owner decides how the issues are resolved. This approach has been used in the credit card example cited earlier. The model will also work for the logistics industry.

The ownership consortium is governed by the owners. The owners define the business rules and processes. The rules and processes affect government processes and functions and, therefore, governments should have control of the rules and processes that impact them. The owners will negotiate these agreements of oversight and control and the government will audit for compliance. This construct of ownership and governance is not new. It is a self-regulating organization. The credit card industry and stock industry have operated under this model for years. The United States phone system was built as a monopoly under a similar type of system of ownership and governance. The approach allows private industry to achieve its goals of efficiency and privacy, while government can also achieve its goals of revenue and security. The self-regulating organization and collective ownership provide solutions which offer many of the attributes of the infrastructure previously discussed. The key to the new TDE solution is putting in place a mechanism to deal successfully with the issues of cost, data sharing and a common set of business rules. These challenges require a focus on new processes, change management and changed, improved governance methods.

The global trade system team has worked with ISO in the development of a common security standard, ISO 28000 series. This standard allows for the development of an industry process approach to trade lane security. A common system owned by the users, instead of an industry stakeholder, country, or service provider offers the opportunity for members to create processes that each member will follow. The self-regulating nature of the group means the violator may be asked to leave the organization since the other members' profitability will likely be affected. This type of consortium-based organization also creates the opportunity for members to negotiate an industry approach to standardize border crossing information for the movement of cargo from any country to any other country. An individual private company cannot do this. Trade organizations attempt to develop solutions which achieve the previously stated goals and may occasionally be successful. Communities of members working together significantly improve the confidence that the stakeholders benefit will enhance a nation's benefit, so "the whole is greater than the sum of the parts" creating a "win" for all.

5 GLOBAL TRADE SYSTEM IMPLEMENTATION

The development of the global trade system was initiated in April 2001. The initial concept was presented to the United Nations in May 2003. The concept was presented to the WCO during 2004. The project was initiated as part of the Department of Homeland Security and Department of Transportation sponsored Operation Safe Commerce, the Advanced Container Security Device, and Intelligent Transportation Systems programmes of the United States government and continued through 2004 and 2005. A proof of concept was developed through the establishment of Kansas City SmartPort during late 2005 and early 2006. The global trade system concept has progressed toward reality by completing the initial conceptualization and design, implementation of a proof of concept and subsequent prototype by partnering with the Kansas City SmartPort government and industry consortium to begin development of an operational prototype.

5.1 Trade Data Exchange—Purpose, Value and Benefits

The goal of the trade data exchange is to create a true end to end (E2E) system. The system will have the ability to track goods from the original purchase order to the cash register or point of consumption. The trade data exchange will create a continuous cargo visibility and integrity network. Visibility, accountability, process efficiency and security are frequently spoken words in conversations about supply chains and global trade logistics. Yet, these are more concepts than reality; currently shipping documents are not sent electronically through the supply chain and logistics companies still perform manual, time-consuming processes to move and deliver cargo. The market needs a viable method to link all stakeholders and provide synergy to the business of global trade. TDE is a cargo data risk management clearinghouse that connects importers and exporters, carriers, freight forwarders, brokers, financial institutions and governments along the supply chain. The trade data exchange is a shared logistics data solution implemented across all nations, all modes, all industries and all trade participants.

The implementation of the global trade system and a TDE will modernize logistics and result in the next generation of trade data management. In the modernized system, commercial industry realizes value in the following areas. Each member of the supply chain in each segment of the supply chain is held accountable for their task. The accountability to a mutually agreeable third party allows for new performance metrics and the ability to contract to those performance metrics. As a result, there is increased effectiveness and optimization of supply-chain assets and operations. A next generation just in time (JIT) supply chain will evolve from adoption of the TDE and the supply chain will enjoy increased visibility of shipments, assets, people and security.

Regional communities realize economic development through improved logistics, regional as well as global. The process of gathering data for all businesses assists local businesses to become more global. Regional communities are able to integrate local logistics data into global logistics data and learn where they need to optimize the system to drive more exports from their community. The community has an increased understanding of the local economy and the logistics and transportation associated with the local economy.

Countries using the TDE gain an earlier and greater knowledge of cargo entering and leaving the country. They are able to use this information to improve investments in regional economic development. The information enables the country to improve targeting of illicit goods, to increase security and to increase Customs' revenues.

Logistics providers have shown interest in the exchange due to a need to modernize their information systems. Increased obsolescence is occurring as a result of:

- global security requirements driving change in process as well as tool; and
- technology continues to advance, and information systems are expensive to replace due to technological obsolescence.

A shared system serving third party logistics providers as well as carriers will become the low cost and most effective model. This shared system economic model succeeds in telecommunications, in airline reservation business, insurance business, the credit card industry and other industries. The trade data exchange allows these providers to retain their competitive advantage while using the shared infrastructure to reduce their fixed cost and achieve greater efficiencies through positive cargo tracking achieving accountability and predictability of cargo movement.

Interest in the system is growing. Users want the features and functions of express carriers for their freight without increased cost. The shared infrastructure provides user control and choice rather than a private vertical solution that mandates standards and requirements and is more expensive.

5.2 TDE Functional Components

The key functional components and associated constituent data flows reveal the operational aspects of the TDE. TDE has seven core functional components: documentation origination, logistics transactions, sensing network, freight risk management, credentials identity, traffic information integration and electronic payment.

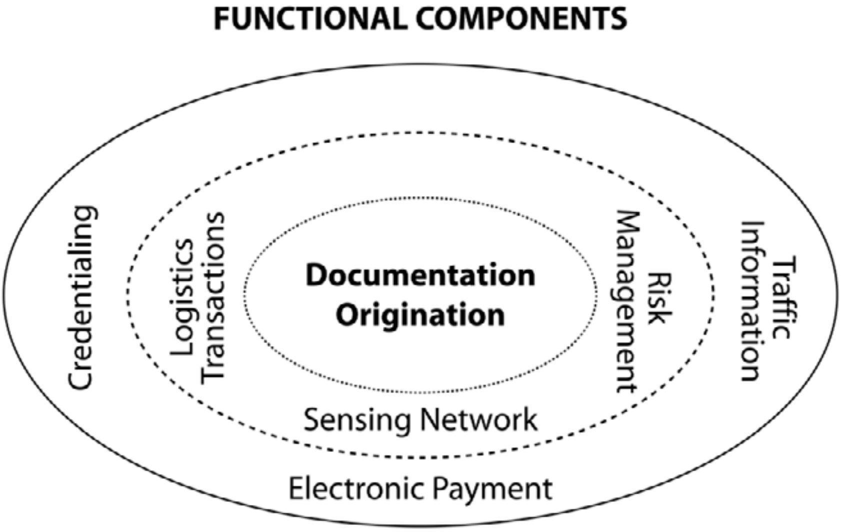


Figure 1: Trade Data Exchange Functional Component

5.2.1 Trade Documentation

A SmartPort branded portal is the TDE user interface through which trade partners gain secure access to all shipments data limited by role-based permissions. SmartPort members exchange shipment data to electronically create and validate commercial trade documentation and to streamline the delivery of commercial trade documentation.

5.2.2 Logistics Transactions

The TDE transportation logistics functionality is the collaboration environment for trading partners to connect and share shipment events, communicate via electronic messaging, receive electronic notifications and proactively monitor shipment progress. The TDE enables well informed logistics choices based on trade lane performance metrics.

5.2.3 Risk Management

The TDE uses data fusion technology to aggregate trade lane data and shipment data to provide commercial risk assessments and provide in-depth cargo, trade and shipper analysis capabilities. When anomalies are identified in trade lane events, risk management interfaces with threat presence services enabling defined escalation and notification.

5.2.4 Sensing Network

The TDE leverages commercial off-the-shelf sensor and tracking components connected through the SensorNet framework to capture in-transit shipment data. The TDE compares route and shipment data to trade lane metrics, continuously monitoring the shipment's end-to-end progress.

5.2.5 Traffic Information

The TDE's multimodal traffic information capabilities inform transportation and logistics service providers of the current status of their shipment. By integrating industry-standard messaging from ground, rail and maritime carriers, the TDE has the ability to provide near real time data of a shipment's location—at any time, at any point throughout the trade lane.

5.2.6 Credentials Identity

The TDE provides the means by which SmartPort members can ensure accurate authentication of participants in their supply chain. The TDE's credentials identity capabilities complies with government objectives for secure, standardized credentials to identify transportation workers whose duties require physical access to secured areas of the transportation system or require cyber access to computer-based information systems related to the security of the transportation system.

5.2.7 Electronic Payment

The TDE accelerates financial transactions process through the use of electronic payment solutions. As a result, SmartPort members can leverage cost-effective means to identify and address financial inefficiencies in the supply chain. The cost savings achieved enable SmartPort members to refocus financial resources to more business-critical areas.

The governance and managed flow of trade data is the heart of the TDE concept. All parties involved create, manage and transmit "branded" trade documentation necessary for the movement of goods. With the TDE, stakeholders enter data once and use many times. Governance creates the ability for the data to become branded.

The common architecture, governance and community create a branded data transaction that has compatibility and conformity. These attributes of the TDE reduce logistics costs and users costs through improvements in processes and utilization of people and assets; improvements are not realized because the

TDE is superior or inferior technologically to the competing systems. A greater understanding can be achieved by reviewing the uses of each constituent and its related data flow.

6 KANSAS CITY SMARTPORT: OVERVIEW AND DESCRIPTION

6.1 The Origins of Kansas City SmartPort

Exports from Asia, particularly Southeast Asia and China, have increased significantly over the past 10 years. Over the past year alone, imports from China have spiked 33.2% and exports increased by 13.7%. This large import/export volume has created a systematic limitation on key US ports, particularly the port of Los Angeles/Long Beach, to the point where alternate West Coast ports will reach full capacity in five years.

Co-terminously, an investor-managed group in Kansas City, known as Kansas City SmartPort, recognized the strategic transportation position of Kansas City and has actively worked to expand its role in domestic distribution, often as the recipient of goods originating in Asia. SmartPort is involved in several very timely and significant trade lane development projects that will result in increased traffic through the Kansa City area. Further, SmartPort is developing a US export capability.

The key ports of entry on the US West Coast are Los Angeles/Long Beach, Seattle/Tacoma, Oakland and Portland, with LA/Long Beach dwarfing the other three. Recent events on the West Coast—the longshoreman's strike, Union Pacific trackage problems, noise and environmental concerns, limitations of the Alameda corridor—all highlight the vulnerability of that port. Further, any disaster, including terror attacks, will hypothetically shut down the port. As a consequence, a number of companies are developing backup plans utilizing other ports. Some companies are moving their business to less busy ports; others are now splitting their cargo between ports.

A number of companies are looking to the west coast Mexican ports for relief. The three principal west coast Mexican ports are Ensenada, Manzanillo and Lazaro Cardenas. Of these, Ensenada and Manzanillo are approaching capacity. Several new ports are under construction in Baja California, and Manzanillo is beginning an expansion programme. For a variety of solid reasons, most recognize the port of Lazaro Cardenas as the most promising port in Mexico. Its key attributes are as follows:

- deepest natural port in Mexico;
- relatively undeveloped infrastructure;
- large amount of available land;
- rail access that does not move through urban areas; and
- available stable workforce.

Kansas City-based Kansas City Southern Railway, in a visionary move, acquired the largest Mexican railway, TFM, and completed that transaction in 2005. The southern terminus of TFM (which is now known as Kansas City Southern de Mexico (KCSdM)), is the port of Lazaro Cardenas. This provides the unprecedented ability to land cargo at this Mexican port and carry it on KCSdM all the way to the centre of the US—terminating in Kansas City, one of the safest points of entry/departure in the United States.

Kansas City SmartPort sets the following goals for regional logistic development:

- development and implementation of a cost-effective infrastructure that keeps pace with secure, safe, and legal trade and transportation regulations along North American trade lanes;
- maintaining and creating the secure flow of commercial vehicles, drivers, and cargo associated with movement of pre-processed, low-risk, in-bond freight transactions throughout the Kansas City region;
- policies and procedures in accordance with US Department of Homeland Security (DHS) security objectives for securing supply chains into the United States;
- enhance the capabilities of trade gateway operators, regulatory agencies, and enforcement agencies associated with the Kansas City SmartPort secure FMS; and
- establish appropriate technologies necessary to develop, deploy, demonstrate and evaluate an inland port of entry (POE).

In the request for proposal (RFP), Kansas City SmartPort defined their situation and goals as follows:

> The Kansas City SmartPort Intelligent Transportation Systems (ITS) project is a key component of the Kansas City metropolitan area freight transportation and international trade strategy. The primary partners for this project are Kansas City SmartPort, the Mid-America Regional Council (MARC), the Missouri Department of Transportation (MoDOT) and the Kansas Department of Transportation (KDOT).

This project will rely heavily on advanced technology strategies to improve the operational efficiency of existing freight transportation infrastructure. It will integrate recent developments in Kansas City's Intelligent Transportation Systems (ITS) architecture with corridor-wide ITS/CVO initiatives and state and international trade compliance initiatives. Finally, it will advance strategic trade, transportation and security goals of the Kansas City region, of the I-35, I-29 and US-71 high priority highway corridors, the rail corridors and of the Federal Highway Administration (FHWA).

More specifically, this deliverable is designed to identify specific freight and commercial transportation processing functions, operational processes and ITS technologies. When combined, these processes and technologies will be capable of creating a secure "trade lane" for handling pre-processed, in-bond freight transactions across North America. This concept, known as the secure freight management system (secure FMS) embodies the following elements:

- a cost-effective infrastructure that keeps pace with secure, safe and legal trade and transportation regulations along North American trade lanes;
- the secure flow of commercial vehicles, drivers, and cargo associated with movement of preprocessed, low-risk, in-bond freight transactions throughout the Kansas City region;
- US Department of Homeland Security (DHS) security objectives for securing supply chains into the United States;
- enhanced capabilities of trade gateway operators, regulatory agencies, and enforcement agencies associated with the KC SmartPort secure FMS; and
- appropriate technologies necessary to develop, deploy, demonstrate, and evaluate an inland POE.

In effect, the proposed secure FMS will create secure and efficient "trade lanes" for moving pre-processed, low-risk, in-bond freight transactions without significant infrastructure additions or civil modifications. The key to the KC SmartPort system architecture is the integration of existing sensors, information systems, the associated databases, and a secure FMS network to support information sharing.

6.2 System's Features and Attributes

6.2.1 Developing the Secure Trade Lane

One of SmartPort's goals in defining its role in both international commerce and domestic distribution is the ability to offer differentiating services. SmartPort understands the reality that a natural trade corridor, running through Kansas City exists and continues to grow. The provisions of the North American Free Trade Agreement (NAFTA) facilitate international trade with Mexico and Canada. Local transportation, warehousing and logistics infrastructure are capitalizing on the central location of Kansas City and are attracting other related investment.

SmartPort recognizes that the changing landscape offers both opportunity and challenges. While tasked with increasing the role of Kansas City as a trade and transportation centre, SmartPort also recognizes the need to effectively manage the associated risk. SmartPort has embarked on an ambitious, funded project to develop the infrastructure needed to support several specific trade lanes.

At this time, SmartPort has basically completed the trade lane architecture study and high level requirements. SmartPort is currently running live operational tracking and tracing tests for the planned opening of the Mexican

Customs office, demonstrating cargo risk management and transportation information integration on Mexico-bound, in-bond cargo.

6.2.2 Compatibility with Existing and Developing Freight Systems

The Kansas City SmartPort ITS System Architecture and Concept of Operations task is intended to establish the System Architecture functional performance characteristics achieved by deploying applicable technologies in the Kansas City region. To date, a number of other related freight processing projects have been developed or are in the planning process both here and around the country. Therefore, compatibility to the extent possible with these systems is important. These projects currently include the following systems:

- free and secure trade (FAST) programme;
- Customs-Trade Partnership Against Terrorism (C-TPAT);
- automated commercial environment (ACE) programme; and
- commercial vehicle information systems and networks (CVISN) programme.

A significant Kansas City SmartPort objective is to establish international rail and truck corridors from SmartPort to the borders with Mexico and Canada. A key function will be the capability to process freight at SmartPort for movement with minimal delay and processing at the border. Two of the six objectives established in the RFP issued by Kansas City SmartPort for the international corridor integration project (ICIP) are pertinent to the operational testing. They are:

- analyse and develop a service delivery model that includes the development of security profiles, storage capacity, transportation routes, intermodal locations, technology and infrastructure needed to track and secure container moving from point to point on the corridor; and
- assess customs and legal constraints, coordinate green lane arrangements and develop the economic model for the project and conduct a series of operational tests on the corridor between Kansas City and Mexico with specific attention placed on freight cleared by the Mexican Customs facility in Kansas City destined for markets in Mexico on rail and truck.

The next phase of the global trade system will be implemented in 2007 at Kansas City SmartPort. The goal of this implementation will be to begin development of foundational components of the TDE. A governance process must be developed and the TDE must begin operation, achieving the requirements and goals of SmartPort. To understand the global trade system, an understanding of SmartPort is helpful.

6.2.3 Integrated Transportation Information

SmartPort users have indicated the industry's need for visibility into freight and cargo movements. SmartPort stakeholders complain of intermodal "black holes" when freight changes hands across modes and carriers. Visibility will only be possible through the integration of carrier, shipper, broker, importer, exporter and forwarder information.

Currently EDS is demonstrating that it is possible to integrate disparate transportation information. The SmartPort ITS architecture will play a vital role in laying the foundation for large-scale information integration and needs to continue to be adapted to allow for information to be provided quickly and easily to SmartPort stakeholders. A broader information net needs to be set to capture the information necessary to remove "black holes". The natural by-product of increased ITS integration is improved operations efficiencies and ultimately increased security.

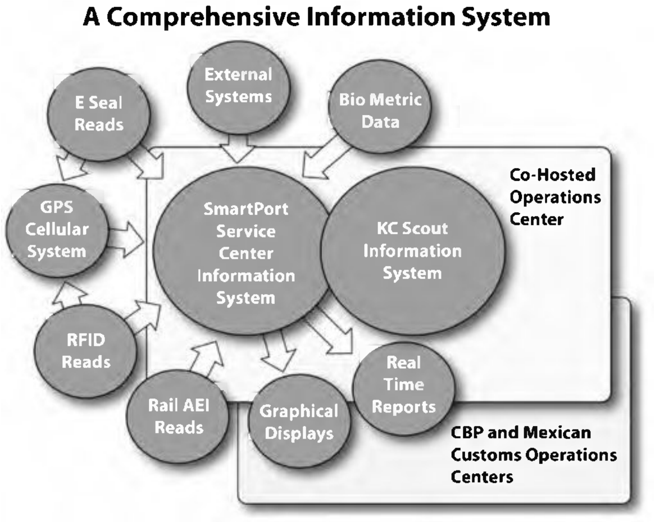

A Comprehensive Information System
E Seal Reads
External Systems
Bio Metric Data
GPS Cellular System
SmartPort Service Center Information System
KC Scout Information System
Co-Hosted Operations Center
RFID Reads
Rail AEI Reads
Graphical Displays
Real Time Reports
CBP and Mexican Customs Operations Centers

Figure 2: SmartPort Conceptual Architecture

6.2.4 Risk Management and Security

Regardless of the port of entry, the volume of cargo coming from Third World exporting countries challenges the US Customs and Border Patrol (CBP). The risk associated with this stream of cargo is not insignificant, and those who would like to harm the US do not appear to be resting. Likewise, it is not reasonable to hand-search each of these in-bound cargo containers.

Beginning with the Operation Safe Commerce project, it became apparent that the multi-modal solution to the problem is based on the application of effective sealing, sensing and tracking technologies coupled with data-driven risk management. The sensing envisioned is complementary to and compatible with SensorNet capabilities. With this in mind, we see a significant opportunity to participate in the development of this risk management model for freight moving in-bound to and out-bound from Kansas City.

Traffic through the Kansas City area will naturally increase with the flow of goods from Asia. In the initial deployment, we look to implement sensors along the KCS line from Lazaro Cardenas to Kansas City and on the BNSF line from Seattle/Tacoma to Kansas City. This will give us a real-time profile of the rail cars and associated cargo as it approaches its Kansas City destination. Looking beyond this deployment, we would like to then begin the process earlier, as the containers are loaded onto the US-bound ships.

Long term, we believe that this project could set the standard for international trade data risk management and result in an even broader deployment of sensors. To meet the needs of Kansas City SmartPort, a solution was developed using the global trade system concepts.

6.3 Phase Implementation and Outlook

The start-up phase is being initiated across multiple global locations. As of January 2007, three projects are in multiple stages of development. Kansas City SmartPort is funded and initial operation is expected during the last half of 2007. A second United States city has shown interest in joining the SmartPort community. A country is initiating a study to develop a solution for their nation.

The Kansas City SmartPort will begin by moving shipments from Kansas City to Mexico. During the prototype phase, economic advantages were identified for Kansas City manufacturers. These economic advantages will be put into play during the initial operation phase of the project. The economic advantages were found in areas of more predictable shipping times, greater accountability by stakeholders in the shipments, and greater coordination between the stakeholder communities. The community financial benefits over a 10-year period from the Kansas City SmartPort implementation has been estimated to be:

- operational savings for logistics stakeholders of $166 million to $227 million;
- increase in gross regional product of $870 million;
- creation of 9,200 new full-time equivalent jobs;
- increase in personal income of $482 million; and
- increase in state and local revenue of $90 million.

A second United States city has shown interest in joining the SmartPort community. This community will be integrated into the SmartPort solution. The objective of the community is to make local business more efficient exporters and regional development. Initial studies are anticipated in 2007.

A particular nation has shown interest in reworking their approach to freight. The country initially mandated a nationwide solution which affected industry adversely, imposing a significant burden to interface with the government system. This approach resulted in untracked cargo sitting on the export docks during the Christmas season. In this case, the government and private sector will work together to establish and implement the requirements using the TDE as their mutual conduit.

Multiple logistics communities (nodes) will be added to the other nodes. As additional ports, communities and countries are added, a structured process will be applied to define the financial benefit for each participant. All nodes will be added to a common data backbone. Each node increases the value of the other nodes. The more nodes that join the network, the greater the value of the entire network to the participants. As the number of nodes increase on the network, value is created for participating municipal communities, nations and member businesses because information flows more smoothly between the nodes so efficiencies are created and all stakeholders benefit.

6.4 Global Build-out Schedule

Total build out is expected to progress similarly to the global development of the credit card industry. The US credit card model is very mature, while other nations are still developing. The credit card effort was started in the early 1970s. Acceptance and development is still under way in a number of nations. Global development of the credit card industry will require decades for completion before credit cards are used everywhere by all merchants.

The full global trade system in the form of TDE will take decades to complete, while the economic and security benefits are expected to be immediate for the participants who adopt the TDE. The pace of development will be driven by the number of nations, communities, and companies that participate in TDE or attempt to develop their own "proprietary" systems

Visibility of the economics of a unified global system could accelerate development based on the network effect. The network effect is defined as the resulting increased value of a product because more and more people use it. Telephones, fax machines and computer operating systems are examples. Its success is due to compatibility and conformity issues, not that the product or technology may be superior or inferior to the competition. The rule of thumb becomes: "the value of a network with *n* members is not *n* squared, but rather n times the logarithm of *n*." Their primary justification for this is the idea that not all potential connections in a network are equally valuable. For example, most people call their families a great deal more often than they call strangers in other countries, and so do not derive the full value *n* from the phone service.

As more nodes are added, the network effect creates exponential growth of a shared system that lowers cost while improving profitability and security of the global trade system.

7 CONCLUSIONS

The TDE is a real-time commercial logistics data aggregator, based on public-private partnerships and a self-regulating organization (SRO), similar to a credit card clearinghouse or stock exchange. TDE is a new system that is being implemented to modernize logistics systems so they can meet the security needs of the world's nations while improving logistics and growing global commerce.

The global trade system has experienced small incremental changes since its introduction in 2003. In this chapter we have outlined the multi-fold benefits of TDE programmes and the different mechanisms of TDE implementation, focusing in particular on the SmartPort programme in Kansas City, USA, as a case study. Other TDE implementations are being discussed with other communities and nations. Similarly, other organizations are being sought which have an interest in development of an exchange and becoming a part of the global trade system community.

REFERENCES

Kothmann, D.L., 2003, "Sharing the Gains of Globalization in the New Security Environment", *In Global Trade System: A Public/Private Partnership*, Operation Safe Commerce—Pacific Proposal.

Liebowitz, S.J. and Margolis, S.E, 1999, *Winners, Losers and Microsoft*, The Independent Institute, Oakland: CA.

Supply Chain Digest, 2005, *Kansas City SmartPort Request for Proposal*, also available at *http://www.scdigest.com/assets/newsviews/05-09-23-3.cfm*, accessed on-line in May 2006.

CHAPTER 3

DEVELOPING AND IMPLEMENTING GLOBAL INTEROPERABLE STANDARDS FOR CONTAINER SECURITY

Christoph Seidelmann

International Container Security Organization (ICSO), Brussels, Belgium

1 INTRODUCTION

Today's international trade is heavily dependent on movements of intermodal containers. Containerized shipments account for 70% by value of US international trade and account for a significant portion of international trade in other developed countries. China is heavily dependent on containers to support their export economy.

In 2005 the international freight container fleet counted as follows:

- 6,288,000 units 20-ft container;
- 6,650,000 units 40-ft container;
- 165,000 units 45-ft container; and
- 531,000 units various non-standard container.

More than 13 million ISO containers are in active circulation. This number is growing at a rate of approximately 8.5% per year. In the year 2010 there will be an estimated 27 million containers in circulation. The US alone receives 11 million loaded containers per year. The volume of container shipments into the European Union is at similar level.

Foreign trade is truly the lifeblood of the global economy. A significant event in any of the above countries would have far reaching economic consequences. A Booz Allen Hamilton war game simulation concluded that the consequences of an attack which resulted in the explosion of a dirty bomb would cost the US economy US$58 billion. This figure does not include the ripple effect on other economies that depend on US foreign trade, e.g. China. Another Brooking Institute study pegged the cost to the US economy of a nuclear device exploding at a major port at US$1 trillion. One of the assumed consequences of this incident was the shutdown of all US ports for an extended period of time and, as with the war game simulation, there would be a large ripple effect on other global economies. One would expect a similar economic impact if such an incident happened somewhere in the European Union. Intermodal transport and commerce is widely viewed as a huge, soft target for terrorism.

2 SYSTEMS APPROACH TO CONTAINER SECURITY

Container security must be regarded as a system of interconnected subsystems. Unfortunately, container security experts cannot give politicians a magic device that creates security in a way that everybody in the country feels secure and understands that their government does what is needed.

A container security system needs three main elements:

1. *Standardization*: The container transport system has achieved its current efficiency and importance in the market mainly through standardization. Standardization created the economic benefits of economy of scale and the seamless cooperation of very different parties. More than 2,000 companies own a fleet of some 13 million containers, and we may assume that more than 95% of this fleet has been built to an international standard, i.e. ISO 1496 (ISO = International Standardization Organization). All of these containers are marked with an identity code according to ISO 6456. Whoever wishes to enter the container transport system must comply with these standards, otherwise they will be forced to organize for an exceptional transport regime that is expensive and difficult to manage.
2. *Container loading by trustworthy people*: Container security needs a sub-system that ensures that only trustworthy individuals load the container with goods as described in the accompanying documents, and subsequently close and secure the door of the container.
3. *In-transit container security*: Another sub-system surveys the container on its voyage to the consignee until his authorized agent opens the door. This sub-system must monitor eventual unauthorized intrusion into the container.

3 SECURITY STANDARDS AND THEIR DISCUSSION: THE MECHANICAL SEAL

Experts and representatives from the United States have always insisted on a standard approach in container security. Soon after 9/11, the US asked for seals on containers: all containers moving towards the US must be sealed, and the seal shall be designed according to international standards.

This request had a very reasonable background. The Customs Convention for Containers, Geneva 1972, contained some paragraphs about sealing within the function “container transport under customs seal”. These articles foresaw a seal designed and or approved by the national Customs administration that organizes its use. In consequence, there are worldwide some 10,000 different design species of a customs seal in application. A meaningful security system cannot rely on such diversity.

The problem with the standard mechanical seal was that at that time no standard was available. International Standardization Organization Technical Committee 104 just had not worked on that issue. However, when the request of the US for a standard seal came out, immediately such a standard was discussed and elaborated and finally agreed on. This international standard on container seals has been meanwhile published as Draft International Standard DIS 17712 Freight containers—Mechanical Seals. This standard describes three types of mechanical seals:

- high security seal;
- security seal; and
- indicative seal.

An annex adds examples and guidelines for best practices. It contains, e.g. regulations on how to ensure that standard seals for security will be only delivered to authorized parties, that used seals will be destroyed, and that producers and traders of such seals take care of their stock.

This document is agreed on by the parties concerned, so we can expect that it will soon become an ISO standard as ISO 17712.

> The security seal primarily serves as a tamper indication device, which offers a reliable indication of an unauthorized removal or attempted removal of the security seal. In addition, by virtue of its construction, the security seal provides limited resistance to an intentional or unintentional physical attack. Increased container security provides deterrents against terrorism and enhances international trade.

The public administration and the customs officers mainly rely on the high security seal. This seal can only be removed or destroyed or opened with specific tools. People working at a terminal having access to such tools can be normally identified. Such tools are normally a size such that they cannot be easily hidden by a person.

3.1 Container End Door Design

A simple seal fixed to the end door locking device can only produce high security if the design of the door is enhanced to ensure that the complete door arrangement cannot be easily removed. “ISO TC 104 Freight containers” has worked on the design of the container doors and its bolts and hinges to improve security features. This stronger door design is now included in “ISO 1496 Freight containers—Specification and Testing”, the base standard on the technical design of all containers:

> International Standard ISO 1496–1.1990/DAmd 5: 2006 “Series 1 freight containers —Specification and testing—Part 1 General cargo containers for general purposes —Amendment 5 Door end security”.

3.2 Electronic Seals

Since 1999, a specific taskforce in ISO TC 104 has been discussing various approaches to an electronic seal.

Some basic principles have been agreed on: the standard electronic seal will be an attachment device fixed to (or integrated into) the mechanical seal that secures the door of the container. The seal is programmed with a standardized set of data with the following coded information:

- the identity number of the seal manufacturer;
- a unique current number that the manufacturer of the seal has attributed to this seal;
- an indication of the time when the seal had been closed and when it had been opened; and
- a bit that indicates an eventual tampering of the seal.

Meanwhile the parties have agreed on the concept of such an electronic seal and finalized a draft that was submitted for vote as a Final Draft International Standard.

The partners involved in that process—mainly container ocean carriers, terminal operators and vendors of electronic equipment—discovered in these lengthy debates that a solution covering all these functions is yet not available. One major item is the fact that only very few radio frequencies are allowed for commercial use all over the world—and those that are allowed show some shortcomings in application.

The current draft described an electronic seal that operates on two important frequency bands, the 433 MHz and 2450 MHz bands. But one major technology provider has produced a study on the technology used in the standard. The conclusion of the report is that the current technique includes shortcomings that might become a severe problem with future practical application. In consequence, standardization work will continue to define technical solutions for an electronic seal for the future.

- ISO FDIS 18185-1 Freight containers—Electronic seals—Part 1: Radio-frequency communication protocol.
- ISO FDIS 18185-2 Freight containers—Electronic seals—Part 2: Application requirements.
- ISO 18185-3 Freight containers—Electronic seals—Part 3: Environmental characteristics.
- ISO FDIS 18185-4 Freight containers—Electronic seals—Part 4: Data protection.
- ISO FDIS 18185-7 Freight containers—Electronic seals—Part 7: Physical layer.

3.3 Container Identity

Information of the seal number and seal integrity makes sense only if, simultaneously, the identity number of the container, on which the seal has been fixed, is checked and compared to the data given in the documentation of this transport. If the seal number and status is identified by electronic means, it will be more desirable to act similarly with the container identity reading.

Various technologies exist for such services, and various solutions compete with each other. The debate about the optimum system for electronic container identification has been conducted since the very start of the standardization activity.

The basic problem is that an electronic seal will be designed as a one-trip device; it must not last longer than one container voyage, i.e. some eight weeks maximum. Such seals can be easily fitted with batteries, because batteries with an operational lifetime of eight weeks are easily obtained. So, the electronic seal will most certainly be a battery-mounted piece of equipment. However, permanent container identity data needs an electronic device that lasts as long as the container, i.e. some 15–20 years. The best battery solution that is available at a reasonable price provides energy for 8–10 years.

A non-battery mounted transponder has an almost unlimited lifetime, but needs a high-energy radio signal from the interrogator. US legislation allows for such signals, most European legislation does not. According to European legislation a radio signal to interrogate a non-battery mounted transponder on a container will have a maximum reading range of some 2–3 metres, and this distance is rather short compared to the desires of the terminal operators.

Finally, the industry must go one way or the other. It must decide on a non-battery device with limited performance, or a battery device that covers most needs of container and terminal operators. Possibly, the following solution will be applied: fix a cheap non-battery transponder on the container that can be used in all applications where a 3-metre reading range can be operationally achieved. Such a transponder should be rather cheap so that this spending can be justified even when its use is limited to certain cases.

Those who wish may add a battery-mounted transponder or container security device for identity check, seal integrity check and, possibly, whatever function is required.

3.4 Standards on Container Security Devices

The US authorities have announced that there will eventually be an increased role for container security devices. These are battery-mounted intelligent small devices, to be fitted easily inside the container (with a small antenna outside). These devices will store the container number and date and time of each door opening together with a record of the communication between an outside reader and the device.

Various companies and manufacturers, mainly in the security industry, have presented concepts of such devices, and some solutions to industrial production will soon be available.

The users—mainly shippers and forwarders—and the other actors in the security chain—mainly port terminals and customs administrations—have insisted on an interoperable approach. They do not wish to install multiple RF access points for container security devices from different producers. The

International Container Security Organization has taken this challenge and started to work on such standards. First drafts have been finalized, but not yet published. ICSO will wait for the US administration to come out with their requirements. As far as possible, a set of container security device standards shall comply with such requirements.

4 CONCLUSIONS: OUTLOOK AND FURTHER STANDARDIZATION

Container security will, eventually, be a most complex system of interrelated activities in information, data capture, controlled re-distribution and physical surveillance of the container, and inquiries into the various actors in the supply chain. Standardization will be an important tool in streamlining these activities and to set certain benchmarks in the desired quality level of security. However, on the other hand, a published standard may serve for the people on the other side as a valuable guideline for their dark activities. Before starting a standardization process the parties must take this into account and decide on privacy or on the participation of a wider public in the work.

PART II

SYSTEMS FOR ENHANCING PORT SECURITY AND OPERATIONAL EFFICIENCY

This page intentionally left blank

CHAPTER 4

PLANNING AND IMPLEMENTING RFID TECHNOLOGIES TO ENHANCE SECURITY IN PORT OPERATIONS

Giovanni Luca Barletta and Khalid Bichou

Port Operations Research and Technology Centre (PORTeC), Centre for Transport Studies, Imperial College London, London SW7 2BU, UK

Abstract
After the 9/11 events, governments and industries have recognized the need to secure both infrastructures and cargo movements within ports. With the introduction of many initiatives aiming at enhancing port and sea trade security (CSI, SST, C-TPAT, 24-hour rule), electronic container seals and RFID systems have taken the lead over other technologies. However, beyond the general advantages brought about by these technologies, there is a need to reflect on the extent to which they can enhance port operations, both in terms of risk reduction and efficiency improvements. This study investigates how port operations can be enhanced by the use of RFID technology and presents a functional model of the "RFID-enhanced" port model, based on IDEF0 modelling tools. In particular, we examine the role of RFID to secure yard operations, and highlight technological issues and other potential problems incurred when adopting and implementing such technology.

1 INTRODUCTION AND LITERATURE REVIEW

Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object using radio waves. It is grouped under the broad category of automatic identification technologies. RFID is designed to enable readers to capture data on tags and transmit it automatically to a computer system. A typical RFID tag consists of a microchip attached to a radio antenna mounted on a substrate. A reader is used to retrieve the data stored on an RFID tag. A typical reader (which can be either fixed or mobile) is a device that has one or more antennas that emit radio waves and receive signals back from the tag. The reader then passes the information in digital form to a computer system (through the middleware). Middleware is a generic term used to describe software that resides between the RFID reader and applications. It is a critical component of any RFID system, because the middleware takes the raw data from the reader—a reader might read the same tag 100 times per second—filters it and passes on the useful event data to back-end systems. Middleware plays a key role in getting the right information to the right application at the right time (Palival *et al.*, 2004).

1.1 Terminology

Although a full discussion of all the types and capabilities of RFID is beyond the scope of this chapter, in the next section there will be a basic understanding of the types of RFID systems available.

The main types of RFID tags that are of primary interest are active, semiactive and passive. Active RFID tags contain a battery to boost reading range. Active tags can have a range up to 100 metres (depending on the power allowed in different countries' regulations). These tags have a large memory capacity to store relevant data (up to 32Kb) that is typically encrypted to prevent unauthorized reading. Active tags may contain sensors, global positioning system (GPS) devices (to be tracked on during all the transportation process), satellite links, or other enhancements.

Semi-active RFID tags contain a battery but this is not used to enhance reading range. The battery is used to power sensors or volatile memory. Read range depends on the frequency and type of tag. Also of interest are RFID identification cards (passive RFID), which can be regarded as contactless smart cards. These are passive since they contain no battery and have a more limited range (up to 2–3 metres). Passive RFID tags may also be found on pallets and other load devices within shipping containers (Politecnico di Milano, 2005).

1.2 RFID in Port Operations

While much of the attention in the literature and in industry has been focused on the role of RFID in retail logistics, there is a much wider range of applications of RFID than the current generation of disposable tags. RFID has been successfully used in transportation and manufacturing since the mid-1980s and its use is growing rapidly as costs have come down and benefits have been recognized (Brewer *et al.*, 1999; Ni *et al.*, 2004).

The primary advantage of RFID in a port/terminal application is that it is an "automatic" data collection technology. That is, no operator intervention or action is required (with the exception of the overall control of the system). Whereas other forms of data collection, whether bar code or manual methods, depend on employees to record information, RFID relieves them from this time-consuming and error-prone process. The two direct benefits of this are:

- accurate and complete data collection; and
- better utilization of employees' time.

In addition, security measures, as will be argued later in this chapter, can be significantly enhanced through the use of RFID.

There are five major areas where RFID can be used effectively in a port cargo terminal:

- access control;
- container security;
- container identification and location;
- activity tracking; and
- regulatory compliance.

Some of these applications offer benefits to the terminal/port operator, either directly or as added services for shippers. Other benefits must be seen more as means of simplifying compliance with increasing governmental security regulations and record-keeping requirements. While many of the applications will require the cooperation of shipowners, shippers, carriers and terminal operators in employing RFID and may, therefore, seem to be excessively forward-looking, the regulatory environment will likely encourage adoption in a much shorter timeframe than might be evident at this moment.

1.2.1 Access Control

In addition to helping comply with security measures like the International Maritime Organization (IMO) ISPS Code, ensuring that only authorized personnel are admitted to the terminal area is necessary to prevent loss and possible mischief.

RFID employee identification badges can provide automated time and attendance and can also be used to associate an employee with a particular piece of equipment. Employee identity can be used to ensure that an employee is qualified to operate a certain piece of equipment or enter a certain area. In many cases security or operations personnel can be relieved of these duties because the RFID badge will contain the necessary clearances or permissions. In an increasing number of applications, RFID badges also function as stored value cards, allowing workers to make purchases within the workplace without the need to carry cash (Politecnico di Milano, 2005).

1.2.2 Container Security

A great deal of attention is being focused on a new generation of "smart seals" to ensure the integrity of a container and its contents. Whereas conventional security seals will provide evidence of tampering, they require visual inspection to do so. Evidence of tampering is usually discovered long after the fact and offers little benefit other than proof of loss. RFID seals, on the other hand, can alert terminal personnel at the time of tampering (Chin and Wu, 2004; Stowsky, 2005). Smart seals are active RFID tags and will broadcast the fact that they have been opened or removed without authorization.

Typically, these tags would be purchased and affixed by the shipper. However, terminals must be equipped to receive signals from these tags if they are to be effective. Smart tags can also be equipped with sensors to monitor environmental conditions within the container. Some tags, such as those used by the US military on high security containers, also contain GPS, sensors (Bruckner *et al.*, 2003) and satellite phone capabilities to constantly report the location of the container and the conditions within it. For perishable, sensitive, or high value cargos this type of tag offers the highest level of security. These tags, and the satellite phone portals, are available to commercial shippers. Because they can report breaches to the shipment owner directly, terminals do not need to make special accommodations for them.

1.2.3 Vehicle Control

Equipping tractors and other equipment with RFID tags is becoming increasingly common in fleet and yard management operations. Readers placed at fuelling stations, gates and other access points can be used to enable access or egress as well as to record the exact time at which a particular truck and container entered or left the terminal. RFID employee badges can be used to validate that the right driver has the right vehicle and load. Tags on vehicles or RFID badges can be used to unlock fuel pumps and record fuel usage. We are going to talk more about this issue later on this section.

1.2.4 Container Identification and Location

While there has been an International Organization for Standardisation (ISO) standard for tagging of maritime containers for a number of years, few container owners have implemented tagging. Primarily, this is because the costs of tags was initially very high. A new generation of active tags, however, has brought the cost down considerably, making it more feasible to tag the tens of thousands of containers in use. Thus, ISO has recently started the process for a standard dedicated to the new freight container electronic seals (ISO 2005).

A continuing problem with intermodal containers is the presence of multiple identification numbers on many containers (Hayashi *et al.*, 2003). There may be one number on the side and another number on the end—and terminal operators have little guidance as to which is correct. The increased concerns over the possible use of maritime shipping containers as a means of entry for illegal immigration, weapons and chemical or biological agents means that positive identification of each container, under Smart and Secure Trade-lanes (SST) and Container Security Initiative (CSI) compliance, is likely to increase (Banomyong, 2005). RFID tags can provide a secure answer to this requirement. Readers placed on gantries and yard vehicles will be able to automatically record the identity of each container as it is offloaded and transported within the terminal.

This is the reason why the "Smart Box", which is a device made by combining active RFID and sensors in order to detect unauthorized openings, changes in temperature and weight has been mentioned by several consultants to the US Homeland Security Department and by US Border and Custom Protection, as a useful mean in SST and Customs Trade Partnership Against Terrorism (C-TPAT) compliance.

1.2.5 Location Tracking

Even with sophisticated management software containers are not always placed where they should be. RFID tags can be buried at regular intervals in the aisles to serve as location markers. These tags can be read by RFID readers in fixed locations and provide information on the exact location of the container and the vehicle. These readers could also capture the ID of the container being transported. Communicated to the office via a wireless local area network (LAN), the location of any vehicle or container can be automatically recorded and displayed (Hayashi, 2003).

1.2.6 Activity Tracking

Productivity is an issue that is of concern not only to terminal operators but to the shipowners, shippers and consignees as well. Ensuring the most efficient loading and offloading of container ships is critical to profitability. Certainly time spent looking for containers that have not been placed where they should have been can cause losses of time and, in the case of perishable goods, may result in the loss of the entire or part of the shipment. The use of RFID tags to record the location of containers and monitor the location and activities of yard vehicles could improve the overall quality of data and, therefore, the efficiency of the operations. In addition, it will enable collection of detailed data that may uncover inefficiencies in established procedures that could not previously be identified (such as biometric data).

RFID provides the ability to automatically collect real-time data without burdening employees. This provides managers with an up-to-the-minute picture of activities and that, in turn, allows them to respond to developing situations in a timely manner.

1.2.7 The Architecture

The architecture of an RFID system for yard management can be graphically shown as follows:

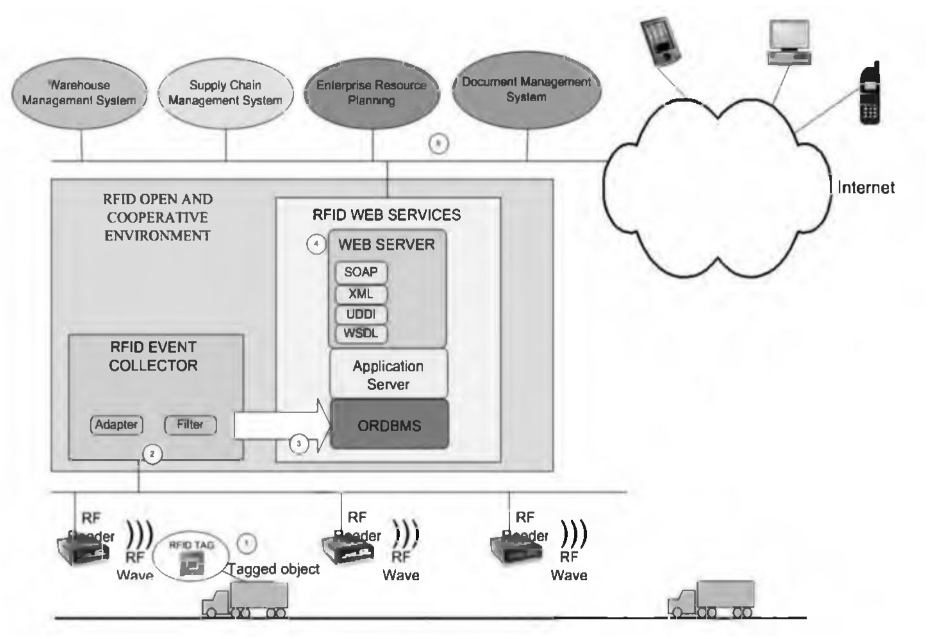


Figure 1: RFID Architecture

It is possible to define a three-tier architecture:

- *physical layer*: links between objects (containers or trucks) and readers (fixed or mobile);
- *communication layer*: transfer of information from readers to the information system; and
- *application layer*: interface between applications (both internal and external to the port system) and information system.

The *physical layer* is given by the RFID infrastructure itself. The information exchange between tags and readers gives two types of information:

- identification and state of container; and
- localization.

The information captured by the physical layer is managed by the communication layer, which is typically given by a wireless LAN linking the readers with the servers of the information system.

Once the information arrives from readers, the middleware takes charge of filtering signals (giving priority and identifying the single item) and then passes the information to the data base management system (DBMS, or, if object-oriented as in this case ORDBMS). The DBMS is in charge of managing all information and, through the web, is allowed to interface the application layer both within and outside the local system (Leaver, 2004).

2 RFID AND REGULATORY COMPLIANCE

2.1 Main Container and Maritime Security Measures

We analyse here the main features of the major international security initiatives other than ISPS. It must be said that these initiative are all supervised and enforced by the US government.

From the US SST and CSI initiatives to the EU food tracking mandates, more and more burdens are being placed on every link in the supply chain to record the movement of goods from the point of origin to the point of consumption. The use of automatic identification and data collection (AIDC) technologies, including bar codes and RFID, will permit companies within the supply chain to efficiently cope with these data collection regulations. With the US SST and CSI regulations, there are increasing burdens on suppliers and terminals to ensure the integrity of containers once they have been inspected. The use of RFID technology for employee ID badges, access control, security seals and terminal operation will provide assurances that container integrity has been maintained. Containers that can meet all these requirements will be "fast tracked" on arrival in the US, allowing them to be moved out of the terminal faster (US Customs, 2004).

While there is currently no mandate for RFID in any of the current regulations (even if in SST it is strongly recommended), there is every indication that it will be recognized within a few years as a means of compliance.

2.1.1 CSI

CSI addresses the threat to border security and global trade that is posed by potential terrorist use of a maritime container to deliver a weapon. CSI uses a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the US.

The four core elements of CSI are to:

- identify high-risk containers: CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence;
- pre-screen and evaluate containers before they are shipped: containers are screened as early in the supply chain as possible, generally at the port of departure;
- use technology to pre-screen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade: this technology includes large-scale x-ray and gamma ray machines and radiation detection devices; and
- use smarter, more secure containers: these will allow CBP officers at United States ports of arrival to identify containers that have been tampered with during transit.

2.1.2 SST

The goals of SST include:

- implementing baseline capability in container security and tracking consistent with government requirements of Operation Safe Commerce and Customs;
- coverage of the global networks of the top three global port operators (Hutchison, PSA, P&O);
- participation by key multinational shippers;
- ensuring no reduction inefficiency for supply-chain participants and that any solution is economically viable; and
- supporting and aid of policy and legislation through continuous dialogue with government agencies.

SST works with CSI Task Force domestically and internationally (HK and Singapore).

2.1.3 24-Hour Rule

On 2 February 2003 the US Customs Service began enforcing new regulations requiring carriers to provide the US Customs with the vessel's cargo manifest (cargo declaration) at the latest 24 hours before loading at a foreign port, cargo destined for the US or passing through US ports in transit. It is important to note that the regulations do not apply to bulk cargoes. In the case of break-bulk cargoes an exemption may be available.

The so-called "24-hour rule" has been implemented to try to help the US Customs evaluate the risk of smuggled weapons of mass destruction before the goods are loaded on vessels for importation in the US while, at the same time, enabling the US Customs to facilitate the prompt release of legitimate cargo following its arrival in the US. In all circumstances, the cargo declaration must be submitted to the US Customs at least 24 hours in advance of loading.

Failure to provide the required information within 24 hours prior to loading may result in the delay of a permit being issued to discharge the cargo in the US and/or the assessment of penalties or claims for liquidated damages levied on the carrier by the US Customs.

2.1.4 MARSEC 2

Some of the main features of ISPS heightened security level (MARSEC 2) related to cargo handling and monitoring of port security are summarized below (IMO 2003):

- detailed checking of cargo, cargo transport units and cargo spaces;
- intensified checks to ensure that only the intended cargo is loaded;
- intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships and increased frequency and detail in checking of seals

or other methods used to prevent tampering by increasing the frequency and detail of visual and physical examination, increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs and/or coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures;

- enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion detection devices;
- detailed checking of cargo, cargo transport units and cargo storage areas within the port facility;
- intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship; and
- intensified searches of vehicles and increased frequency and detail in checking of seals and other methods used to prevent tampering.

2.2 Synoptic View of RFID Features

Table 1 shows a view of RFID features in the main maritime security initiatives. Three combinations of requirements and feature availability in RFID technologies were identified: features required by the initiative and featured by means of RFID; features not required by the initiative but featured by RFID; and features required by the initiative but not featured by RFID.

Noticeably, almost all the requirements are met by RFID. The only feature which is not granted by RFID is container inspection, which a fundamental issue, although far beyond RFID capabilities. CSI and SST refer directly to the port environment and therefore RFID can be more widely used. The 24-hour rule, on the other hand, is more related to information issues and relates to the origin port of loading. In order to comply with this last rule, in fact, RFID is placed onto the container, constituting the so-called e-seal.

RFID ensures compliance with many aspects of MARSEC 2, avoiding heightening the security level from MARSEC 1 to MARSEC 2. This feature means that it is possible to avoid the extra cost of passing from one level to the other. This cost is relevant. An estimate of US Coast Guard (USCG) reveals that passing twice a year for six weeks in total from MARSEC 1 to MARSEC 2 will cost the 361 American ports a total of US$241 million. Roughly calculating the cost of adopting RFID for yard management it is possible to estimate a cost per port of US$150,000, which is, of course, very much influenced by the size of the port and of the area to be covered. An estimate of these costs is shown below:

- middleware (open source—up to US$60,000)
- reader <US$50,000

- tag <US$5,000
- gate US$10,000–50,000
- total cost <US$150,000

Therefore, if we hypothesize a massive adoption of RFID in all American ports, we can calculate a total investment of US$150,000 × 361 = US$54 million, which constitutes a fixed cost, not including the labour costs (included in USCG estimate). The only feature which is not allowed by the use of RFID is the inspection of cargoes (performed by means of physical inspection and x or gamma ray machines). In conclusion, it is possible to imply that, once the container has been inspected, it is possible to comply with the main requirements of security initiatives by means of RFID and, moreover, to perform other activities (like vehicle localization).

Features required	*Security initiatives*		
	CSI	SST	24-Hour rule
Container identification	⋆	⋆	⋆
Container inspection	●	●	●
Container localization	⋆	⋆	○
Container status monitoring	⋆	⋆	○
Vehicle localization	○	○	○

Table 1: Synoptic View of RFID Feature in Maritime Security Initiatives

⋆ = Feature required by the initiative and featured by RFID
○ = Feature not required by the initiative but featured by RFID
● = Feature required by the initiative but not featured by RFID

3 USE OF RFID IN YARD MANAGEMENT OPERATIONS: AN IDEF0 MODEL

3.1 Introduction to IDEF0 Modelling Technique

IDEF0 has been derived from a graphical language know as structured analysis and design technique (SADT), developed by Ross and Softech (Ross, 1977). In its original form, IDEF0 includes both a definition of a graphical modelling language (syntax and semantics) and a description of a comprehensive methodology for developing models. For new systems, IDEF0 may be used first to define the requirements and specify the functions, and then to design an implementation that meets the requirements and performs the functions. For existing systems, IDEF0 can be used to analyse the functions the system performs and to record the mechanisms (means) by which these are done.

The result of applying IDEF0 to a system is a model that consists of a hierarchical series of diagrams, text and glossary cross-referenced to each other. The two primary modelling components are functions (represented on a diagram by boxes) and the data and objects that interrelate those functions (represented by arrows). IDEF0 is a modelling technique based on combined graphics and text that are presented in an organized and systematic way to gain understanding, support analysis, provide logic for potential changes, specify requirements, or support systems level design and integration activities. An IDEF0 model is composed of a hierarchical series of diagrams that gradually display increasing levels of detail describing functions and their interfaces within the context of a system. There are three types of diagrams: graphic; text; and glossary. The graphic diagrams define functions and functional relationships via box and arrow syntax and semantics. The text and glossary diagrams provide additional information in support of graphic diagrams.

In addition to definition of the IDEF0 language, the IDEF0 methodology also prescribes procedures and techniques for developing and interpreting models, including ones for data gathering, diagram construction, review cycles and documentation (for a complete review of IDEF0 method see Jorgensen (1995), Coloquhoun and Baines, 1991, Bravoco and Yadav, 1985 and Softech, 1981).

The semantics of IDEF0 boxes and arrows is shown below (Figure 2).

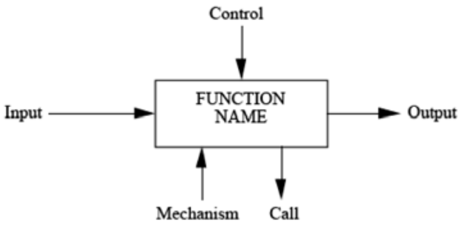


Figure 2: Semantics of IDEF0 Box and Arrows

IDEF0 models are composed of three types of information: graphic diagrams; text; and glossary. These diagram types are cross-referenced to each other. The graphic diagram is the major component of an IDEF0 model, containing boxes, arrows, box/arrow interconnections and associated relationships. Boxes represent each major function of a subject. These functions are broken down or decomposed into more detailed diagrams, until the subject is described at a level necessary to support the goals of a particular project. The top-level diagram in the model provides the most general or abstract description of the subject represented by the model. This diagram is followed by a series of child diagrams providing more detail about the subject. A decomposition structure is shown below.

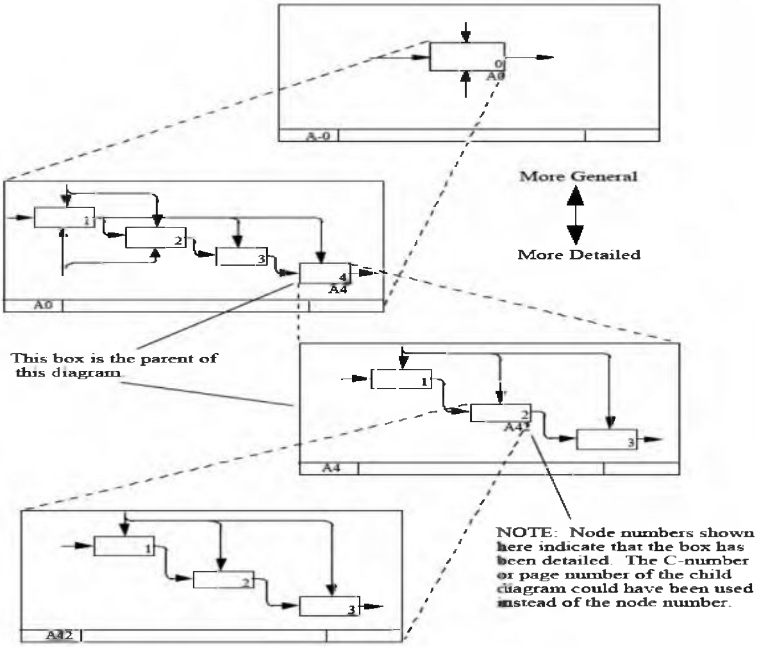

0
A0
A-0
More General
More Detailed
1
2
3
4
A4
A0
This box is the parent of this diagram
1
2
A42
3
A4
NOTE: Node numbers shown here indicate that the box has been detailed. The C-number or page number of the child diagram could have been used instead of the node number.
1
2
3
A42

Figure 3: Decomposition Structure

IDEF0 method has been created in order to analyse and model business processes in a manufacturing environment. There is in fact an extensive literature of different applications of this technique in various contexts but especially in manufacturing. Among the others, it is worth quoting the works by Cullinane *et al.*, 1997, Leong, 1999, Leong *et al.*, 1999 and Dorador and Young, 2000.

A survey of the literature has not found an attempt to use IDEF0 method for the analysis of a port system. Although there have been some models for shipping company operations (Lyridis *et al.*, 2005), for the overall shipping system (ADVANCES Project, 2004) and for port operations (Paik and Bagchi, 2000) which had used BPR techniques, the literature does not seem to include attempts to focus on the re-engineering of port and yard operations through IDEF0.

3.2 Top Level View Point

The top level view point of the model is as follows:

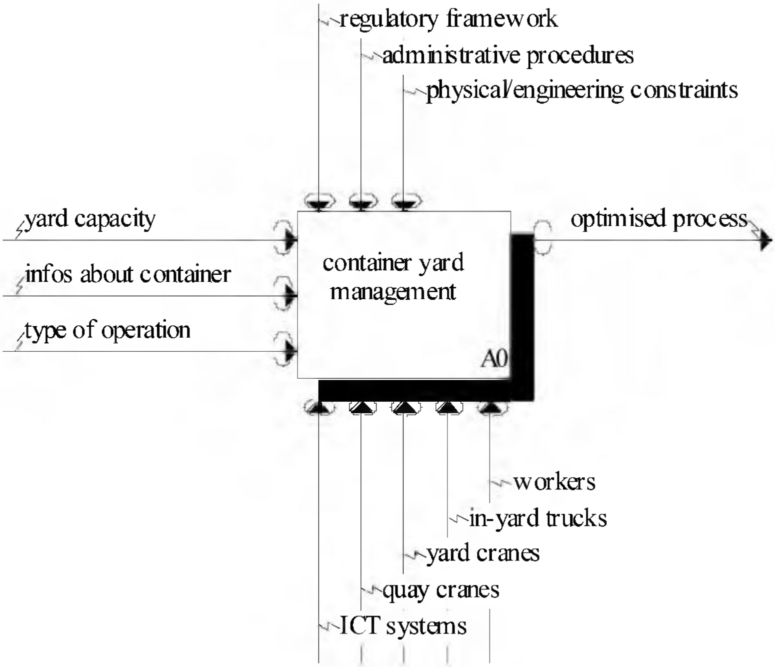


Figure 4: Top Level View

In more detail, the above is represented by the following diagram:

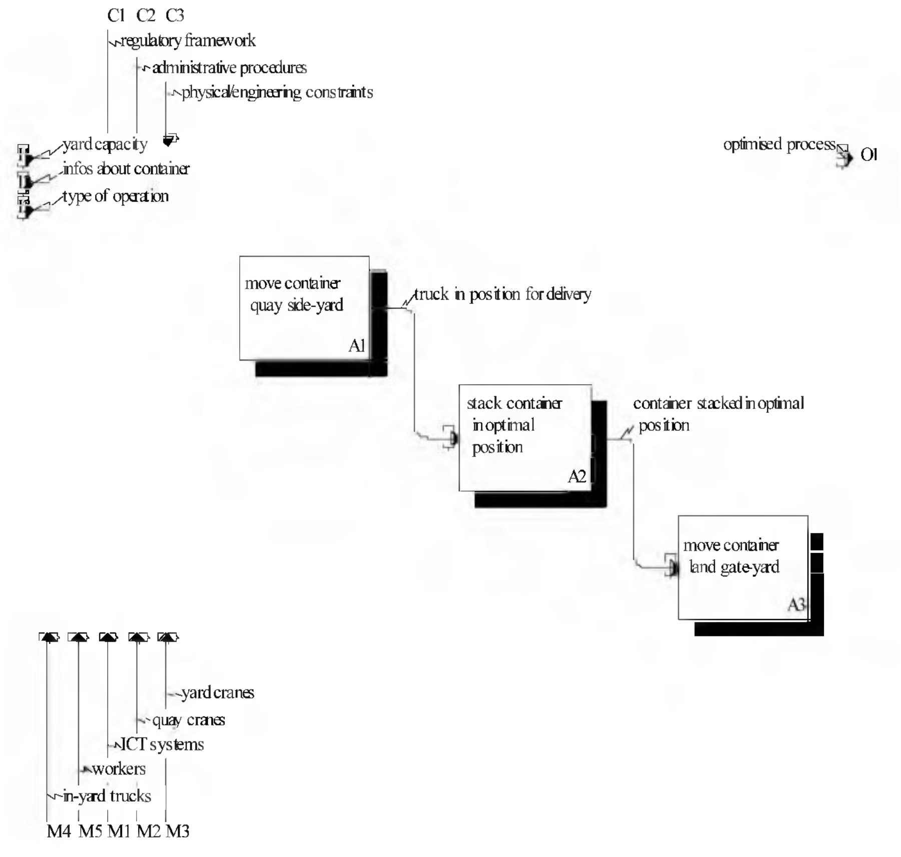

C1 C2 C3
regulatory framework
administrative procedures
physical/engineering constraints
yard capacity
infos about container
type of operation
optimised process
O1
move container quay side-yard
A1
truck in position for delivery
stack container in optimal position
A2
container stacked in optimal position
move container land gate-yard
A3
yard cranes
quay cranes
ICT systems
workers
in-yard trucks
M4 M5 M1 M2 M3

Figure 5: Container Yard Management View

3.3 IDEF0 Model for Non-RFID-Enhanced Operations

Let us state some further assumptions about the process we are now going to model:

- yard capacity, i.e. configuration: RTG;
- information about container: regular FCL;
- type of operation: import;
- regulatory framework: security level 1; and
- ICT systems: RFID *not* adopted.

Let us now go into more detail. Activity A1 is detailed in such way:

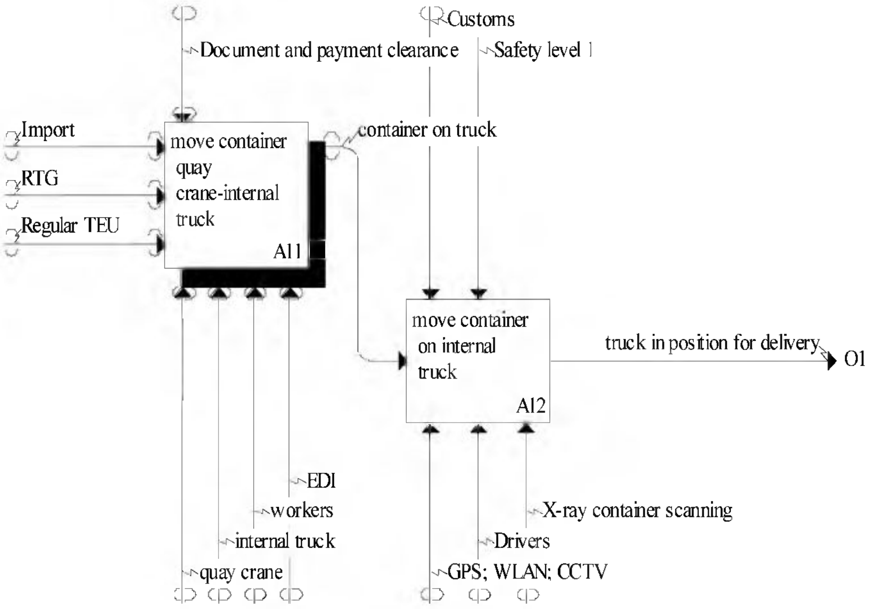


Figure 6: "Move Container QuaySide Yard" View

As we can see, one of the constraints in activity A12 is Customs. As better explained in the next section, this represents one of the main differences between the RFID and non-RFID cases. It is, in fact, a requirement for all cargoes to proceed with Customs' clearance operations and maybe inspections by Customs officers, e.g. using x-ray container scanning machinery. However, as stated in SST regulations, the use of secure and smart technologies can overcome this duty because all information needed and a real-time automated control of the state of the container are available.

When the container is on the internal truck, it is moved from the quayside to the stack yard (activity A12). At this stage, it might be subject to control by Customs. In this case, the truck must go to the Customs space and be checked. However, the percentage of containers checked by Customs is currently 2%. During the transportation of the container in the yard, according to the security level, the tracking of the truck is required. Following the assumption that RFID is not used, the main technologies used (the mechanisms of the model) are GPS (in particular the differential GPS), radio communications, and CCTV. However, it is worth noting that at this stage we are tracking the truck rather than the container, i.e. we do not know the information about the container (it is momentarily "lost") but only about the truck which is transporting it. We will note in the next section that adopting other technologies can overcome this problem.

3.4 IDEF0 Model for RFID-Enhanced Operations

As we have done in the case of non-RFID-enhanced operations, let us state some further assumptions about the process we are now going to model:

- yard capacity, i.e. configuration: RTG;
- information about container: regular FCL;
- type of operation: import;
- regulatory framework: security level 1 (theoretical, i.e. level 2 is granted by RFID); and
- ICT systems: RFID adopted.

We will show how the impact of RFID can change some of the constraints we put in the model. Some activities, however, are not going to be affected by the use of RFID technology and therefore they are going to be modelled in the same way as before. Given the high degree of flexibility of this technology, we are going to specify case-by-case in the mechanism arrows which capability of RFID is foreseen. The specification of activity A1 "move container quayside yard" is detailed in Figure 7.

It is possible to note that the mechanism "RFID" has been introduced for the sub-activity "move container on internal truck" and that the control "Customs" has been cancelled. Although the security level does not change, in fact, RFID avoids Customs inspection because all information necessary for Customs is already written on the smart tag and is readable at any point in the yard. This is the aim of many security initiatives like Smart and Secure Tradelanes, Container Security Initiative and Customs Trade Partnership Against Terrorism (C-TPAT). Information about the cargo such as origin, destination, contents and status are stored in the active RFID tag and are not likely to be altered due to different levels of cryptography. This feature can generate savings in terms of time spent for customs clearance and therefore can increase the efficiency of the operations, reducing the processing time and giving access to more secure information.

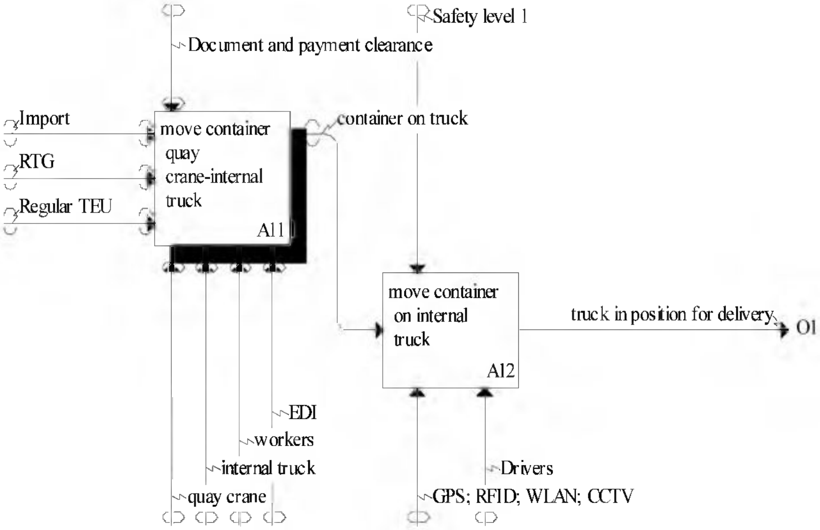

Safety level 1
Document and payment clearance
Import
RTG
Regular TEU
move container quay crane-internal truck
A11
container on truck
move container on internal truck
A12
truck in position for delivery
O1
EDI
workers
internal truck
quay crane
Drivers
GPS; RFID; WLAN; CCTV

Figure 7: “Move Container Quayside Yard” View

Another feature of active RFID tags is that it possible to use them for tracking the containers (and therefore the trucks) during their movements within the yard. Through the utilization of localization algorithms (like triangulation) it is possible to know, in a discrete way, the position of the container with a precision of almost one metre. At the same time, an active RFID tag linked to the so-called Smart Box with sensors can give real-time information about the general condition of the container and the cargo stored inside (temperature, tries of forced openings, change in weight, etc.). It is worth noting that the presence of RFID do not exclude integration with other technologies. Differential GPS for instance, is a more accurate means of localization than RFID, although the accuracy less than one metre does not affect the actual scope of localization too much. For the same reason, and to respect the regulation about security in the yard, the use of CCTV is complementary to RFID and cannot be replaced. Moreover, given that the range of transmission of RFID is around 100 metres, it is necessary to link the readers with the intranet in order have the information actually available. This is possible by linking, as nowadays featured by almost every producer although with some incompatibility of frequency, the RFID readers with a wireless LAN spot, maybe sharing the infrastructure with wireless CCTV, which has become more and more utilized in open spaces like ports.

4 CONCLUSIONS

The aim of this work was to show whether RFID technologies, which are widely used for security purposes, could enhance the efficiency of yard operations. The results were not conclusive in the absence of an appropriate cost-benefit analysis and of a sufficient number of case studies, although some significant results emerged:

- first, it has been shown that the automated compliance to security regulations allowed by RFID can avoid some operations (e.g. Customs inspections), thereby reducing the processing time and increasing the efficiency of the port;
- secondly, "automatic" compliance to level 2 of ISPS code (heightened security) is ensured by the adoption of RFID, avoiding in this way the extra cost of passing occasionally, but repeatedly, from level 1 to level 2; and
- finally, it has been shown that RFID can provide a cheaper alternative to other technologies for identification and localization purposes.

As a reflection of the limitations constraining the model, a further development of this work could be the extension of the modelling to other configurations and other environments. The analysis of the impact of RFID technologies in different yard configurations would give room to different conclusions, either in a more or less encouraging way. For instance, the application of RFID in a tractor chassis yard system seems likely to fit well with RFID characteristics. In a similar way, it would be interesting to analyse what might happen to RFID-enhanced containers during the handling process (LCL containers).

REFERENCES

ADVANCE Project (2004) *ADVANCE Project Final version*, Project funded by the European Community under the "Competitive and Sustainable Growth Programme" (1998–2002).

Bravoco, R. and Yadav, S. (1985) "A methodology to model the functional structure of an organisation", *Computers in Industry*, 6(4), 245–361.

Brewer, A., Sloan, N. and Landers, T.L. (1999) "Intelligent tracking in manufacturing", *Journal of Intelligent Manufacturing*, 10(3–4), 245–250.

Buckner, M., Crutcher, R., Moore, M.R. and Smith, S.F. (2003) "GPS and sensor-enabled RFID tags", *RFID paper No. 120*, ORNL unclassified paper.

Chin, L.P. and Wu, C.L. (2004) "The Role of Electronic Container Seal (E-Seal) with RFID Technology in the Container Security Initiatives". In: *Proceedings of the* 2004 *International Conference on MEMS, NANO and Smart Systems (ICMENS'04)*, Alberta: 25–27 August.

Colquhoun, G.J. and Baines, R.W. (1991) "A generic IDEF0 model of process planning", *International Journal of Production Research*, 29(11), 2239–2257.

Cullinane, T.P., Pratap, S., Chinnaiah, S., Wongvasu, N. and Kamarthi, S.V. (1997) "A Generic IDEFO Model of a Production System for Mass Customization", In: Proceedings of PICMET '97: Portland International Conference on Management and Technology.

Dorador, J.M. and Young R.I.M. (2000) "Application of IDEF0, IDEF3 and UML methodologies in the creation of information models", *International Journal of Computer Integrated Manufacturing*, 13(5), 430–445.

Hayashi, H., Tsubaki, T., Ogawa, T. and Shimizu M. (2003) "Asset tracking system using long-life active RFID tags", *NTT Technical Review*, 1(9), 19–26.

IMO (2003) International Ship and Port Facility Security (ISPS) Code.

ISO (2005) *Freight containers—Electronic seals—Part 7: Physical layer—ISO 18185*, Draft. Available at: *www.iso.org/iso/en/commcentre/isofocus/isoupdate/pdf/june06.pdf*.

Jorgensen, F. (1995) "Overview of Functional Modelling—IDEFO", *Information Management in Computer Integrated Manufacturing: A Comprehensive Guide to State-of-the-Art CIM Solutions* (Springer-Verlag), 340–354.

Leaver, S. (2004) "Evaluating RFID middleware", Forrester Research Inc. Available from: *www.forrester.com*.

Leong, A. (1999) "Enactment of IDEF0 models", *International Journal of Production Research*, 37 (15), 3383–3397.

Leong, A., Pheng, K.L. and Leng G.R.K. (1999) "IDEF*: a comprehensive modelling methodology for the development of manufacturing enterprise systems", *International Journal of Production Research*, 37(17), 3839–3858.

Lyridis, D.V., Fyrvik, T., Kapetanis, G.N., Ventikos, N., Anaxagorou, P., Uthaug, E. and Psaraftis H.N. (2005) "Optimizing shipping company operations using business process modelling", *Maritime Policy and Management*, 32(4), 403–420.

Ni, L., Liu, L., Lau Y.C. and Patil, A.P. (2004) "LANDMARC: Indoor Location Sensing Using Active RFID", *Wireless Networks*, 10(6), 701–710.

Paik, S. and Bagchi, P. (2000) "Process Reengineering in Port Operations: A case study", *The International Journal of Logistics Management*, 11(2), 59–72.

Palival, A., Adam, N., Bornhövd, C. and Schaper, J. (2004) "Semantic Discovery and Composition of Web Services for RFID Applications in Border Control", *3rd International Semantic Web Conference, ISWC 04*, Hiroshima, Japan, 7–11 November.

Politecnico di Milano (2005) "RFID between past and future. [RFID tra presente e futuro]", *Quaderni AIP*, Politecnico di Milano, 49–56.

Ross, D.T. (1977) "Structured Analysis: a language for communication ideas", *IEEE Transactions on Software Engineering*, 3(1), 16–34.

Softech (1981) *ICAM Architecture*, Part II, vol. II, Wright-Patterson Air Force Base.

Stowsky, J. (2005) "Harnessing a Trojan Horse: Aligning Security Investments with Commercial Trajectories in Cargo Container Shipping", Paper Prepared for the Public Policy Institute of California (PPIC) project on port security. Available from: *http://brie.berkeley.edu/~briewww/publications/stowsky%20port%20security.pdf*.

US Customs (2004) *Securing the Global Supply Chain*. US Customs and Border Protection. November 2004. Available from: *http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategic plan.ctt/ctpat_strategicplan.pdf*.

CHAPTER 5

PORT RECOVERY FROM SECURITY INCIDENTS: A SIMULATION APPROACH

Ghaith Rabadi and C. Ariel Pinto

Engineering Management and Systems Engineering Department, Old Dominion University, Norfolk, Virginia, USA

Wayne Talley

Economics Department, Old Dominion University, Norfolk, Virginia, USA

Jean-Paul Arnaout

Industrial and Mechanical Engineering Department, Lebanese American University, Byblos, Lebanon

Abstract

The security incident cycle of ports consists of four phases: (1) prevention—creates barriers that deny terrorist plans and events; (2) detection—provides early apprehension of planned terrorists acts using inspection, tracking and monitoring; (3) response—mitigates the impact of a security incident to the port once it has occurred; and (4) recovery—promotes the port's return to normal operations following a security incident. There has been much ex ante investigation in securing (prevention and detection) ports from security incidents, but little ex post investigation into the response and recovery from port security incidents once they have occurred. This chapter investigates port recoverability from security incidents, i.e., how long it will take for a port to return to normal operations following the occurrence of security incidents or due to elevating port security measures. The investigation is undertaken by first developing a simulation model of the operations of a US container marine port terminal to capture container movements and storage within the terminal as well as the arrival and departure of containers via ships, trucks and rail. Critical recourses such as ship-to-shore cranes, straddle carriers and truck chassis are also modelled in simulating the terminal's container throughput. The simulation model of the terminal's throughput can then be used to simulate the impact of various security incidents on the terminal's throughput and operations resulting from, for example: shifting resources to handle security incidents; reducing the number of terminal gates in use; and delays to conducting the screening of inbound containers. The model will use these impacts, in turn, to investigate the terminal's recoverability based upon various recoverability strategic decisions of terminal decision makers. An analysis of the latter will provide the decision makers with insights into strategic decisions for improving the recoverability of port operations following security incidents.

1 INTRODUCTION

Ocean transportation is the primary transportation mode for world trade particularly in the US where ports handle approximately 2 billion tons of cargo annually and is expected to double within 15 years (Nagle, 2005). It transports 95% of US intercontinental trade. Hence, a security incident at a US port that results in its shut down for a significant length of time will not only have a devastating effect on the local port and community, but also on US intercontinental trade and the economy.

A security incident that reduces the throughput at a port (but not its shutdown) can also be costly to the port in terms of revenue foregone and the loss of future throughput (from ships going elsewhere). In order to forecast the extent of throughput reductions for a given port from various security incident scenarios, a port simulation throughput model may be used. The model may also be used to investigate the effectiveness of various port management scenarios in reducing security incident delays.

In this chapter, we present a discrete-event simulation that models port operations of a US container port on the east coast to study the impact and analyse the risk that certain security incidents or scenarios may have on the port's operation continuity. In a broader sense, the same model can be used to evaluate business scenarios such as implementing a certain operational policy, increasing/decreasing resources, or deploying a new technology. Various performance measures can be evaluated including delays, queue times, resource utilization, throughput and turnaround times. This will help the port's administrators plan for operational decisions to minimize the disruption of possible security incidents. The longer-term objective is to provide insights into strategic decisions for better continuity of port operations in light of continuing changes in security technologies, policies and guidelines

2 BACKGROUND ON TERMINAL PROCESSES

The port addressed in this paper is a US container port that handles cargo stored in standardized boxes or containers, generally 20 or 40 feet in length without wheels—i.e. as one TEU (20-ft equivalent unit) or as one FEU (40-ft equivalent unit). This port is considered an intermodal node in the transportation network, where cargo changes modes of transportation (e.g. from a ship to an inland transport mode and vice versa) (Talley (2006).

The modelling of this port was designed at a granularity level of containers, trucks, cranes, straddle carriers, trains and ships. Other resources and components that are at a lower granularity were considered embedded in the ones listed above, and other resources (e.g. personnel) were considered readily available whenever needed. The flow of operations at most container ports including the one described here can be categorized as follows:

2.1 Truck Flows (Figure 1):

- Full and empty containers on truck chassis move through police gates then interchange gates to container storage areas. Full containers are removed from chassis by a straddle carrier and placed in storage or ship departure areas. Empty containers are removed from chassis using the empty container handler and placed in a storage area for empty containers. In most cases, chassis remain attached to trucks to load containers to take back inland. However, in some cases chassis may be unhooked and left in a chassis storage area on terminal. Both cases are accounted for in this model.
- Truckers enter truck gates with chassis to container storage areas or ship arrival areas. A straddle carrier then obtains a specific full container from a container storage area or a ship arrival area and places it on the trucker's chassis for departure. If the trucker is to pick up an empty container, the empty container handler is used to load it on the chassis.
- Truckers enter truck gates without chassis, move to a chassis storage area to hook chassis to the tractor, and then a straddle carrier obtains a specific container from a storage or ship arrival area and places it on the trucker's chassis for departure. If the trucker is to pick up an empty container, the empty container handler is used to load it on the chassis

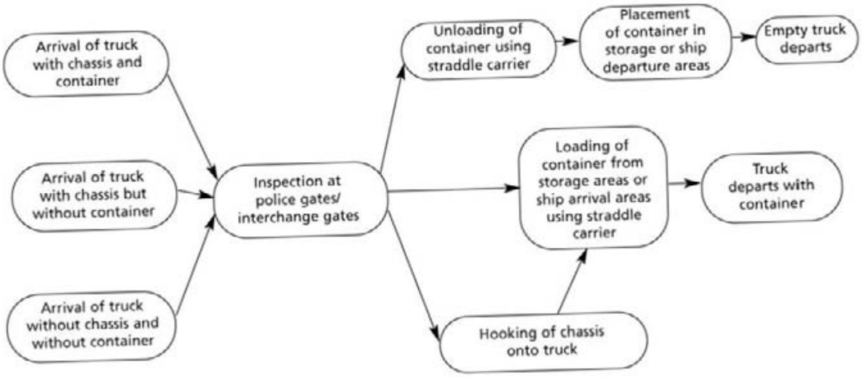

Arrival of truck with chassis and container
Arrival of truck with chassis but without container
Arrival of truck without chassis and without container
Inspection at police gates/ interchange gates
Unloading of container using straddle carrier
Placement of container in storage or ship departure areas
Empty truck departs
Loading of container from storage areas or ship arrival areas using straddle carrier
Truck departs with container
Hooking of chassis onto truck

Figure 1: Flowchart for Trucks

2.2 Train Flows (Figure 2)

- A double stack train moves through rail gate and stops at train loading and unloading area. Containers are then removed from the train by a transtainer and placed on truck chassis attached to a tractor and hauled to container storage areas or ship departure areas.

- An empty double stack train is located at train loading and unloading area (arrived previously as a loaded train), a transtainer obtains specific containers from the container storage area or ship arrival area and places them on cars of the double stack train for departure.

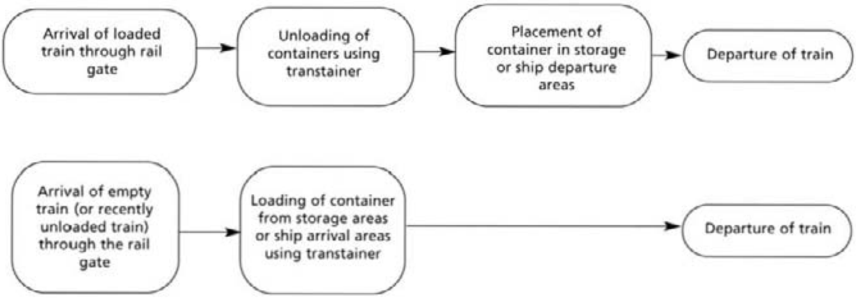

Arrival of loaded train through rail gate
Unloading of containers using transtainer
Placement of container in storage or ship departure areas
Departure of train
Arrival of empty train (or recently unloaded train) through the rail gate
Loading of container from storage areas or ship arrival areas using transtainer
Departure of train

Figure 2: Flowchart for Trains

2.3 Ship Flows (Figure 3)

- Ships arrive to berths and unload full and empty containers using port cranes on to unloading areas. Straddle carriers are then used to deposit containers in their designated storage areas. Water-to-water containers do not leave the ship.
- After the ships finish unloading containers, port cranes are used to load containers on to the ship from the loading areas. Prior to that, straddle carriers would have brought the containers to the berth's loading area.
- Ships depart after container loading is complete.

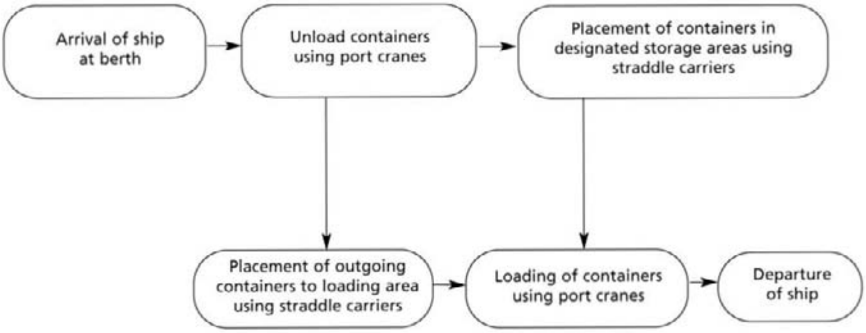

Arrival of ship at berth
Unload containers using port cranes
Placement of containers in designated storage areas using straddle carriers
Placement of outgoing containers to loading area using straddle carriers
Loading of containers using port cranes
Departure of ship

Figure 3: Flowchart for Ships

3 PORT SIMULATION

In this chapter, a discrete-event throughput simulation that models the movements described earlier is presented. The purpose of the model is to evaluate the impact of certain security incident scenarios on the terminal's measures of performance including throughput, delays, queues and/or resource utilization. Discrete-event simulation simulates a system as it evolves over time and for which the state variables change instantaneously at separate points in time (Law and Kelton, 2000). Simulation models have been used to evaluate scenarios or changes to systems before they occur in order to better understand the associated risk. In this chapter, discrete-event simulation was selected as the tool of choice due to its ability to capture the dynamics of complex systems and model stochastic processes. Although traditional analytical (mathematical) and queuing models can be used, they generally do not consider system randomness, and when they do, they require in most cases crude assumptions and closed mathematical formulae making the validity of the results questionable. In addition, simulation is a very flexible tool that easily enables decision makers to inject the system with different scenarios and observe the outcome.

It has been demonstrated that discrete-event simulation is an effective tool for modelling operations including port operations. For example, Shabayek and Yeung (2002) developed a discrete-event simulation model to simulate the operations of Kwai Chung container terminals in Hong Kong. Parola and Sciomachen (2005) have used simulation to model a port system in Italy. Leathrum *et al.* (2004) have used discrete-event simulation for modelling military port operations. Port simulation models have also been developed by Koh *et al.* (1994) and Legato and Mazza (2001).

Although simulation models have been developed for a number of container ports around the world, it is important to recognize that there are usually some differences among ports that may make them logistically unique due to specific geographical location and management style. In addition, the focus of most of existing models has been on port design or improvement of business processes. In this chapter, however, the focus is to present an approach for measuring the impact of security scenarios on the continuity and recoverability of ports.

3.1 Simulation Model Scope

The model is comprised of several components that capture the dynamic movements described earlier. The model components can be classified into entities, resources, processes and transporters as shown in Table 1. Note that although transporters are listed separately from resources, in effect they are a special type of resources for which queues may form when entities are waiting for a transporter and that transporter is busy.

Model component type	*Model component names*
Entities	Trucks, chassis, trains, ships, and containers
Processes	Inspection at police gates, check-in at interchange gates, check-out at interchange gates, inspection and check-in at train gates, check-out at train gates, hooking chassis to trucks, unhooking chassis off trucks, loading containers on chassis, unloading containers off chassis, loading containers on ships, unloading containers off ships
Resources	Police gates, interchange gates, train gate, chassis remover
Transporters	Straddle carriers, empty container handler, transtainers, cranes

Table 1: Simulation Model Components

3.1.1 Input Analysis

In a commercial port environment, logistical complexity with a touch of randomness will inevitably result in variability that will lead to stochastic processes. To have a valid representation of the real system, the simulation model must include realistic levels of input uncertainty; otherwise its output may lead to inaccurate conclusions.

Therefore, port historical data was fitted to statistical distributions and was then statistically tested using Chi-square and Kolmogorov-Smirnov (K-S) goodness-of-fit tests to ensure they are a good representation of the real processes. Historical data did not exist for some processes and, therefore, subject-matter experts (SMEs) were surveyed to provide input for these processes from their experience or other systems to which we had no access. The following inputs were based on historical data:

- types of trucks, i.e. trucks with full containers, empty containers, no containers, or no chassis;
- number and type of containers to load on, or unload from, ships and trains;
- interarrival times for ships, trains and trucks; and
- the number of trucks performing one operation (i.e. dropping off or picking up containers) versus those performing two operations (i.e. dropping off and pick up containers).

Data inputs provided by SMEs took one of two forms: single point estimates (i.e., constants) or a uniform distribution based on the SMEs' long experience in port and terminal operations. The authors performed a quick verification of these inputs during terminal visits. SME inputs to the simulation and whether they were a point or distribution estimates are as follows:

- time to load a container on a truck (uniform distribution);
- time to load a container on a train (uniform distribution);
- time to load a container on a ship (uniform distribution);
- time to unload a container from a truck (uniform distribution);
- time to unload a container from a train (uniform distribution);
- time to unload a container from a ship (uniform distribution);
- time at the police gates (uniform distribution);
- time at interchange gates (single estimate);
- time hook chassis (single estimate);
- time to unhook chassis (single estimate);
- speed of straddle carriers (single estimate);
- speed of cranes (single estimate);
- speed of empty container handlers (single estimate); and
- speed of transtainers (single estimate).

3.1.2 Model Validation and Output Analysis

Ports usually invest in processes or technology that can show immediate saving on the operational level such as reducing container delays, reducing truck turnaround time, or increasing the utilization of scarce resources. Security incidents could be damaging and costly. This project is an initial framework to evaluate the impact of potential security scenarios if they were to occur. Therefore, the simulation can also be used to justify and prioritize investments in port security. The model, however, must be validated before it can be used for these purposes. The simulation validation method followed in this chapter is to compare the model's outputs to the real historical data whenever available. For processes and operations that did not have historical data, technical SMEs were presented with simulation output for validation. Figures 4 and 5 show the validated simulation output.[1] In particular, Figure 4 shows how closely the simulated truck traffic compares with historical data while Figure 5 shows the average time spent by trains, ships and trucks in the port as well as the corresponding 95% confidence interval.

[1] Actual data has been masked for confidentiality and protection.

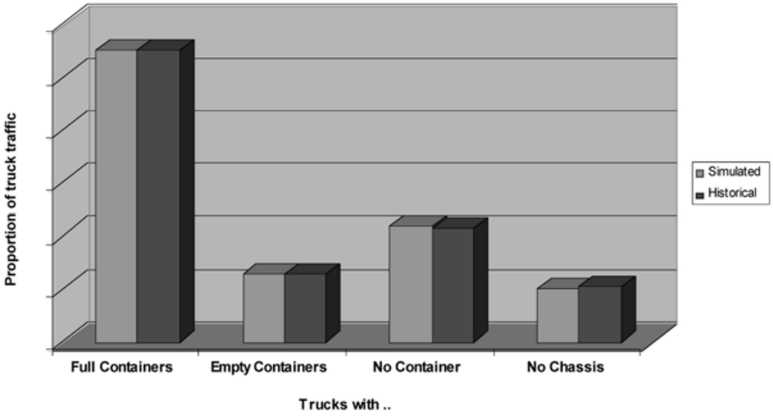


Figure 4: Proportion of Historical and Simulated Truck Traffic by Type

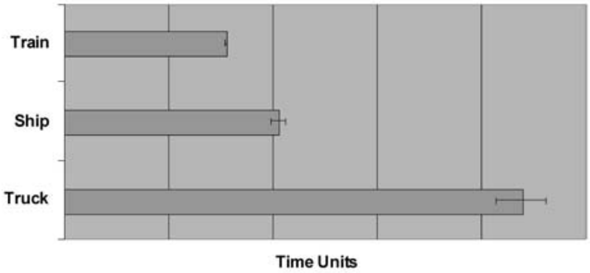


Figure 5: Time spent by Trains, Ships, and Trucks in Port (average and 95% confidence interval)

3.1.3 Security Scenario

Ultimately, the management of the port authority would want to understand and quantify the amount of risk by playing different risk scenarios and measuring the operational delays and reduction in throughput until the flow goes back to normal (i.e. measuring port recoverability). This should help management decide how to allocate their resources for minimizing operational risk. The following hypothetical scenario was considered to demonstrate the approach:

> US intelligence agencies intercept information on a plan for a major terrorist attack on the US transportation infrastructure that may take place around the middle of the month. Specifically, their plan is to acquire empty containers in the US with forged shipping documents indicating that the containers are empty and are being returned to other ports overseas for re-use, while in reality they will be loaded with explosives. Innocent trucking companies will deliver them to some port(s) to be

detonated there causing a widespread shutdown of intermodal and maritime transportation, and resulting in devastating loss to the US economy and destroying public confidence in US homeland security efforts. The Department of Homeland Security (DHS) raises the alert level for all intermodal transportation (ports, rail and trucking) and so does the Coast Guard for all US commercial ports. Consequently, stringent requirements were enforced on all containers entering the truck gates to be opened and inspected, which is expected to increase the delay at the police gates of an average of five minutes per truck. This procedure will be followed for two days, and non-intrusive inspections of all containers will be conducted for another two days, which will increase the delay at the police gate by an average of three minutes. The question the port authority is interested in answering is what impact the added security procedure will have on the port in terms of delays, queue times and throughput?

3.1.4 Computational Tests

In order to test this scenario, the simulation was run for 10 replications (with different initial random seeds) for one month under normal operational conditions, and for another 10 replications (with different initial random seeds) under the previous hypothetical security scenario. The number of replications was determined by following the approach recommended by Kelton *et al.* (2004) where an initial number of replications n_0 was arbitrarily set to 2 resulting in a fairly large half width. To obtain a desired half width of 2.5% (i.e., 95% confidence interval) the following equation was used (Kelton *et al.*, 2004):

$$n \cong n_0 \frac{{h_0}^2}{h^2},$$

where n_0 and h_0 refer respectively to the initial number of replications (2) and its associated half width; h refers to the desired half width; and n is the number of needed replications, which came out to 10.

3.1.5 Simulation Scenario Results

After running the simulation model, the following observations were drawn for the month that included the security incident:

- the number of chassis on terminal has increased by 4.2% because fewer trucks were able to use them;
- the number of full containers on terminal has increased by 19.6%;
- the number of empty containers on terminal has increased by 16.8%;
- the average queue for trucks at the police gates has increased by 188.6%; and
- an increase in the truck turnaround time by 4.4%.

Figures 6 and 7 show the difference in the moving average of the trucks' turnaround time without and with the incident scenario, respectively. The moving average was calculated in increments of 2.5 hours and as can be seen in Figure 4, there is a clear increase in turnaround time due to increased security at day 15 (hour 360 on the *x* axis). The turnaround time eventually goes back to normal port operations at hour 465. It should be noted, however, that even after the security went back to normal (after four days), the trucks' turnaround time stayed relatively high and did not go back to normal until nine hours later.

From the results, one can conclude that due to tightened security trucks were having problems getting on terminal and, therefore, the number of chassis and containers increased as there were not enough trucks to pick them up. Not only does this impact container throughput, but may also have a serious terminal congestion problem due to container storage space limitations.

Another important impact caused by the scenario is the large increase in the police gate queue. Obviously such a queue will impact the highways and roads around the terminal, causing traffic congestion and backups.

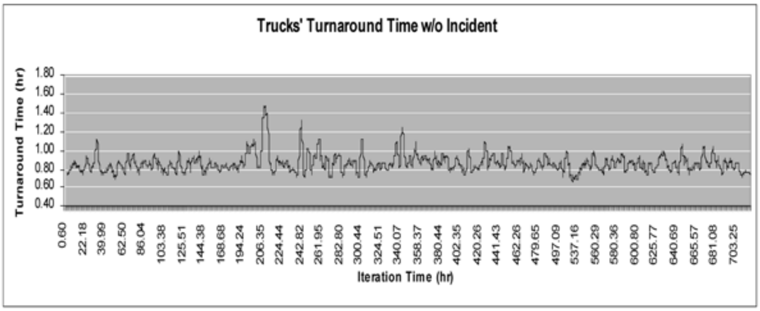


Figure 6: Truck Turnaround Time under Normal Conditions

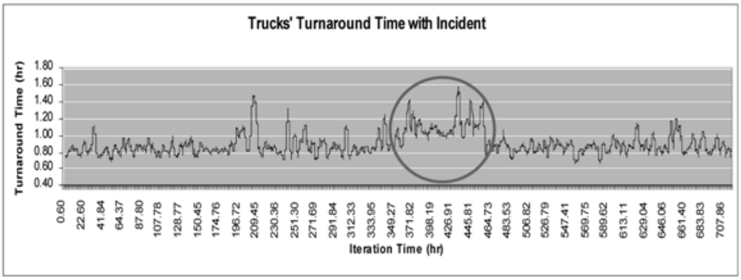


Figure 7: Truck Turnaround Time with a Security Incident

4 CONCLUSIONS

A discrete-event simulation model was developed for port operations in a US marine intermodal terminal. The main objective of the model is to evaluate the impact of security scenarios on port recoverability, i.e. its ability to go back to normal operations. The model captures the movements of full and empty containers from sea to inland and vice versa. It also includes the movements of trucks, train and ships, which are modelled as dynamic entities. Terminal gates are modelled as recourses with specific capacities, while straddle carriers, cranes and transtrainers are modelled as transporters. Model inputs and stochastic processes are based on historical data that was fitted to statistical distributions to reflect the variability in the real system. The model was then validated by comparing its output to historical data whenever possible, and by presenting the output to subject-matter experts whenever data was unavailable. To demonstrate the proposed approach for risk evaluation, a hypothetical scenario was implemented and tested to show its impact on port recovery in terms of throughput, delays and queue times. The simulation results for the hypothetical scenario showed that the number of containers and chassis on terminal, as well as the truck turnaround time would increase significantly, while the police gate queue time might be unacceptable. An estimate of how long it will take for the terminal to go back to normal can also be obtained by comparing the simulation runs with and without the scenario.

The simulation model can be further utilized by the port authority to evaluate additional security and business scenarios. In the future, this model can be extended beyond the terminal's gates to evaluate the impact on the transportation network (e.g. traffic congestion) and supply-chain security.

REFERENCES

Kelton, W.D., Sadowski, R.P. and Sturrock, D.T. (2004) *Simulation with Arena*, 3rd edn, McGraw Hill.

Koh, P-H., Goh, J., Ng, H-S. and Ng, H-C. (1994) "Using Simulation to Preview Plans of Container Port Operations", *Proceedings of the 1994 Winter Simulation Conference*, eds J.D. Tew, S. Manivannan, D.A. Sadowski and A.F. Seila.

Law, A.M. and Kelton, W.D. *Simulation Modeling and Analysis*, 3rd edn, McGraw Hill, (2000).

Leathrum J.F., Mielke, R.R., Mazumdar, S., Mathew, R., Manepalli, Y., Pillai, Y., Malladi, R.N. and Joines, J. (2004) "A simulation architecture to support intratheater sealift operations", *Mathematical and Computer Modelling*, 39(6–8), pp. 817–838.

Legato, P. and Mazza, R.M. (2001) "Berth planning and resources optimisation at a container terminal via discrete event simulation", *European Journal of Operational Research*, 133(3), 537–547.

Nagle, K. (2005) "Nation's Ports Concerned About Security, Harbor Dredging Funding Shortfalls in Fy'06 Budget", *The Propeller Club Quarterly*, Spring, 13–14.

Parola, F. and Sciomachen, A. (2005) "Intermodal container flows in a port system network: Analysis of possible growths via simulation models", *International Journal of Production Economics*, 97, 75–88.

Shabayek, A.A. and Yeung W.W. (2002) "A simulation model for the Kwai Chung container terminals in Hong Kong", *European Journal of Operational Research*, 140(1), 1–11.

Talley, W.K. (2006) "An Economic Theory of the Port", *Port Economics: Research in Transportation Economics*, eds, K. Cullinane and W. Talley, Vol. 16, 43–66. Amsterdam, Elsevier.

CHAPTER 6

SECURITY AND RELIABILITY OF THE LINER CONTAINER-SHIPPING NETWORK: ANALYSIS OF ROBUSTNESS USING A COMPLEX NETWORK FRAMEWORK

Panagiotis Angeloudis, Khalid Bichou and Michael G.H. Bell

Port Operations Research and Technology Centre (PORTeC), Centre for Transport Studies, Imperial College London, UK

Abstract

Since the events of 9/11, more focus has been given to the role of sea ports as critical nodes in the functioning and security of international shipping and logistics, with particular emphasis being placed on container ports and terminals. However, little or no work has addressed the robustness and the reliability of the container port network, be it at the level of terminal operating systems or at the level of international trade and logistics patterns. In this chapter, ports and scheduled liner containership services between Western Europe and North America are modelled as the nodes and links of a global network. Following recent work in urban transportation, the properties of the network are examined in the context of complex network theory, with particular reference to error and attack robustness. Generic frameworks and a hypothetical case study are presented to identify points in the network where failure would lead to a wider collapse.

1 INTRODUCTION

The theory of complex networks is a fast growing field of applied mathematics. Having its roots in the random graph model by Erdös and Ranyi (1959), interest in the field has been sparked by the recent development of the small-world and scale-free models by Watts and Strogatz (1998). Studies on the subject have shown interesting results in fields as diverse as ecology and social science, possibly the most famous being the discovery that on average only six degrees of separation exist between any two people selected at random. Networks such as the air travel grid, road and subway systems have been analysed this way (Angeloudis and Fisk, 2006; Albert *et al.*, 2002; Dunne *et al.*, 2002), but the technique has yet to find application in other major transportation networks. There has been parallel interest in the application of complex networks theory to supply-chain topologies, regarding such aspects as robustness, resilience and agility (Swaminathan *et al.*, 1998; Thadakamalla *et al.*, 2004). Nevertheless, there has been little or no use of the theory in the context of sea port and maritime transport networks.

Traditionally, international shipping networks have followed a trade-led pattern where new routes are opened and operated to link two or multiple markets, ideally on the basis of a balanced traffic. In liner shipping, much of the world's containership capacity is deployed to serve within one or a combination of the three major trade lanes: the trans-Pacific; the trans-Atlantic; and the Europe–Asia routes. However, both traffic and operational constraints regarding traffic type and volume, route distance and seasonal variations, containership's size and capacity, etc., have forced shipping lines to develop new operational patterns in an effort to optimize ship utilization and efficiency. The key point is that the pattern of routes is not master planned but has evolved from many micro decisions. Evolving complex networks such as hub-and-spoke and transhipment routes are a common feature of today's liner routes, although neither model (in its current format) has succeeded in achieving optimal solutions with regard to the combination of economic, capacity, safety and scalability constraints.

In the post-9/11 era, the robustness and survivability of the maritime network against node failures is a high priority. Research to date has looked at different but fragmented areas of network robustness including such aspects as system vulnerability, risk avoidance, mitigation strategies and supply-chain resilience. In ports and shipping available models of risk assessment and attack avoidance, be it regulatory-based (e.g. the ISPS port facility security plan) or industry-led (e.g. the Lloyd's Register See-threat programme), only identify risk elements based on logical mapping of internal processes, but there has been no applied research on the robustness of the shipping network link (route) and node (port/terminal) topology, quite apart from the perspective of the complex network theory (Bichou, 2005).

Current maritime transport networks have been designed to respond to an extensive set of market and operational requirements, but their robustness and reliability *vis-à-vis* random or targeted failures have long been taken for granted. We emphasize that system or node failure could be trigged by a variety of precursors and not just malicious or unexpected actions such as terrorist attacks. Examples of node failure causes include industrial strikes, ship collision or safety incidents, government or regulatory measures such as port closure in extreme weather conditions, and any other operational incidents in ports (damage to ship's structure while being operated at quay, system failure for automated terminals, etc.) or at intermodal interfaces (e.g. road network congestion).

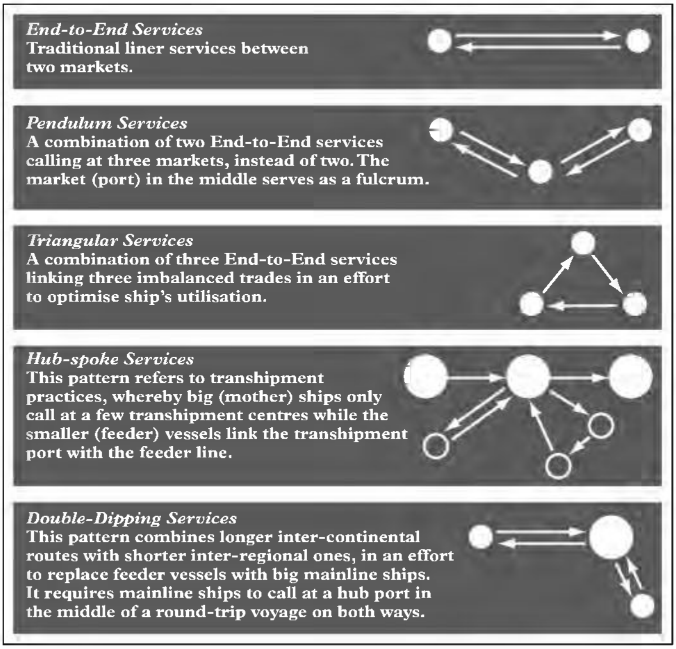
This study proposes to investigate the robustness properties of the current liner-shipping routes using complex networks theory. We build a shipping network linking European and North American sea ports based on current liner routes, and use a simulation model specifically developed for the purpose of this study to test and analyse the robustness of the network. The subject of this paper is part of a larger project aiming to model the global liner network and link it to selected port and intermodal networks in order to investigate its survivability and scalability with respect to a variety of objectives, including operational efficiency, system resilience and flexibility, as well as the design of optimal connectivity solutions. This chapter only reports on selected aspects of network robustness and node failure.

The remainder of the chapter is structured as follows. Section 2 briefly describes trade versus operational patterns in liner shipping, while section 3 reviews the literature on the complex network theory and its applications to date. Section 4 describes the dataset and the network architecture before reporting the results of the simulation model. Section 5 concludes with summaries and suggestions for future research.

2 REVIEW OF OPERATIONAL PATTERNS IN LINER SHIPPING

The international shipping industry may be divided into two different categories: tramp shipping and liner shipping. Industrial shipping may be a third category, but this is generally treated as a closed and separate market. Unlike tramp ships that operate in the spot market and thus can go everywhere at any time, liner shipping consists of pre-scheduled and regular maritime routes linking fixed ports and terminals. Containerships operate on different markets and routes according to a number of criteria. The routes are normally those between two trade markets (supply and demand) with a range of ports being visited between and at either side of the route. Trade routes or lanes ideally link two or multiple markets based on an equitable traffic pattern and any other relevant requirements. Route optimization in this approach follows from the formulation of origin–destination (O/D) models, and much of the literature on shipping network planning and design falls into this category (see for instance Iakovou *et al.*, 1999; Beuthe *et al.*, 2001).

Too often though, traffic is unbalanced between regions in either or both direction and could be stable on some routes while variable on others. This can result from structural or seasonal variations but is sometimes due to the nature of the route, for instance, in terms of distance, traffic type and cargo volume. Similarly, the growth in containership size makes it less profitable for carriers to call at every port on their journey. For such reasons and others, the problem of liner network routing has been reduced to a ship's scheduling problem (Bendall and Stent, 2001, Christiansen, *et al.*, 2004; Fagerholt, 2004) and different operational patterns have evolved through the years. This means that within one or a combination of trade lanes, a different logistics pattern is undertaken to ensure optimum ship utilization and efficiency. Major operational patterns in liner shipping include the end-to-end, pendulum, triangular, hub-and-spoke, double-dipping and round-the-world services. Finally, it is worth underlining that many aspects of maritime network design under supply-chain constraints and uncertainty remain largely unexplored in the maritime and ports literature, contrary to the great amount of scholarly work on the subject for inland-based distribution networks.



End-to-End Services
Traditional liner services between two markets.

Pendulum Services
A combination of two End-to-End services calling at three markets, instead of two. The market (port) in the middle serves as a fulcrum.

Triangular Services
A combination of three End-to-End services linking three imbalanced trades in an effort to optimise ship's utilisation.

Hub-spoke Services
This pattern refers to transhipment practices, whereby big (mother) ships only call at a few transhipment centres while the smaller (feeder) vessels link the transhipment port with the feeder line.

Double-Dipping Services
This pattern combines longer inter-continental routes with shorter inter-regional ones, in an effort to replace feeder vessels with big mainline ships. It requires mainline ships to call at a hub port in the middle of a round-trip voyage on both ways.

Figure 1: Description of Selected Operational Patterns in Liner Shipping

3 OVERVIEW OF COMPLEX NETWORK THEORY

Random graphs are one of the earliest and most extensively studied network models. They are defined as networks with N nodes and n links which are assigned at random. On the opposite side of the network model spectrum, one encounters regular networks, where link creation adheres to strict rules.

Watts and Strogatz (1998) propose a network model that interpolates between regular and random networks by applying a random rewiring procedure on a regular ring lattice, as shown in Figure 2. In a variant to this model, Newman and Watts (1999) propose the "small world" model where the edges are added randomly between vertices without removing others in the ring lattice. Networks produced by this process have a smaller average shortest path length compared to a similar random graph network. The name of the model originates from its roots in social systems and more specifically from a well-known experiment by social psychologist Stanley Milgram who discovered that there are on average six degrees of separation between any two residents in the United States. Another property of small worlds is an increased clustering coefficient, which is used to quantify the tendency of nodes in various parts of the network to form interconnected groups with many links within them, but only few between them. For a node i with k_i links, the local clustering coefficient C_i is obtained through the following relationship:

$$C_i = \frac{2E_i}{k_i\ (k_i - 1)}$$

where E_i is the number of edges between the k_i nodes. The overall clustering coefficient of the network is the average of all the local values.

Scale-free networks were introduced by Barabasi and Albert (1999) in order to explain the behaviour of many real world systems (like the WWW) that could not be adequately modelled as random networks. According to the model, the number of links k originating from a given node adheres to a power law $P(k) \sim k^{-\gamma}$, which for large networks is free of a characteristic scale. This effectively means that some nodes will have an exceptionally large number of links when compared to the vast majority of nodes in the network. Scale-free network are thought to be created by a process of preferential attachment ("the rich get richer"), whereby new nodes will be more likely to be linked to existing nodes with a higher degree (number of links) in order to benefit from their increased connectivity to other parts of the network.

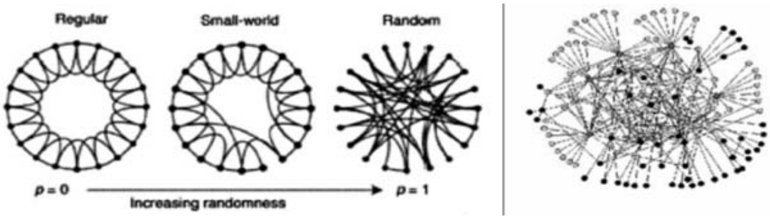


Figure 2: Illustration of the Small-world Rewiring Procedure (from Watts and Strogatz, 1998)

When studying scale-free networks, more emphasis is given to their robustness against errors and robustness against attacks, which effectively represent two different strategies of node removal. In the investigation of error robustness, the underlying assumption is that nodes to be removed are selected at random in order to simulate the likely impact of evenly distributed operational errors on the network's robustness. Regarding attack robustness, the modeller must hold sufficient prior information about the system, which is then targeted strategically with a view to maximizing the impact. Scale-free networks exhibit an exceptional degree of robustness against random node failures due to the dominance of few hubs over their topology. The situation is reversed in the case of intentional attacks, since major hubs are relatively easy to identify.

Soon after the initial publication of the two network types in the late 1990s, a movement began among researchers to model real world networks. Systems that have been modelled using such approaches include food webs, power grids, rail and subway networks and supply-chain configurations (see, for instance, Albert *et al.*, 2002; Angeloudis *et al.*, 2006; Dunne *et al.*, 2002). Nonetheless, we are not aware of any application of complex networks theory to shipping and ports, particularly in the contexts of security and system reliability.

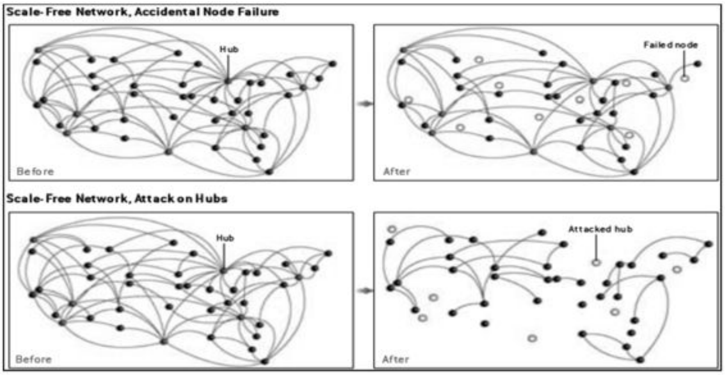

Scale-Free Network, Accidental Node Failure
Hub
Before
Failed node
After
Scale-Free Network, Attack on Hubs
Hub
Before
Attacked hub
After

Figure 3: Node Failure Scenarios in Scale-Free Networks. (from Albert *et al.*, 2003)

4 MODELLING LINER SHIPPING ROUTES

4.1 Dataset and Model Assumptions

The aim of the modelling process was to create a relatively precise model of the global container liner shipping network, which should also be used for future projects. A database was built using the information on current fleet deployment and liner schedules as posted on individual websites of global shipping lines, ports and relevant web-based information providers such as *Containerisation International.* Due to the large scale and scope of the global shipping network, it has been decided to limit the analysis at this initial stage to the liner routes linking Europe to North America. The focus on the trans-Atlantic routes is also justified by the priority given to security and reliability issues, proven by the amount and extent of security regulations targeting the shipping and port industry in both sides of the Atlantic. One should emphasize, however, that many trans-Atlantic routes are part of a wider global network such as round-the-world trips, and as such they are fully included in the model.

Most transport and freight distribution systems follow a node-link network structure, although the nature and properties of the network differ greatly between and within systems. For instance, unlike rail and road systems, maritime links may be established between any two or more sea port locations subject to fewer infrastructural (ports, canals, locks, etc.) and operational (volume, capacity, price, etc.) constraints. In the context of this chapter, liner shipping networks are defined as scheduled routes using regular service lines that link predefined series of ports and terminals. This assumption represents a major constraint on the flexibility of the network, but can be discarded in situations involving node failure. The model described in this paper accounts for this feature and allows ships to move freely between available nodes (ports) in the event of node failure.

The above feature of the model requires the elimination of physical and any other constraints to both node and link structures. This can be captured by assuming that no response is further constrained by physical limits such as ship size or port capacity. Both assumptions are hypothetical because in the real world ships and ports are of different size, draft, capacity, etc. The assumptions do not, however, represent an intrinsic limitation of the model since it is possible to develop a database that includes all the relevant information about each port and vessel in the network. Figure 4 depicts the shipping network generated by in-house modelling software that was developed for the purpose of complex network modelling. The route inputs on the network are in the form of ports of call sequences for each route. Through combining these sequences with port data, we generated the network shown below, where each port is represented as a circular node and the links between represent trips.

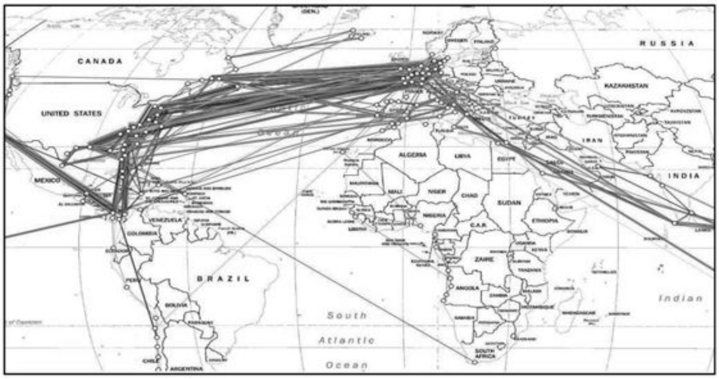
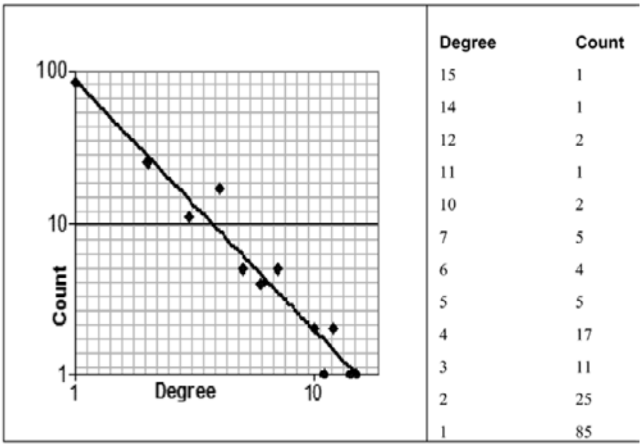


Figure 4: The Liner Shipping Network between Europe and North America

4.2 Analysis and Results

The network generated has 159 nodes, a size much smaller than databases generated by previous studies such as for power grids, the Internet or the air travel network. In a network of such a small size, it is difficult to observe well-defined features of the common network models (Dunne *et al.*, 2002). Nevertheless, the behaviour of the network can still be identified by examining the different properties attached to it. Among these, the degree distribution of the model is a property of particular interest. Basically, a node degree denotes the number of connections each node is linked to. However, due to the fact that more than one service may provide a path between two ports, it makes more sense to consider as degree the number of neighbours that a port has. The resulting degree distribution (shown in Figure 3) can be approximated by a very strong power law equal to $P(k) = 87.3k^{-1.6}$, which could be indicative of an underlying scale-free network.

Regarding the remaining complex network properties of the model, it was found to have an average path between any two nodes of approximately six stops, a clustering coefficient of 0.0278, and a network diameter (maximum number of stops between any two nodes) of 28. Further tests can be run in order to determine the busy nodes on the network. The table below presents a selection of the most heavily used nodes under different definitions of heavy use. (Opt.Paths in the table refer to the number of optimum paths between any two ports in the network that the examined port is a part of.)



Degree	Count
15	1
14	1
12	2
11	1
10	2
7	5
6	4
5	5
4	17
3	11
2	25
1	85

Figure 5: Degree Distribution of the Liner Shipping Network between Europe and North America

Station	*Neighbours*	*Links*	*Opt. Paths*
Antwerp	15	152	5239
Bremerhaven	7	124	903
Charleston	12	174	3661
Felixstowe	7	35	216
Halifax	7	47	1585

Station	*Neighbours*	*Links*	*Opt. Paths*
Hamburg	7	78	387
Le Havre	11	112	1891
Manzanillo	10	54	3900
Miami	6	54	2092
Montreal	10	64	1653
New York	12	144	2745
Rotterdam	14	156	5371

Table 1: Critical Nodes and Under Various Definitions of Network Vulnerability

Simulations of informed intentional attacks using these results targeted the busiest nodes and assessed the impact of each action on the network. After each individual attack on a node, the state of the network was reassessed in order to identify the most vulnerable node that would also constitute the next target.

Further analysis can be performed to evaluate the impact of various events on the network as a whole. Our algorithms are capable of determining how container shipments would have to be rerouted to account for the defective node, by identifying a new minimum cost path given the current situation. Through this procedure, optimal container routes and points of transhipment are recalculated, and the resulting state of the network is compared to the original one before the events. As such, shipment reroutings necessary to avoid currently infeasible paths are identified. Using these results, we can get an estimate of the additional load borne by different parts of the network in its current state by calculating the changes in the number of container routes passing through each node.

The figure below provides a visualization of this process. Indicated by the arrow is the port of Singapore, which is closed due to an imaginary attack, while the circles in bold are the indirectly affected ports that will face the highest extra transhipment load so that containers will reach their destinations without being handled in the affected port of Singapore. As shown in the figure below, the most heavily affected ports are Long Beach, Shanghai and Pusan, with a lot more lying in Europe and Far East that are affected to a smaller but not negligible extent. The wide distribution of the indirectly affected nodes illustrates the global impact of the closure of Singapore.

It is worth mentioning that our process at this early stage of the project does not take into account the processing capacity of the ports, and assumes that indirectly affected ports will be able to process the additional load. The repercussions would be even wider if, more realistically, capacity is taken into account. Modelling capacity is one of the immediate goals of this project.

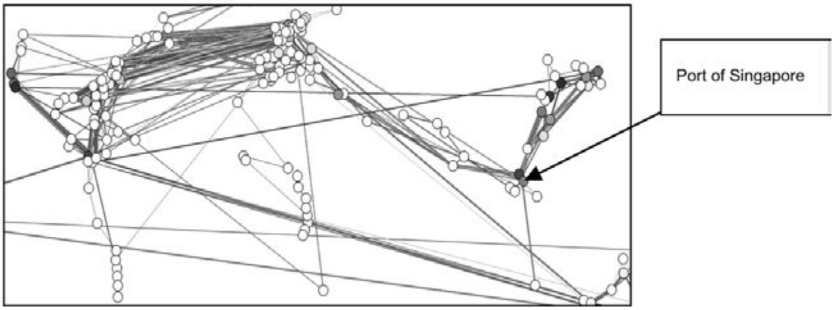


Figure 6: Visualization of Impact of Network Events

5 CONCLUSION AND FUTURE RESEARCH

This chapter started by providing a brief introduction to the complex network theory and its potential applications for modelling liner shipping networks. For the purpose of this chapter, we only modelled part of the global shipping network, namely the trans-Atlantic network, and have limited the analysis to system robustness and reliability against node failure. Nevertheless, we also mentioned current and future efforts to model the global maritime container transportation network and related intermodal links.

We have collected a database from one of the world's busiest shipping networks and modelled them as if belonging to one of the standard types of complex network for the purpose of robustness against both random and targeted node failure. Analysis of the network properties has shown that it relates closely to generic scale-free networks with an average path of approximately six port stops. Simulation of both random and intentional attacks has revealed that the most critical nodes are not necessarily the busiest ones, and that some ports may be more heavily affected than others, with impacts stretching to ports located beyond the trans-Atlantic network studied in this paper.

More analysis is needed to fully understand the structure, network properties and robustness of the global shipping network, but the study reported here can shed some light on how complex networks theory can be as useful for the analysis of shipping and intermodal routes as it is for other real world networks. One of the immediate goals of this project is to remove various assumptions made so far in the interests of greater realism. The database of maritime routes will be extended to cover all of the currently existing liner routes, with ship scheduling also taken into account. Finally, port parameters like TEU storage and number of quay cranes will also be added to the model in order to obtain estimates of handling and storage capacities.

REFERENCES

Albert R. and Barabasi A., 2002, "Statistical mechanics of Complex Networks", *Reviews of Modern Physics*, 74, 47–96.

Angeloudis P. and Fisk D., 2006, "Large subway systems as complex networks", *Physica A*, In Press.

Barabasi A. and Albert R., 1999, "Emergence of scaling in random networks", *Science*, 286, 509–512.

Barabasi A. and Bonabeau E., 2003, "Scale-Free Networks", *Scientific American*, May 2003, 50–59.

Bendall H.B. and Stent A.F., 2001, "A scheduling model for a high speed containership service: a hub and spoke short-sea application", *International Journal of Maritime Economics*, 3, 262–277.

Beuthe M., Jourquin B., Greets J.F., Koul C. and Ha N., 2001, "Freight transportation demand elasticities: a geographic multimodal transportation network analysis", *Transportation Research*, E, 37, 253–266.

Bichou K. (2005), "Maritime security: framework, methods and applications". Report to UNCTAD, Geneva: UNCTAD, June 2005.

Christiansen M., Fagerholt K. and Ronen D., 2004, "Ship routing and scheduling: status and perspectives", *Transportation Science* 38(1): 1–18.

Dunne L., Williams R. and Martinez N., 2002, "Small Networks but not Small Worlds: Unique Aspects of Food Web Structure", Viewed 05/2004, *http://www.santafe.edu/research/publications/wpabstract/200203010.*

Erdos P. and Renyi A., 1959, "On random graphs I", Publ. Math. Debrecen 6: 290–297.

Fagerholt K., 2004, "Designing optimal routes in a liner shipping problem", *Maritime Policy and Management*, 31(4), 259–268.

Iakovou E., Douligeris C., Li H., Ip C. and Yudhbir L., 1999, "A maritime global route planning model for hazardous materials transportation", *Transportation Science*, 33(1), 34–48.

Newman M. and Watts D., 1999, "Scaling and percolation in the small-world network model", *Physical Review*, 60(6), 7332–7342.

Swaminathan J.M., Smith S.F. and Sadeh N.M., 1998, "Modelling supply chain dynamics: a multi-agent approach", *Decision Sciences*, 29(3), 607–632.

Thadakamalla H.R., Raghvan U.N., Kumara S. and Albert A., 2004, "Survivability of multiagent-based supply networks: a topological perspective", *IEEE Intelligent Systems*, Sept–Oct, 24–31.

Watts D., Strogatz S., 1998, "Collective dynamics of 'small-world' networks", *Nature*, 393, 440–442.

This page intentionally left blank

CHAPTER 7

PORT EFFICIENCY AND THE STABILITY OF CONTAINER LINER SCHEDULES

Michael G.H. Bell, Khalid Bichou and Kevin Feldman

Port Operations and Research Centre (PORTeC), Centre for Transport Studies, Imperial College London, UK

Abstract
This chapter examines the stability of schedules, with particular reference to a container liner operating a regular service along a fixed route collecting containers at each port of call. There are, of course, many sources of random variation for an operation of this type, but only one is considered in this chapter, namely the arrival headways at the first port of call. It is assumed that there is no slack in the schedule, so an extension to the arrival headway at the first port allows more containers to arrive at the port (they are assumed to arrive at a uniform rate with no random variation), which then take longer to be loaded. This causes an extension to the departure headway which is longer than the initial extension to the arrival headway. A similar process occurs at subsequent ports of call, so that a small extension to the arrival headway at the first port of call becomes a rather larger extension to the arrival headway at the last port of call. If the schedule is resumed at the first port of call after a perturbation, the schedule may or may not re-establish itself at subsequent ports of call. It is shown in this chapter that the condition for this to occur is that the rate at which containers can be loaded must be at least twice the rate at which containers arrive at each port of call. If this condition does not apply, any perturbation will cause the schedule to break down irretrievably and the system is therefore not stable.

1 INTRODUCTION

This chapter examines the stability of schedules, with particular reference to a container liner operating a regular service along a fixed route collecting containers at each port of call. There are, of course, many sources of random variation for an operation of this type, but only one is considered here, namely the arrival headway which is the period between the arrivals of two consecutive ships at a given terminal.

This chapter draws upon the model developed by Newell and Potts (1964) which is one of the first models that analysed bus service reliability. The main assumptions are that the passenger arrival rate, the bus loading rate, scheduled headway and travel time between successive stops do not vary between stops or buses. These assumptions remain in this chapter by replacing the passenger arrival rate by the container arrival rate to the quay, the bus loading rate by the ship loading rate, stops by ports of call and buses by ships. Further, Newell and Potts assumed that there was, at each stop, approximately the same number of passengers disembarking as there were passengers boarding. This process occurs simultaneously through the front and the back door of the bus. We can use this assumption here, assuming that there are at least two quay cranes respectively loading containers onto the ship and unloading containers from the ship onto the quay. Further, in the initial model, the unloading rate exceeded the loading rate, which explains why the calculation of the bus departure times only took into account the loading time. Newell and Potts's model has been successfully used to describe real-life situations with respect to bus scheduling.

The literature, to our knowledge, contains no study of the stability of schedules in the container shipping industry.

We are assuming that all containers which have arrived at the quay must be loaded onto the ship at the port and that containers can be loaded on any ship of the line. It is assumed that there is no slack in the schedule, so an extension to the arrival headway at the first port allows more containers to arrive at the port (they are assumed to arrive at a uniform rate with no random variation), which then take longer to be loaded. This causes an extension to the departure headway—the period between the departures of two consecutive ships from a given terminal—which is then longer than the initial extension to the arrival headway. A similar process occurs at subsequent ports of call, so that a small extension to the arrival headway at the first port of call becomes a rather larger disruption to the scheduled arrival headway at the last port of call. In this situation, the following ship will encounter fewer containers to pick up at the terminal and will thus spend less time at port than planned, meaning that it will leave the port prior to the scheduled time and thus catch up the leading ship. Because of this phenomenon and of the further assumption that ships do not overtake each other, "ship bunching" will occur.

An important assumption in our model is that the arrival rate of containers reflects the arrival rate at the quay crane, implying that the containers, once "arrived", are ready to be loaded onto the ship. Indeed, we are not considering that containers arrive from the hinterland into the yard and then to the quay but are considering a simple process where containers arrive continuously at the quay in order to be loaded onto the ship.

If the schedule is resumed at the first port of call after a perturbation, the schedule may or may not re-establish itself at subsequent ports of call. It is shown in this chapter that the condition for this to occur is that the rate at which containers can be loaded must be at least twice the rate at which containers arrive at each port of call. If this condition does not apply, any perturbation will cause the schedule to break down irretrievably and the system is therefore not stable.

The chapter goes on to derive analytical expressions for the variances for the arrival headways at the second and third ports of call. While expressions could be derived for subsequent ports, these become more complex along the route because of the growing complexity of the autocorrelation in the arrival headways. Simulation results show how the arrival headway variance grows explosively along the route, even where the system is stable. This variance can, however, be substantially reduced by increasing the rate at which containers are loaded. Thus the operating speed of quayside cranes is important for schedule stability.

2 STABILITY AT A SINGLE TERMINAL

Following Newell and Potts (1964), and substituting ships for buses, terminals for stops and containers for bus passengers, consider a single terminal exporting containers and define:

α = arrival rate of containers
β = loading rate of containers
σ = ratio of arrival to loading rate
h = arrival headway of vessels (assumed to be uniform)
$d^{(n)}$ = nth departure headway (arrival headway at the next port of call)

The nth departure headway is equal to the arrival headway minus the delay caused by the loading the leading ship plus the delay caused by loading the following ship, namely:

$$(1)\ d^{(n)} = h - \sigma d^{(n-1)} + \sigma d^{(n)}.$$

This simplifies to:

$$(2)\ d^{(n)} = \frac{1}{1-\sigma} h - \frac{\sigma}{1-\sigma} d^{(n-1)} \text{ (assuming } \sigma \neq 1).$$

At equilibrium:

$$(3)\ d = \frac{1}{1-\sigma} h - \frac{\sigma}{1-\sigma} d$$

which implies that $d = h$, as one would expect. Further, it can be noted that equilibrium also implies that $\sigma < 1$ since the loading rate of containers must always exceed the arrival rate of containers at the quay. Subtracting (3) from (2) yields:

$$(4)\ (d^{(n)} - d) = -\left(\frac{\sigma}{1-\sigma}\right) (d^{(n-1)} - d).$$

This demonstrates that a small positive deviation from equilibrium departure headway leads to a subsequent negative deviation from equilibrium departure headway. Whether this is larger or smaller than the initial deviation depends on whether $\frac{\sigma}{1-\sigma}$ is greater than or less than 1. Stability therefore requires that $\frac{\sigma}{1-\sigma} < 1$, which in turn requires that $\sigma < 0.5$. When $\frac{\sigma}{1-\sigma} > 1$, instability of the system will lead to ship bunching.

Consider a port where a ship calls regularly every day (or every 24 hours, so $h = 24$). If there is a one-hour deviation in the initial departure ($d^{(0)} = 25$), subsequent departures will be affected as shown in Table 1 when $\sigma = 0.3$ or $\sigma = 0.6$:

		$d^{(n)}$	
n	h	$\sigma = 0.3$	$\sigma = 0.6$
1	24	23.57	22.50
2	24	24.18	26.25
3	24	23.92	20.63
4	24	24.03	29.06
5	24	23.99	16.41
6	24	24.01	35.39
7	24	24.00	6.91
8	24	24.00	49.63
9	24	24.00	0.00
10	24	24.00	60.00

Table 1: Arrival and Departure Headways ($h = 24$, $d^{(0)} = 25$)

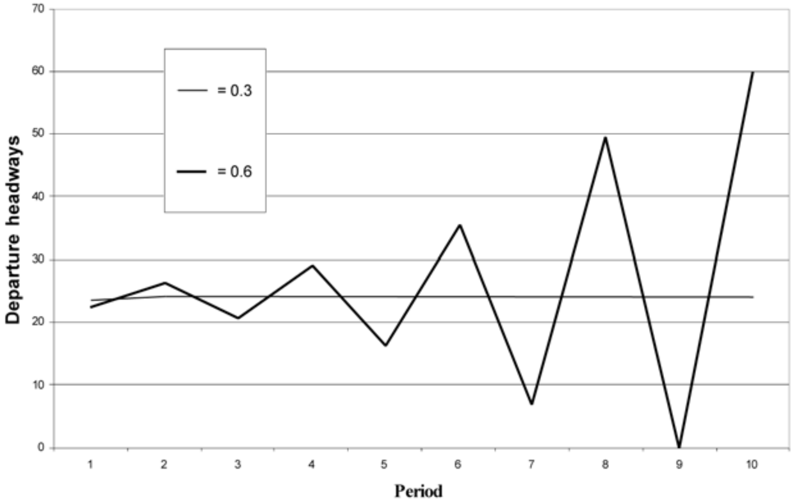


Figure 1: Arrival and Departure Headways (h = 24, $d^{(0)}$ = 25)

When $\sigma = 0.3$, the schedule eventually re-establishes itself. However, when $\sigma = 0.6$, the schedule breaks down irretrievably and we get ship "bunching".

3 STABILITY FOR TWO TERMINALS

This analysis is now extended to the case of two ports, identified by subscripts 1 and 2.

$$d_1^{(n)} = \frac{1}{1-\sigma_1}\, h - \frac{\sigma_1}{1-\sigma_1}\, d_1^{(n-1)}$$

$$d_2^{(n)} = \frac{1}{1-\sigma_2}\, d_1^{(n)} - \frac{\sigma_2}{1-\sigma_2}\, d_2^{(n-1)} = \frac{1}{(1-\sigma_1)(1-\sigma_2)}\, h - \frac{\sigma_1}{(1-\sigma_1)(1-\sigma_2)} d_1^{(n-1)} - \frac{\sigma_2}{1-\sigma_2}\, d_2^{(n-1)}.$$

Define

$$\mathbf{y} = \begin{bmatrix} h/(1-\sigma_1) \\ h/((1-\sigma_1)(1-\sigma_2)) \end{bmatrix}, \mathbf{A} = \begin{bmatrix} \sigma_1/(1-\sigma_1) & 0 \\ \sigma_1/((1-\sigma_1)(1-\sigma_2)) & \sigma_2/(1-\sigma_2) \end{bmatrix}$$

$$\text{and } \mathbf{d}^{(n)} = \begin{bmatrix} d_1^{(n)} \\ d_2^{(n)} \end{bmatrix}.$$

Hence:

$$(5)\ \mathbf{d}^{(n)} = \mathbf{y} - \mathbf{A}\mathbf{d}^{(n-1)}.$$

As before,

$$(6)\ (\mathbf{d}^{(n)} - \mathbf{d}) = \mathbf{A}(\mathbf{d}^{(n-1)} - \mathbf{d})$$

with $\mathbf{d} = \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}$.

Stability requires that the determinant of **A** is less than one, which in this case means that $\det(\mathbf{A}) = \frac{\sigma_1\sigma_2}{(1-\sigma_1)(1-\sigma_2)} < 1$. However, this is a *necessary* rather than a *sufficient* condition, as it may be possible for $\frac{\sigma_1}{1-\sigma_1} > 1$, $\frac{\sigma_2}{1-\sigma_2} < 1$, and $\frac{\sigma_1\sigma_2}{(1-\sigma_1)(1-\sigma_2)} < 1$. The departure headway from the first port is unstable and ship bunching will arise.

Table 2 shows the results for two ports in series, when at the first terminal $h = 24$ and $d^{(0)} = 25$.

		$\sigma_1 = 0.3$, $\sigma_2 = 0.3$		$\sigma_1 = 0.6$, $\sigma_2 = 0.3$	
n	h	$d_1^{(n)}$	$d_2^{(n)}$	$d_1^{(n)}$	$d_2^{(n)}$
1	24	23.57	33.67	22.50	32.14
2	24	24.18	20.12	26.25	23.72
3	24	23.92	25.55	20.63	19.30
4	24	24.03	23.38	29.06	33.25
5	24	23.99	24.24	16.41	9.19
6	24	24.01	23.90	35.39	46.62
7	24	24.00	24.04	6.91	0.00
8	24	24.00	23.99	49.63	70.90
9	24	24.00	24.01	0.00	0.00
10	24	24.00	24.00	60.00	85.71

Table 2: Arrival and Departure Headways for Two Ports in Series

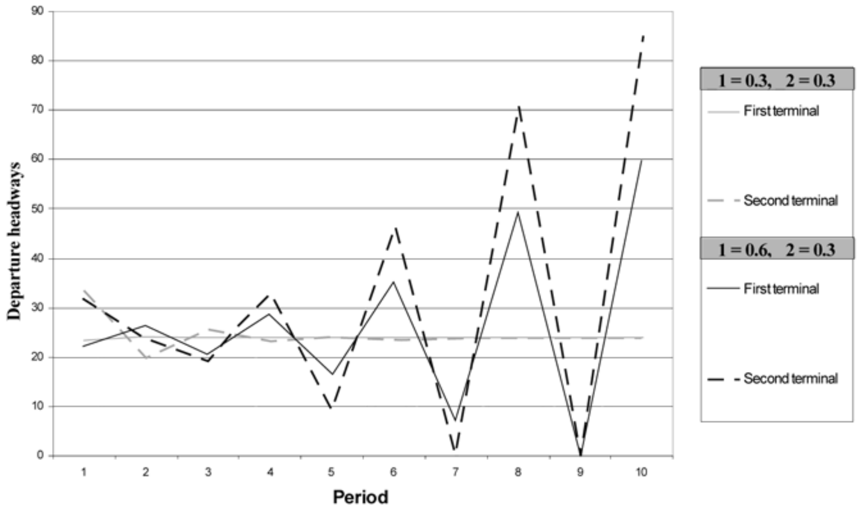


Figure 2: Arrival and Departure Headways for Two Ports in Series

It is evident that deviations from schedule are magnified as the ship progresses from the first to the second terminal. However, when $\sigma_1 = 0.3, \sigma_2 = 0.3$, operations gradually return to the schedule. When $\sigma_1 = 0.6, \sigma_2 = 0.3$, bunching arises although $\frac{\sigma_1 \sigma_2}{(1-\sigma_1)(1-\sigma_2)} = 0.6429 < 1$ (departure headways are set to zero when they would otherwise be negative, implying that ships cannot overtake each other).

4 STABILITY FOR *n* TERMINALS

The above argument for two ports generalizes for n terminals. In this case, stability would require $\frac{\sigma_i}{(1-\sigma_i)} < 1$ for $i = 1 \ldots n$.

4.1 Stochastic Stability

In the preceding, we assumed that the arrival headway at the first port is a constant h. We now assume that the actual headway varies randomly around a mean value of h. Thus for the first stop

$$(7)\ (d^{(n)} - d) = \frac{1}{1-\sigma}(h^{(n)} - h) - (\frac{\sigma}{1-\sigma})(d^{(n-1)} - d).$$

Define $x^{(n)} = d^{(n)} - d$ and $y^{(n)} = h^{(n)} - h$. Then

$$(8)\ x^{(n)} = \frac{1}{1-\sigma}y^{(n)} - (\frac{\sigma}{1-\sigma})x^{(n-1)}$$
$$= \frac{1}{1-\sigma}y^{(n)} - (\frac{\sigma}{1-\sigma})(\frac{1}{1-\sigma}y^{(n-1)} - (\frac{\sigma}{1-\sigma})\ x^{(n-2)})$$
$$= \frac{1}{1-\sigma}\ (y^{(n)} + (\frac{-\sigma}{1-\sigma})\ y^{(n-1)} + (\frac{-\sigma}{1-\sigma})^2\ y^{(n-2)} +\ldots+ (\frac{-\sigma}{1-\sigma})^n\ y^{(0)}) + (\frac{-\sigma}{1-\sigma})^n\ x^{(0)}$$

Let $v_d = E\{(x^{(n)})^2\}$ and $v_h = E\{(y^{(n)})^2\}$. Assuming that the series of arrival headways at the first port, namely $y^{(0)}, y^{(1)}, \ldots$, is not auto correlated and that $(\frac{-\sigma}{1-\sigma})^n\ x^{(0)}$ vanishes as n tends to infinity, we obtain for large n

$$(9)\ v_d = \frac{v_h}{1-2\sigma}.$$

This follows because

$$(10)\ (\frac{1}{1-\sigma})^2(1+(\frac{-\sigma}{1-\sigma})^2+ (\frac{-\sigma}{1-\sigma})^4+\ldots) = \frac{1}{1-2\sigma}$$

provided the series is convergent (provided $\sigma < 0.5$). We see that the variance of the departure headway is always greater than the variance of the arrival headway (since $\sigma > 0$) and that the variance of the departure headway tends to infinity as σ tends to 0.5 from below. The system is therefore stochastically stable provided $\sigma < 0.5$.

This result may unfortunately not be applied recursively along the route of a container liner, as the series of arrival headways at the second port is autocorrelated. For the second port (where the subscript denotes the port)

$$(11)\quad \begin{aligned} x_2{}^{(n)} &= \frac{1}{1-\sigma_2}x_1{}^{(n)} - (\frac{\sigma_2}{1-\sigma_2})x_2{}^{(n-1)} \\ x_1{}^{(n)} &= \frac{1}{1-\sigma_1}y^{(n)} - (\frac{\sigma_1}{1-\sigma_1})x_1{}^{(n-1)} \end{aligned}$$

In this case

$$(12)\ x_2{}^{(n)}$$
$$=\frac{1}{1-\sigma_2}(x_1^{(n)}+(\frac{-\sigma_2}{1-\sigma_2})x_1^{(n-1)}+(\frac{-\sigma_2}{1-\sigma_2})^2x_1^{(n-2)}+\ldots+(\frac{-\sigma_2}{1-\sigma_2})^n x_1^{(0)})+(\frac{-\sigma_2}{1-\sigma_2})^n x_1^{(0)}$$

Let $v_1 = E\{(x_1^{(n)})^2\}$ and $v_2 = E\{(x_2^{(n)})^2\}$. In this case it can be shown that

$$(13)\ v_2 = \frac{1}{1-2\sigma_2}(1+2\frac{\sigma_1\sigma_2}{1-\sigma_1-\sigma_2})v_1$$

because

$$(14)\ E\{(x_1^{(n)})(x_1^{(n-m)})\} = (\frac{-\sigma_1}{1-\sigma_1})^m v_1,\ \forall m > 0$$

which in turn follows from

(15) $E\{(y^{(n)})(x_1^{(n-m)})\} = 0, \forall m > 0$

Unfortunately, (13) cannot be applied recursively for the third (or subsequent) ports as

(16) $E\{(x_1^{(n)})(x_2^{(n-m)})\} \neq 0, \forall m > 0$

Table 3 compares simulation with analytic results. It is assumed that container ships follow a daily routine with one arrival at each port every 24 hours. It is assumed that the arrival headway at the first port can vary by up to +/– 1 hour, with a uniform distribution, giving a variance of 0.3387 h^2. There are no other sources of random variation in this model. At each port, it is assumed that the rate of arrivals of containers is 1/3 the loading rate, so $\sigma_1 = \sigma_2 = \sigma_3 = 1/3$. The simulated arrival headway variance at the second port magnifies to 0.8333 h^2. The variance calculated by (9) is in good agreement with the simulated value. At the third port, the arrival headway variance magnifies again to 2.9950 h^2, in good agreement with the value calculated by (13). By the time the fourth port is reached, what was initially a small headway perturbation has become huge, having a variance of 13.7513 h^2.

Headways	*Mean (h)*	*Simulated variance (h^2)*	*Calculated variance (h^2)*
Arrival at 1st port	24.0151	0.3387	
Arrival at 2nd port	24.0147	0.8333	0.8467 (from equ. 9)
Arrival at 3rd port	24.0141	2.9950	3.0693 (from equ. 13)
Arrival at 4th port	24.0139	13.7513	

Table 3: Arrival Headway Variance for Three Ports in Sequence ($\sigma_1 = \sigma_2 = \sigma_3 = 1/3$)

If the loading rate can be speeded up to four times the arrival rate of containers, the effect on stability is significant. When $\sigma_1 = \sigma_2 = \sigma_3 = 1/4$, we obtain the results in Table 4.

Headways	*Mean (h)*	*Simulated variance (h^2)*	*Calculated variance (h^2)*
Arrival at 1st port	24.0151	0.3387	
Arrival at 2nd port	24.0148	0.6689	0.6774 (from equ. 9)
Arrival at 3rd port	24.0143	1.6537	1.6934 (from equ. 13)
Arrival at 4th port	24.0138	4.8555	

Table 4: Arrival Headway Variance for Three Ports in Sequence
($\sigma_1 = \sigma_2 = \sigma_3 = 1/4$)

The simulated arrival headway variance at the fourth port is reduced from 13.7513 h^2 to 4.8555 h^2, with calculated variances at the second and third ports being in good agreement with the simulated values.

5 CONCLUSIONS

Taking the unrealistic case of a shipping line calling at equidistant ports, schedule stability requires that loading be twice as fast as the arrival of containers at the terminal. In reality, travel times between ports will vary. Nonetheless, it is evident the schedule stability depends critically on the speed of loading and unloading.

Even where schedules are stable over time, the variance of arrival headways can grow explosively along the route. The rate of growth of arrival headway variance may, however, be reduced by speeding the rate at which containers are loaded and unloaded.

Hence we see that the performance of the quay crane is essential to the stability of ship schedules. This confirms the importance of quay crane performance in the context of ship and port operations.

REFERENCES

Newell, G.F. and Potts, R.B. (1964) "Maintaining a bus schedule". Proc., Second Conference. Australian Road Research Board, Melbourne, Vol. II, pp. 388–393.

Nicholson, A. and Kong, M.H. (2004) "Assessing the Effect of Congestion on Bus Service Reliability". The Second International Symposium on Transportation Network Reliability, New Zealand, pp. 21–27.

CHAPTER 8

PREDICTING THE PERFORMANCE OF CONTAINER TERMINAL OPERATIONS USING ARTIFICIAL NEURAL NETWORKS

Richard Linn

Boeing 787 Program, Everett, WA 98204-1710, USA

Jiyin Liu

Business School, Loughborough University, Leicestershire LE11 3TU, UK

Yat-wah Wan

National Dong Hwa University, Hualien, Taiwan

Chuqian Zhang

Information Technology, Columbia University, New York, USA

Abstract
With high average quay crane (QC) rate generally associated with short vessel turnaround times and minimum operations delays, the QC rate is often adopted as the performance indicator by container terminals. It is frustrating for container terminals to realize only in retrospect the decrease of the QC rate but lose the opportunity to reverse the trend. In this study, we identify factors that affect the QC rate. Based on these factors we develop artificial neural network (ANN) models to predict the QC rates of the next planning period, for both the overall rate of a container terminal and the individual rates of specific vessel types. The models are trained and tested using data collected from container terminals in Hong Kong. The results show that the average relative prediction error is small, especially for the models predicting QC rates of specific vessel types. Such predictions also lead to possible remedial actions to increase the QC rates.

1 INTRODUCTION

Container terminals play a critical role in global transportation. Their effective operation ensures orderly flows of containers between ocean-going vessels and landside transportation. Operation in a container terminal includes the gate house, the quayside, and the container storage yard processes and the latter two represent the majority of physical container handling activities. Figure 1 shows schematically the operations of a container terminal (Zhang *et al.*, 2003).

Vessels bring in inbound containers. When a vessel is berthed, inbound containers are discharged from the vessel by the quay cranes (QCs) and transported by the internal trucks (ITs) to their storage blocks in the yard. When a container arrives at its storage block, a yard crane (YC) lifts up the container from the IT and puts it in the block for temporary storage. Consignees then send external trucks (XTs) to the terminal to pick up the inbound containers. When an XT comes to a storage block, the YC there retrieves the required container and places it onto the XT which takes the container out of terminal through the gate house.

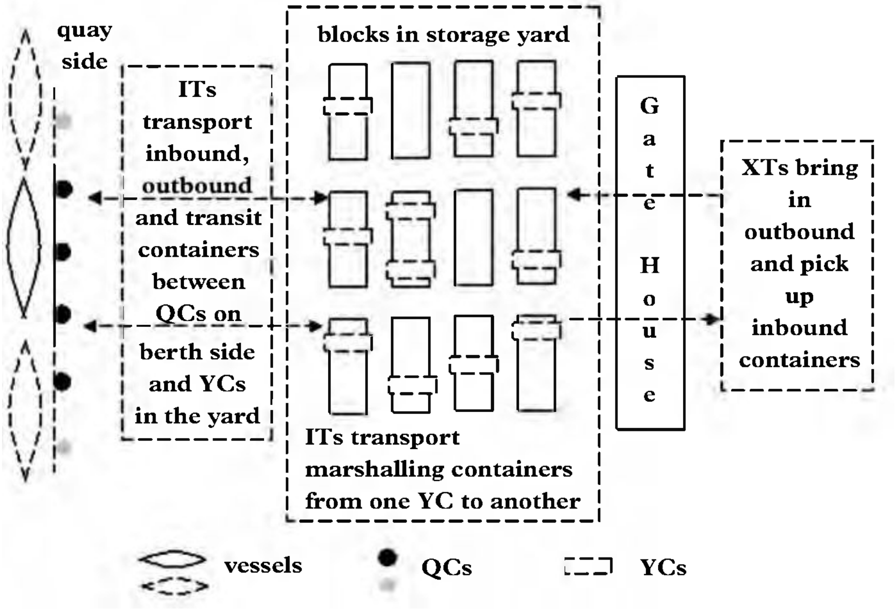

quay side
ITs transport inbound, outbound and transit containers between QCs on berth side and YCs in the yard
blocks in storage yard
ITs transport marshalling containers from one YC to another
Gate House
XTs bring in outbound and pick up inbound containers
vessels
QCs
YCs

Figure 1: A Schematic Diagram of a Container Terminal

Outbound containers flow in the reversed direction. They are sent in by XTs from shippers and stored by YCs in a block. When their vessel is berthed, the outbound containers are retrieved again by the YCs and transported by the ITs to the QCs for vessel loading. Transit containers are brought in by a vessel, stored in the yard, only for transit onto its next vessel. Containers stored in the yard may be relocated, or marshalled, to different locations in the yard to streamline future operations. Marshalling a container requires an IT trip between the two locations and two YC moves for retrieving and storing the container at the origin and the destination, respectively.

Terminal operations involve many decisions, such as assigning berths and QCs to arriving vessels, assigning storage space for incoming containers, scheduling YCs and ITs, deciding plans for marshalling moves, etc. The operations and the decisions involved in different areas of a terminal interact with each other. Due to the scale and complexity of the terminal operations, it is impossible to make all decisions altogether in one model to optimize the performance of a terminal. To simplify the operations problem and to make feasible decisions, a hierarchical and distributed approach is often adopted. Longer-term and global decisions concerning the whole terminal are made first. With known results from these decisions, more short-term and local decisions concerning a specific area or function are then made. Such an approach usually works well to keep smooth operations of the terminal. For detailed description of terminal operations, decision problems and previous research on different specific decision problems, see Vis and de Koster (2003), Steenken *et al.* (2004) and Murty *et al.* (2005).

From shipping lines' perspective, the performance of a terminal is measured by vessel turnaround times. To incorporate the objective of shipping lines into theirs, terminals often use the (overall) *quay crane* (QC) *rate* as a unified performance indicator for the terminal efficiency. Suppose that in a given period the total number of containers, N, loaded onto and discharged from the vessels and the total QC working hours spent, T, are known. Then the QC rate is the ratio of N to T. There can be a QC rate defined for a specific vessel type. In that case, the QC rate of type i vessels is the ratio of N_i to T_i, where N_i is the total number of containers loaded onto and discharged from type i vessels, and T_i is the total QC working hours spent on type i vessels.

The performance of terminal operations, as reflected in QC rates, fluctuates. Sometimes the fluctuations, such as that induced by changes of workload over time, are known ahead of time. However, more often than not once a low performance is observed it is too late to correct, leaving the terminal operating in low efficiency.

In this chapter we propose to tackle the problem by predicting the terminal performance. Driven by the practical needs in Hong Kong container terminals, the goal of this study is to provide a satisfactory prediction of terminal performance, so that preventive remedial actions can be taken if the performance is going to be poor. Rule-base procedures and variants of linear regression have been tried in practice to such a prediction-correction problem without leading to concrete results. The main hurdle is the complex relationships among the variables in the terminal operations. Such relationships are not only non-linear but also difficult to describe by any simple functions. Before any sensible predication can be made, the modelling and the characterization of these relationships are already difficult when done using rules or regression models. Instead of relying on rules or regression we adopt an artificial neural network (ANN) approach to predict the future QC rate from the current available data. This approach captures the non-linear interaction of variables through searching, with historical data fed in, the best parameter values of an ANN. Conceptually an ANN can fit to any amount of data to any degree of accuracy, subject to the allowable computation effort. The approach has been applied to classifications, pattern recognition, optimization and prediction for problem contexts as diversified as business, engineering design, medical diagnoses, agriculture, etc. See, for example, references in Du *et al.* (2002), Magdon-Ismail and Atiya (2002), Mena (2003), Ray *et al.* (2005), Wong *et al.* (2000), Zhao *et al.* (2003) and Kominakis *et al.* (2002) for various applications; see, for example, Murray (1995), Mehrotra *et al.* (1997) and Haykin (1999) for the systematic development of the theories of ANN.

The remainder of the chapter is organized as follows. First, we identify the input factors affecting the QC rates in the next section. The structure of the ANN models and the training method are then presented. Subsequently we evaluate the performance of the ANN models and suggest ways of using the models to identify remedial actions. Finally conclusions are drawn.

2 IDENTIFICATION OF INPUT FACTORS

For prediction purposes, we divide an operation day into a number of basic periods. Our task in each period is to predict the QC rates in the next period, both for the overall rate and for the rates of specific vessel types. To develop such a model, we need to identify factors affecting the QC rates with information obtainable in the current period. We worked closely with the terminals in Hong Kong port analysing the operations flow and data records. The analysis leads to the following principles for determining the input factors of the prediction model:

- an input factor should have a significant impact on the QC rate;
- the total number of input factors must be manageable;
- the factors should be representative for the status of the whole terminal (even though some factors may be in an aggregate form); and
- the factors can be obtained from information available in the current period.

The execution of the principles appears to be an art rather than a science. The amount and status of equipment is easy to keep track of. However, the activities and factors in a container terminal interlock so much that one can never quantify the actual effect of such equipment on the performance of a container terminal. Some factors for the container terminal, e.g. the intensities of activities, are intangible in nature such that any tangible indictors are at best approximation for such factors. Moreover, the appropriate number and the best forms of input factors are just a matter of choice. With rounds of discussion and testing, eventually we settle on a total about 20 input factors.

In the next two subsections, we first describe the development of the ANN model for prediction of the overall QC rate and then proceed to develop ANN models to predict QC rates of specific vessel types.

2.1 Input Factors for Predicting the Overall QC Rate

Our observation and analysis show that there are three categories of factors affecting the overall QC rate. They are the estimated workload in the predicted period, resources to be deployed in the predicted period, and the container yard status and workload distributions. The term "yard status" is used here to mean the general situation of container storage in the yard.

Since we want a relatively small number of factors, it is not desirable to define input factors for individual storage blocks. Therefore, workloads and resources deployed are expressed in terms of totals for the whole yard. For yard status and workload distributions, again, we need to use a small number of input factors to reflect the density and distributions of container storage. As mentioned above, there is no fixed way to represent such factors. We simply introduce (weighted) average and imbalance measures as aggregated indicators to represent the traffic conditions, the resource utilization and the amount and distribution of workload, which are not easy to measure directly. The input factors of the model are finally selected as listed below.

Workload to be performed

- I_1: the number of containers to be loaded onto vessels during the period.
- I_2: the number of containers to be discharged from vessels during the period.
- I_3: the number of other vessel related moves during the period.
- I_4: the number of containers to be picked up by XTs during the period.
- I_5: the number of containers to be brought in by XTs during the period.
- I_6: the number of outbound containers to be marshalled during the period.
- I_7: the number of inbound containers to be marshalled during the period.

The values of input factors I_1 to I_7 can be read directly from the vessel schedule and the marshalling plan.

Resources to be deployed

- I_8: the number of QCs to be used in the period.
- I_9: the number of YCs to be used during the period.
- I_{10}: the number of ITs to be used for serving QCs.
- I_{11}: the number of ITs to be used for marshalling.

The values of input factors I_8 to I_{11} can be read directly from the resource deployment plan. Input factors I_{12} to I_{18} below are compiled from raw data of yard layout, containers stored in yard, vessel schedule and marshalling plan. Each of these input factors is listed below with its compiling method immediately following.

Yard status and workload distribution

- I_{12}: current weighted average density in the yard (*WAYD*).

Let B be the total number of storage blocks in the yard; B_i be the capacity of block i, $i = 1, 2, \ldots, B$. The density of block i, $D_i = a_i/B_i$, where a_i is the current number of containers in block i. Then

$$WAYD = \sum_{i=1}^{B} (B_i \times D_i) \;/\; \sum_{i=1}^{B} B_\text{i}.$$

- I_{13}: the imbalance of current density in the yard (*IMD*)

$IMD = 1 - (\sum_{i=1}^{B} D_i \;/\; D_{max}) \;/\; B$, where $D_{max} = \max\,(D_1, D_2, \ldots., D_B)$.

A value of *IMD* close to 0 indicates that the block-inventory is evenly distributed and a value of *IMD* close to 1 indicates the sharp difference of block-inventory among all blocks.

Factors I_{12} and I_{13} represent, respectively, the average yard density level in the period and the distribution of container storage among all the blocks.

- I_{14}: the weighted average distance to be travelled between berth and storage block (*WD*).

Let S be the number of vessels served in the planning period; x_{ij} be the number of containers to be discharged from vessel i to block j during the planning period; y_{ij} be the number of containers to be loaded from block j to vessel i during the planning period; and d_{ij} be the distance between (the planned berth for) vessel i and block j, $i = 1, 2, \ldots, S$, $j = 1, 2, \ldots, B$. Then *WD* is defined as follows.

$$WD = \sum_{i=1}^{S}\sum_{j=1}^{B} (x_{ij} + y_{ij})d_{ij} \Big/ (\sum_{i=1}^{\text{s}}\sum_{j=1}^{B} (x_{ij} + y_{ij}).$$

- I_{15}: the imbalance of total workload in the yard (*IMTW*).

$IMTW = 1 - (\sum_{j=1}^{B} (x_j \,/\, x_{max}) \,/\, B$, where x_j is the total workload of block j and $x_{max} = \max\,(x_1, x_2, \ldots, x_B)$.

Input factor I_{15} reflects the situation of storage assignment for all incoming containers.

- I_{16}: the imbalance of vessel workload in the yard (*IMVW*).

Let $x'_j = \Sigma_i\, x_{ij} + \Sigma_i\, y_{ij}$ be the total vessel workload of block j during the planning period and x'_{max} be the maximum x'_j among all blocks. Then

$$IMVW = 1 - (\sum_{j=1}^{B} (x'_j \,/\, x'_{max}) \,/\, B.$$

Input factor I_{16} reflects the storage assignment of vessel related containers.

- I_{17}: mean of proportion of vessel workload in each block in the yard (*MVW*).

Proportion of vessel workload in block i is defined as

$$PRO\_VW_i = \frac{Vessel\ \ workload\ \ in\ \ block\ \ i}{Total\ \ workload\ \ in\ \ block\ \ i}.$$

Then

$$MVW = \frac{1}{B}\sum_{i=1}^{B} PRO\ \_VW_i.$$

- I_{18}: the variance of proportion of vessel workload in each block in the yard (*VVW*)

$$VVW = \frac{1}{B - 1}\sum_{i=1}^{B} (PRO\ \_VW_i - MVW)^2.$$

Input factors I_{17} and I_{18} indicate the amount of vessel related workload accounted in the total workload in a block and its difference among blocks in the yard.

2.2 Input Factors for Predicting QC Rates for Different Types of Vessels

Vessels come in different sizes and shapes; for example, the sizes and shapes of ocean-going vessels are significantly different from those of barges and lighters linking neighbouring river terminals. The QC allocation and the QC rates for different types of vessels can, therefore, be very different even if other conditions are all the same. To obtain more accurate and detailed prediction of QC rates, we develop individual ANN models for different vessel types. In the ANN model for a specific type of vessels, we choose to use the following input factors.

Workload to be performed

- I_1: the number of containers to be loaded to this type of vessel during the period.
- I_2: the number of containers to be loaded to other vessels during the period.
- I_3: the number of containers to be discharged from this type of vessel during the period.
- I_4: the number of containers to be discharged from other vessels during the period.
- I_5: the number of other vessel related moves during the period.
- I_6: the number of containers to be picked up by XTs during the period.
- I_7: the number of containers to be brought in by XTs during the period.
- I_8: the number of outbound containers to be marshalled during the period.
- I_9: the number of inbound containers to be marshalled during the period.

Resource to be deployed

- I_{10}: the number of QCs to be used by this type of vessel in the period.
- I_{11}: the number of QCs to be used by other vessels in the period.
- I_{12}: the number of YCs to be used during the period.
- I_{13}: the number of ITs to be used for serving QCs.
- I_{14}: the number of ITs to be used for marshalling.

Yard status and workload distribution

- I_{15}: the current weighted average density in the yard.
- I_{16}: the current weighted average density of blocks associated with this type of vessel.
- I_{17}: the imbalance of current density in the yard.
- I_{18}: the imbalance of current density of the blocks associated with this type of vessel.
- I_{19}: the weighted average distance to be travelled between berth and storage block for containers from/to this type of vessel.

- I_{20}: the weighted average distance to be travelled between berth and storage block for containers from/to other vessels.
- I_{21}: the mixing of workloads related to different vessels in the blocks (*XWV*).

Let $z_{ij} = x_{ij} + y_{ij}$ be the total number of containers transferred between vessel *i* and block *j* (i.e., containers discharged from vessel *i* to block *j* and loaded from block *j* to vessel *i*), and

$$z_{max} = \max\{z_{ij} \mid i = 1, 2, \dots, S, j = 1, 2, \dots, B\}.$$

Let a_j be the total number of containers in block *j*. For each block *j*, define an index of mixing $m_j = \frac{1}{S}\sum_{i=1}^{S} z_{ij} \Big/ z_{\max}$. Then

$$XWV = \sum_{j=1}^{B} (a_j \times m_j) \Big/ \sum_{j=1}^{B} a_j.$$

A value of *XWV* close to 1 indicates a higher degree of mixing, i.e., the workload in a block is contributed from different vessels. A value of *XWV* close to 0 indicates a lower degree of mixing.

- I_{22}: the mixing of vessel, marshalling, and XTs related workloads in blocks (*XVMX*).

Let L_j be the total workload related to vessels in block *j*, M_j be the total workload related to marshalling in block *j*, and P_j be the total workload related to XTs in block *j*. Define $MAX = \max(L_1, L_2, \dots, L_B, M_1, M_2, \dots, M_B, P_1, P_2, \dots, P_B)$. For block *j*, further define index $W_j = (\frac{L_j}{MAX} + \frac{M_j}{MAX} + \frac{P_j}{MAX}) / 3$. Then,

$$XVMX = \sum_{j=1}^{B} (L_j + M_j + P_j) \times \mathrm{W_j} \Big/ \sum_{j=1}^{B} (L_j + M_j + P_j).$$

XVMX reflects how the three kinds of workloads compete for YCs in the blocks.

- I_{23}: the imbalance of grounding workload in the yard.

Grounding workload is generated by containers brought in by XTs. This imbalance factor is calculated in the way similar to that for the imbalance of vessel workload.

- I_{24}: the imbalance of pickup workload in the yard.

Pickup workload generated by containers picked up by XTs. Its calculation is again similar to calculating the imbalance of vessel workload.

3 DEVELOPMENT OF THE ANN MODEL

3.1 The Structure of the Model

There are different ANN model structures that can be applied for predicting the overall QC rate and the QC rate for a specific vessel type. We adopt the multi-layer feed-forward perceptron ANN trained with error back-propagation (see Rumelhart *et al.*, 1986) for all QC rates prediction. Our models have three layers—the input layer, the output layer and a hidden layer in between. Such a structure is illustrated in Figure 2. The following generic description applies to all the ANN QC rate prediction models.

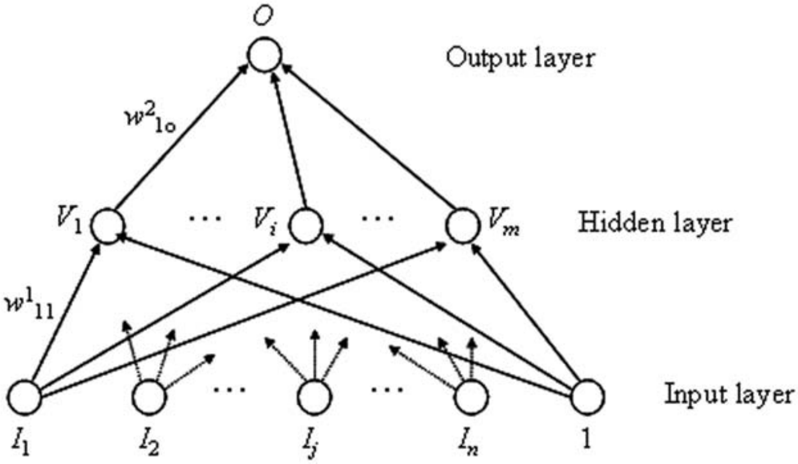


Figure 2: The ANN Structure

The output layer of the ANN has only one node (neuron) giving the QC rate to be predicted. The input layer contains all the input factors identified for predicting this QC rate. A bias node with input 1 is also added to the input layer. Its purpose is similar to that of the constant term in a regression model. The determination of the number of nodes in the hidden layer is more difficult. There is no theoretical method or formulation to determine the optimal number of nodes in the hidden layer. In practice, the trial and error approach is adopted. With too few nodes, the network may not be powerful enough for a given learning task. With a large number of nodes, the computation will be too expensive. Usually one can begin training the ANN either (1) with a large enough number of hidden nodes and then gradually remove them until the performance of the model deteriorates to an unacceptable level, or (2) with a small number of hidden nodes and then gradually increase the number of nodes until the performance of the model becomes acceptable for the application. We adopt the former approach in this study. Naturally, the performance of the model is measured by the deviation between the actual and suggested QC rates for a given collection of training examples.

With this structure the QC rate for a given set of values of the input factors can be predicted in the following way.

$$V_i = \sum_{j=1}^{n} I_j w^1_{ji} + 1 w^1_{1i}, \tag{1}$$

$$VO_i = \frac{1}{1 + \exp(-V_i)}, \tag{2}$$

$$O = \sum_{i=1}^{m} VO_i w^2_{io}, \tag{3}$$

where

I_j: input factor j,
w^1_{ji}: the weight of the link from input node j to hidden node i,
w^2_{io}: the weight of the link from hidden node i to the output node o,
V_i: the net input to hidden layer node i,
VO_i: the net output of hidden layer node i.

All the weights, w^1_{ji} and w^2_{io}, are constants when the ANN is used for prediction. However, their values need first to be derived (trained) from a set of training data which is a set of vectors consisting of input parameters and output $(I_1, I_2, \ldots, I_n, O)$.

All the training and testing samples are represented in a matrix. In the matrix, the last column represents the output and each of the other columns represents an input factor. Each row represents an input pattern p. It is noticed that the values of different input variables may be dramatically different. For example, the imbalance variables have values between 0 and 1 and the workload-related input variables may have values over 1,000. To make the training process faster, we normalize the input vectors by re-scaling each column. For each column (input variable) j, $j = 1, 2, \ldots, n$, the normalized data are obtained as follows:

$$I'_{pj} = \frac{2(I_{pj} - \min_j)}{\max_j - \min_j} - 1, \ p = 1, 2, \ldots, P,$$

where P is the number of input patterns (rows); I_{pj} is the original data in column j, row p; I'_{pj} is the normalized data corresponding to I_{pj}; $\min_j$ is the minimum value in column j; and $\max_j$ is the maximum value in column j.

3.2 Model Training

The back-propagation algorithm is used in training the ANN. See Murray (1995), Mehrotra *et al.* (1997) and Haykin (1999) for the explanation of the algorithm. With an initial set of weights and a given record $(I_{11}, I_{12}, \ldots, I_{1n},$

O_1) of the training data set, the learning mechanism of the ANN first calculates the input and output of each node in the hidden layer using equations (1) and (2); then find the value in the output node O using equation (3). The learning mechanism compares the predicted QC rate with the given one in the training set. The error between these two is propagated back to the hidden layer and then the input layer to adjust the weights. With the updated weights, the second record of the training data is fed into the ANN and the learning mechanism will repeat the process to calculate the input and output values for each node in the hidden layer and in the output layer and the error. If the error is acceptable, the training process stops. Otherwise, the error will be back-propagated again to adjust (update) the weights and the next record of the training data will be fed into the ANN to continue the training.

The back-propagation algorithm is a generalization of the least mean square algorithm that modifies network weights to minimize the mean squared error between the desired and actual outputs of the network. Mean squared error (*MSE*) is defined as follows.

$$MSE = \frac{1}{P}\sum_{p=1}^{P}(O_p - O_{op})^2, \tag{4}$$

where P is the number of input patterns; O_p is the QC rate for input pattern p predicted by the ANN model; and O_{op} is the observed value of QC rate for this input pattern.

Back-propagation uses supervised learning in which the network is trained using data for which inputs as well as desired outputs are known. Once trained, the network weights are fixed and can be used to compute output values for new input samples. One way to minimize the *MSE* is based on the gradient descent method. To do so, the change of a weight w_{ij} is proportional to $-(\partial MSE/\partial w_{ij})$.

The feed-forward process involves presenting an input pattern to input layer nodes that pass the input values on the hidden layer. Each of the hidden layer nodes computes a weighted sum of its inputs using equation (1), passes the sum through its activation function and presents the result to the output layer. In this study, the sigmoid function (equation (2)) is used as the activation function from the input to the hidden layer and linear function (equation (3)) from the hidden layer to the output layer.

For each input pattern $[I_{p1}, I_{p2}, \ldots, I_{pn}]$ (where $p = 1, 2, \ldots, P$), the net input to node i (where $i = 1, 2, \ldots, m$) in the hidden layer is:

$$V_{pi} = \sum_{j=1}^{n} w_{ji}^{1}\, I_{pj}. \tag{5}$$

The output of node i ($i = 1, 2, \ldots, m$) in the hidden layer is:

$$VO_{pi} = \frac{1}{1+\exp(-V_{pi})}. \tag{6}$$

The output of the node in the output layer is

$$O_p = \sum_{i=1}^{m} w_{io}^2 \; VO_{pi}. \tag{7}$$

According to the gradient descent, the weight changes are suggested by the following two equations:

$$\Delta w_{io}^2 = \eta(\frac{-\partial MSE}{\partial w_{io}^2}), \tag{8}$$

$$\Delta w_{ji}^1 = \eta(\frac{-\partial MSE}{\partial w_{ji}^1}). \tag{9}$$

$\frac{-\partial MSE}{\partial w_{io}^2}$ and $\frac{-\partial MSE}{\partial w_{ji}^1}$ can be derived from equations (4)–(7). η is the learning rate. The training algorithm is outlined below.

```
Start with an initial set of weights.
While $MSE$ > preset value (which is calibrated to be 0.8 in pilots runs for
this study):
   For each input pattern $p$, $p = 1, 2, \ldots, P$:
      Compute outputs $O_p$ using equation (5)–(7),
      Modify the weights between hidden and output nodes by $\Delta w_{io}^2$,
      Modify the weights between input and hidden nodes by $\Delta w_{ji}^1$,
   End for;
End while.
```

To avoid bias of the initial parameter values, training is generally commenced with randomly chosen initial weight values. In this study, the initial weights are randomly generated from $U(-0.1, 0.1)$.

There are two approaches to learning: "per-pattern" learning in which the weights are changed after every sample presentation; and "per-epoch" learning in which the weights are updated only after all samples are presented to the network. We use "per-pattern" training in this study because it is simple to implement and the stochastic search of weight space reduces the risk of local minima.

As stated before, the changes in weights are proportional to the negative gradient of the error. This guideline determines the relative changes that must occur in different weights when a training sample is presented, but does not fix the exact magnitudes of the desired weight changes. The magnitude of change depends on the appropriate choice of the learning rate η. A large value of η will lead to rapid learning but the weight may then oscillate, while low values imply slow learning. The right value of η will depend on the application. In this study, based on the computation experience, η is initially set at 0.005 and as computation proceeds, it is adjusted by the following heuristic: increase η by a fixed amount of 0.003 at every iteration that improves performance by some significant amount (8%); decrease η by a fixed amount of 0.003 at every iteration that worsens performance by some significant amount (8%).

Back-propagation may lead the weights in an ANN to a local minimum of the *MSE* that is substantially different from its global minimum, the best choice of weights. To prevent the network from getting stuck in some local minimum, we make the weight changes dependent on the average gradient of *MSE* in a small region rather than the precise gradient at a point. However, calculating averages can be an expensive task. A short cut, suggested by Rumelhart *et al.* (1986), is to make weight changes in the $(t+1)^{\mathrm{th}}$ iteration of the back-propagation algorithm dependent on immediately preceding weight changes which were made in t^{th} iteration. This has an averaging effect, and reduces the drastic fluctuations in weight changes over consecutive iterations.

Given a large network, it is possible that repeated training iterations successively improve performance of the network on training data, e.g. by "memorizing" training samples, but the resulting network may perform poorly on other data. This phenomenon is called over-training. There are various techniques that avoid over-training. See Prechelt (1998) for a discussion and empirical study of these methods. One solution to avoid over-training is to constantly monitor the performance of the network on test data on which the system has not been trained. Neural learning is considered successful only if the system can perform well on the test data. We emphasize the capability of a network to generalize "rules" from input training samples, not to memorize data only. Therefore, in this study each time after all the training samples are presented to the network, a test set is presented to the network. The weights are adjusted on the basis of the training set only, but the error is monitored on the test set. The training continues as long as the error on the test set is decreasing, and is terminated if the error on the test set increases or reaches a preset value. Actually, with this stopping criterion, final weights are validated with the test data in an indirect manner. Since the weights are not obtained from the current test data, it is expected that the network will continue to perform well on further test data.

3.3 Prediction Experiment and Remedial Actions

Three ANN models are developed and trained, one for the overall QC rate, one for QC rates of lighter/barge (LTBG), and one for non-self-sustained cellular (NSSC). We collect half a year's data from a Hong Kong terminal. The data set contains 2,060 patterns for the overall model, 7,640 patterns for the LTBG model and 1,370 patterns for the NSSC model. Around 70% of the data are used as training data set; 24% are used as test data in the training process. Once the training is finished, the ANN is ready for use. We use the remaining 6% of data to evaluate the performance of the ANN models. The test data and evaluation data are taken from every month proportionally and within each month they are chosen randomly. As listed in the last two sections, including the bias node the number of input nodes in the overall model is 19 and that in the model for a specific vessel type is 25. The number of nodes in hidden layer of the overall model is eventually set to 10, those for the LTBG model and NSSC model to 30 and 10, respectively.

Overall QC rate prediction

The ANN model is applied to predict the overall QC rate for each record in the evaluation data set. We measure the performance of the ANN on a record *i* by the relative error (RE) defined as follows:

$$RE_i = \left|\frac{\text{Predicted QC rate}(i) - \text{true QC rate}(i)}{\text{Predicted QC rate}(i)}\right|.$$

The performance of the ANN on the whole evaluation data set is measured by the average relative error:

$$ARE = \frac{1}{N}\sum_{i=1}^{N} RE_i,$$

where N is the total number of records in the evaluation data set. Such measures do not differentiate over-prediction from under-prediction of the QC rates. While the two cases can have different economic implications, we treat the errors on both sides equally at this stage as the primary purpose is to predict accurately.

Our experiment results show that about 43% of the records have the prediction error RE_i less than 5%, 23% of the records have the prediction error between 5–10%, and 34% of the records have the prediction error larger than 10%. The average relative error ARE is 8.15%. The performance may be improved by increasing the size of training data set, or further refining of the model structure. However, because this model tries to give a prediction on the overall QC rate of all types of vessels but the types of vessels berthed may change significantly from period to period, the further improvement on the performance may be limited. We expect the ANN models for specific vessel types to give better performances.

QC rate prediction for specific vessel types

There are actually five types of container vessels visiting the terminal. We chose to train specific ANN models for two common types, NSSC and LTBG, because there are sufficient data in the data set for them. After training and with the network weights fixed, we test the performance of the ANN models using the evaluation data sets. The average relative error is 2.1% for NSSC and 3.1% for LTBG. The distributions of prediction error RE_i for LTBG and NSSC are shown in Table 1.

	RE_i<3%	3%≤RE_i≤5%	RE_i>5%	*ARE*
NSSC	82.0%	12.0%	6%	2.1%
LTBG	77.9%	9.3%	12.8%	3.1%

Table 1: Prediction Errors of the Models for LTBG and NSSC

Clearly, the ANN models specifically developed for predicting QC rates of different types of vessels give much more accurate results than the model for overall QC rate. The following are two possible reasons for this.

The inputs to the vessel specific model are more detailed than that of the overall model. The training data set for the ANN for a vessel type has separated the data for the particular vessel from those of all other vessels. Hence the inputs include more pertinent information about the QC rate prediction of that particular vessel type.

For the overall model, the inputs are the averages of the information for all vessels in the predicted period. The variations of the vessel types from period to period make the average QC rate hard to predict. In addition, there is only one average data record in each period and hence the data for the overall model are limited. More data are needed to improve prediction accuracy of the overall model.

In summary, ANN is an effective tool for QC rate prediction. There is still potential to further improve the accuracy of QC rate prediction. Two possible ways are further refining the input data definitions to better reflect the dynamics of terminal operation and increasing the size of training data set.

3.4 Remedial Actions to Improve Efficiency of Terminal Operation

An important purpose of the QC rate prediction is to provide warnings of potential poor operations efficiency in the next period and to identify and take remedial actions to achieve better efficiency. The ANN models are not only a tool for QC rate prediction but also useful in identifying and verifying remedial actions.

Since the QC rate depends on the input factors, the remedial actions should be related to changing the values of the input factors. The inputs to the ANN model are related either directly or indirectly to the resource allocations in the yard. Some inputs, such as number of ITs for marshalling, can be altered directly. Others, such as distances for transporting containers between berths and blocks may only be altered by changing the space assignment plan or marshalling plan. As the first step we identify the input factors that can be directly adjusted, and for such factors we determine their ranges of adjustment. When a poor QC rate performance is predicted, we can make possible changes on the adjustable inputs and use the ANN models to estimate the effect on the QC rates. Figure 3 illustrates the method for identifying the input changes to improve the QC rates.

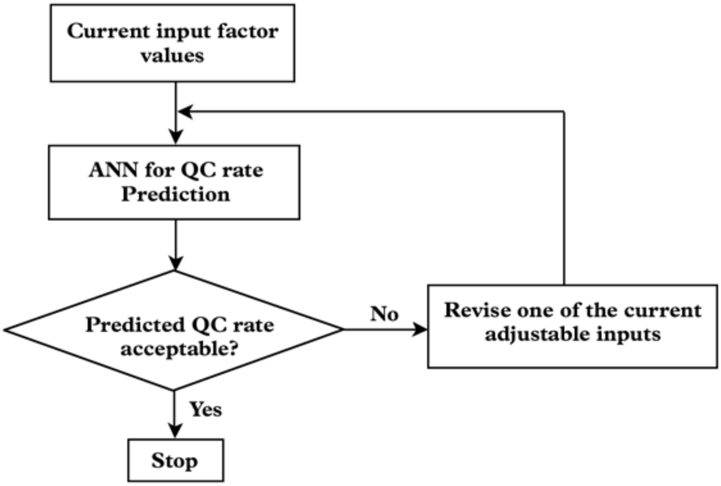

Current input factor values
ANN for QC rate Prediction
Predicted QC rate acceptable?
No
Revise one of the current adjustable inputs
Yes
Stop

Figure 3: The Method of Identifying Changes on Adjustable Inputs

After the input changes are identified, remedial actions can be determined and taken to implement these input changes. In this way poor QC rates can be avoided.

4 CONCLUSIONS

In this chapter we reported a study on predicting the performance of container terminal operations. QC rates were chosen as the performance indicator. We first identified potential factors affecting the overall QC rate and the QC rates for specific vessel types. Based on these we developed artificial neural network models to predict the QC rates in the next period. The models were trained using data collected from a container terminal in Hong Kong. A different data set from the same terminal was used to evaluate the performance of the ANN models. The results showed that the average prediction error is small. In particular the prediction by the models for specific vessel types was very accurate with average relative error of 2.1% and 3.1% for two common types of vessels tested. We also suggested a way of using the models to identify possible remedial actions to improve the QC rate in case a poor QC rate was predicted. The models were developed for applications in normal daily operations to avoid poor performance. In case of the terminal operations being affected by security measures or incidents, the models may also be used to suggest remedial actions.

REFERENCES

Du, K.L., Lai, A.K.Y., Cheng, K.K.M. and Swamy, M.N.S. (2002). "Neural methods for antenna array signal processing: A review". *Signal Processing* 82(4), 547–561.

Haykin, S. (1999). *Neural Networks: a Comprehensive Foundation*. Prentice Hall, NJ.

Kominakis, A.P., Abas, Z., Maltaris, I. and Rogdakis, E. (2002). "A preliminary study of the application of artificial neural networks to prediction of milk yield in dairy sheep". *Computers and Electronics in Agriculture* 35(1), 35–48.

Magdon-Ismail, M. and Atiya, A. (2002). "Density estimation and random variate generation using multilayer networks". *IEEE Transactions on Neural Networks* 13(3), 497–520.

Mehrotra, K., Mohan, C.K. and Ranka, S. (1997). *Elements of Artificial Neural Networks*. MIT Press, Cambridge, MA.

Mena, J.B. (2003). "State of the art on automatic road extraction for GIS update: a novel classification". *Pattern Recognition Letters* 24(16), 3037–3058.

Murray, A.F. (ed.) (1995). *Applications of Neural Networks*, Kluwer Academic Publishers.

Murty K.G., Liu, J.Y., Wan, Y.-w. and Linn, R. (2005). "A decision support system for operations in a container terminal". *Decision Support Systems* 39(3), 309–332.

Prechelt, L. (1998). "Automatic early stopping using cross validation: quantifying the criteria". *Neural Networks* 11 (4), 761–767.

Ray, S.S., Bandyopadhyay, S., Mitra P. and Pal, S.K. (2005). "Bioinformatics in neurocomputing framework". *IEE Proceedings—Circuits Devices and Systems* 152(5), 556–564.

Rumelhart, D.E., Hinton, G.E. and Williams, R.J. (1986). "Learning internal representations by error propagation". In: Rumelhart, D.E. and McClelland, J.L. (eds), *Parallel Distributed Processing*. 1, Chapter 8, MIT Press, Cambridge, MA.

Steenken, D., Voss, S. and Stahlbock, R. (2004). "Container terminal operation and operations research—a classification and literature review". *OR Spectrum* 26(1), 3–49.

Vis, I.F.A. and de Koster, R. (2003). "Transshipment of containers at a container terminal: An overview". *European Journal of Operational Research* 147(1), 1–16.

Wong, B.K., Lai, V.S. and Lam, J. (2000). "A bibliography of neural network business applications research: 1994–1998". *Computer and Operations Research* 27(11–12), 1045–1076.

Zhang, C.Q., Liu, J.Y., Wan, Y.-w., Murty, K.G. and Linn, R.J. (2003). "Storage space allocation in container terminals". *Transportation Research Part B—Methodological* 37(10), 883–903.

Zhao, W., Chellappa, R., Phillips, P.J. and Rosenfeld, A. (2003). "Face recognition: A literature survey". *ACM Computing Surveys* 35(4), 399–459.

CHAPTER 9

CONTAINER TERMINAL OPERATIONS UNDER THE INFLUENCE OF SHIPPING ALLIANCES

Xiaoning Shi

University of Hamburg, Institute of Information Systems, Von-Melle-Park 5, 20146 Hamburg, Germany, and Shanghai Jiao Tong University, Shanghai, China

Stefan Voß

University of Hamburg, Institute of Information Systems, Von-Melle-Park 5, 20146 Hamburg, Germany

Abstract

Nowadays there is a trend to establish new business linkages and alliances within the shipping industry together with customers, suppliers, competitors, consultants and other companies. Notably these include terminal operators in major ports worldwide. A number of studies have attempted to explain this phenomenon occurring in the liner shipping industry using a variety of conceptual and theoretical frameworks. We focus on liner shipping strategic alliances and their influence on container terminal operators. Regarding alliances we briefly discuss the motivations of short-run cooperation among several liner carriers, analyse the pros and cons of being members of liner shipping strategic alliances, and advise on ways to maintain long-term alliance stability by increasing benefits and decreasing risks and drawbacks. Moreover, how do these alliances influence container terminal operators, if there is an influence at all, and what are the possible scenarios for mutual advantages? Our goal is to survey possible issues regarding shipping alliances and their influences on terminal operators.

1 INTRODUCTION

Even in the simplest supply chain, setting the linkage between liner shipping companies and port operators can be regarded as demand and supply-oriented upstream and downstream partnering. Liner vessels visit ports as customers and their desire is driven according to their schedules as well as their hinterland shippers and technology developments. Port operators use every effort to meet the demands and could attract more and more ships by, e.g. good reputation, reliability and agile responses. Thinking about logistic networks in depth, liner shipping transportations and ports obviously act as threads and nodes (i.e. routes or lines and ports) individually, which build up logistics and supply-chain networks. Any minor improvements to the threads or nodes, such as faster mega vessels or newly designed handling cranes, could decrease, e.g. time-oriented measures such as total flow times or lead times within the logistics network and increase customer satisfaction.

A more efficient logistics network would certainly be gained by avoiding bottlenecks in the network (Brennan, 2001) and by harmonizing liner transportation and port operation. Based on this, there are strong links among liner shipping companies and container terminal operators, no matter whether they are regarded as customer-supplier or thread-node. That is, port operators should take into account those linkages independently from considering short-term operations or long-term strategies. The inevitable trend of liner shipping strategic alliances together with dynamic membership pushes port operators towards rechecking their marketing instruments, handling schedule, service provisions, data interchange and information system management and integration, etc.

Many researchers are discussing port operation performance, especially under the influence of liner shipping conferences or alliances. From a global perspective it seems beneficial to distinguish between port economics and shipping economics, although the interdependencies turn out to be of utmost importance. That is, many issues relating to the port industry cannot be investigated without taking into account shipping companies and the shipping industry as its main customers (*cf.* Cullinane, 2005). Various important trends are pushing the port and shipping industries and those players within them towards rethinking and reshaping their service networks (Notteboom, 2004). These trends include globalization, deregulation, logistics integration and containerization. Moreover, regionalization and associated hinterland concepts need to be taken into account also (Notteboom and Rodrigue, 2005).

Despite globalization, various areas show individual characteristics such as European ports versus so-called Asian models. For instance, Wang *et al.* (2004) address Shanghai (China) and Song (2002) discusses Hong Kong's role as the gateway to and from China and the port's competition in the Pearl River delta. Meanwhile, the development of Busan (Korea) is also a valuable example as an emergence of so-called mega ship ports (Fremont and Ducruet, 2005).

A very comprehensive treatment of the economics of sea port container handling is provided by Vanelslander (2005). Some further references can be found in Ninnemann (2006). More general concerns are treated by Blauwens *et al.* (2006). With the ever increasing containerization the number of sea port container terminals and the competition among them has become quite remarkable. An up-to-date survey and literature review on container terminal operations with an operations research focus is provided by Steenken *et al.* (2004).

In this chapter we consider container terminal operations under the influence of liner shipping strategic alliances. The focus here is to provide a rough overview and to discuss opportunities as well as possible risks and pitfalls. The following sections are devoted to the description of shipping alliances, container terminal operators as well as their linkage.

2 LINER SHIPPING CARRIERS: BEHAVIOURS AND TRENDS

2.1 Vessel Types, Fleet Composition and Major Trade Lanes

Different types of ships are considered by shipping lines (see, e.g. Steenken *et al.*, 2004). While the number of container vessels has increased during the last decade the most significant change has been the increase in vessel size (Slack *et al.*, 2002) with deep-sea vessels with a loading capacity of up to 8,000 container units (TEU, 20-ft equivalent units) and beyond. They were being deployed by the end of the 1990s, and serve the main ports worldwide. Those 8,000 TEU vessels are about 320 metres long with a breadth of 43 metres and a draught of 13 metres; on deck containers can be stowed eight tiers high and 17 rows wide, in the hold nine high and 15 wide. Feeder vessels with a capacity of 100 to 1,200 TEU link smaller regional ports with the oversea ports delivering containers for deep-sea vessels. Inland barges are used to transport containers into the hinterland on rivers and channels.

Generations	*Type of vessels*	*TEU*	*Speed (knots)/ percentage that speed applied*
1. 1960s	17,000–20,000 DWT	700–1,500	15–19/58%
2. 1970s	40,000–50,000 DWT	1,500–2,500	18–21/70%
3. late 1970s	Approximately 70000 DWT, Panamax	2,500–4,000	20–24/90%
4. late 1980s to early 1990s	Panamax	4,400–5,000	23–25
5. 1996–1998	Post-Panamax (VLCS)	6,400–7,200	24–26
6. since 1999	Post-Panamax (VLCS)	8,000 and beyond	24–26
7. after 2009	Suez-Max (ULCS)	12,500–13,000	25–26 expected
	Post-Suez-Max	18,000	
	Post-Malacca-Max		

Table 1: Container Ship Generations (DWT: deadweight tonnage, VLCS/ ULCS: very/ultra large container ships)

Source: own composition from *http://info.jctrans.com/wl/hy/hyzs/2006726279397.shtml*, *http://www.nacks.com.cn/shiplist/5400dwt.htm*, *http://www.globalsecurity.org/military/systems/ship/container-types.htm*

Over the previous decades, six generations of container vessels can be distinguished, mainly according to their capacities but also regarding voyage speeds; see Table 1. This also had, and still has, a great influence on container terminal operations. The first generation of container ships was designed to be operated in transatlantic and transpacific routes. The second generation of container ships not only ensured bigger capacity but also shorter voyage time due to increased speed. During the oil crisis in 1973 such fast vessels became uneconomical because of their huge consumption of fuel and lubricating oil. The third generation of container ships appeared with increased capacity and more economical and efficient market performance. Port operators considerably increased handling efficiency to fit the capacities of new container ships. From the third generation of ships to the fourth one, the number of seamen per vessel decreased which led the port operators to improve their handling technology and to catch up the new seamanship. The dimensional barrier of the Panama locks had constrained the progression of ship sizes to about 4,400 TEU, the so-called Panamax limit, until the middle of the 1990s (Slack *et al.*, 2002). Since then the so-called Post-Panamax vessels began to challenge the depth of the Panama Canal, lock chambers, passing bays and container berths; those were the hardest parts for existing port operators to conquer. Actually, the depth limitations could be regarded as one of the most important differences between terminals. From then on, different container terminals were chosen by liner carriers as hubs or feeder ports based on the natural advantages and prospective berth handling technology.

Nowadays, even mega ships with well over 8,000 TEU capacity, called the sixth generation, are not “newly born babies” in the shipping industry. Liner companies attempt to deploy more mega ships in their fleets, although it is common sense that merchant fleets should not only deploy huge or newly built ships. This tendency also strongly pushes container terminal operators to catch up the pace of bigger vessels, apply advanced technology and accomplish better management information systems. It should be noted that some authors see a possible risk in going beyond 8,000 TEU (see, e.g. Müller and Schönknecht, 2005) although the currently planned extension of the Panama Canal might render these calculations obsolete. Moreover, one can find the opinion that freight rates of containerized cargo, namely freight of all kinds (FAK), are not related to the ship type (Shi, 2000). However, the bigger and faster the vessels are, the more efficient they seem to be and the more likely it is to achieve economies of scale.

Regarding fleet composition liner companies build up their fleets and deploy types of ships (e.g. with respect to size) on purpose. Due to the similarity between liner shipping and airline service, problems and solutions of container fleet composition refer to those of aircrafts; see, e.g. Listes and Dekker (2005) and Adrangi *et al.* (1999). The problem for container terminal operators is to attract those types of vessels in the fleets which best match their port performance and obtain higher efficiency. In other words, one attempts to fractionalize the target markets instead of paying attention to all types of ships.

It should be noted that international shipping is an international trade and globalization borne service. Quality and price differentiation make the international goods exchange necessary, meanwhile the transocean lanes make it possible. There are three major long-distance lanes: the transpacific lane; the transatlantic lane; and the Far East–Europe lane. Those ports located along those three main trade lanes with enough depth have a considerable competitive advantage as they gain higher possibilities to be potential hubs. Other ports have to use every effort to compete by cost leadership, service differentiation, etc.

2.2 History and Trends of the Liner Shipping Industry

The history of liner shipping conferences goes back about 130 years (see, e.g. Wang and Zeng, 1997) since the first conference was set up in 1875. In an attempt to protect carriers in the conferences from the new steam ships serving trades to India and the Far East, the traditional liner shipping companies established cartels to control the important trades between these regions. Under the liner conferences system, which has long been an established feature of the shipping industry, a group of shipowners of one or several nationalities serve a group of ports on a given route (Branch, 1982). When there were around 150 liner shipping conferences covering all trading routes around the world, the principle of protecting members in the conferences from new competitors remained. Despite opposition from the shippers exemption was granted from competition rules under the Treaty of Rome based on which the conference system yielded the benefits for their customers.

From the late 1980s liner shipping conferences were no longer fully responsive to customers' needs (Yoshida *et al.*, 2001) (referring to, e.g. agility in supply-chain management and cost reductions) due to the following factors: barriers to trade freedom; inflation on shipping prices; threats of shipping services; and monopolization in price fixing. The liner carriers were trying to meet customers' needs by designing logistics solutions. From a shipper's point of view conferences and the legal protection were seen as antiquated impediments to rational business governed by market forces. Furthermore, the industry suffered from overcapacity on many major lanes. At the beginning of the 1990s, new kinds of vessel sharing arrangements were driven by overcapacity and customer service. It was a less risky way of entering new lanes, increasing the number of sailings and providing a wider range of services while reducing overcapacity. At that time, freight forwarders and ocean liner conferences were the ones most affected by vessel sharing arrangements: the more capacity in line with demand, the less need for conferences.

Strategic alliances in the liner shipping area have grown so dramatically in recent years that they have received a great deal of attention from researchers. For instance, the liner fleet planning and scheduling problem was treated by Xie *et al.* (2000). A more comprehensive literature review is provided by

Christiansen *et al.* (2004). Ryoo and Thanopoulou (1999) suggest liner alliances in the globalization era as an important strategic tool and Song and Panayides (2002) regard members of alliances as game players from a game theoretic point of view. The definition of alliances in a broader context, however, is not as uniform as it is in the area of liner shipping. A liner shipping strategic alliance is a group of liners with a specific agreement to share vessel space and improve service efficiency. Consortia represent operational, technical or commercial agreements between different sea carriers to pool some or all of their activities on particular trade routes (PC, 2004). However, "alliances represent agreements between carriers to cooperate on a global basis" (Czerny and Mitusch, 2005). That is, the scope and extent of those two kinds of cooperations are different.

Over time alliances between ocean carriers were nothing new by 1995. What had accelerated in the early 1990s was an expansion of those alliances to cover almost all major trade lanes. Although the number of such pacts was small, they involved some of the world's most dominant container ship operators. The goal of alliances is to become more efficient with lower cost. On the one hand, liner carriers are prepared to accept and implement new arrangements, which would reduce their operational costs and provide service offerings at a small extra cost. On the other hand, shippers welcome benefits like the increased sailing frequency.

The name of alliances	*Members*
Grand Alliance	Hapag-Lloyd, NYK Line, NOL, P&O
Global Alliance	MOL, Nedlloyd, OOCL, APL(NOL), MISC
CKY	COSCO, K-Line, YangMing
United Alliance	Hanjin, DSR-Senator, Cho Yang
Maersk Sealand	
Evergreen	

Table 2: Liner Shipping Alliances in 1995–1996

(Source: from *www.snet.com.cn*)

Table 2 shows the original position of liner shipping alliances around 1995–1996. P&O and Nedlloyd merged in January 1997 while APL merged with NOL in November 1997 which showed the combined membership from different alliances (Grand Alliance and Global Alliance). That is, the membership of liner alliances changed as well as their names. For instance, since 1998 the Global Alliance has been called "The New World Alliance" (TNWA).

The name of alliances	*Members*
Grand Alliance	Hapag-Lloyd, NYK Line, P&O Nedlloyd, MISC, OOCL
TNWA	MOL, APL, HMM
CKYH	COSCO, K-Line, YangMing, Hanjin
United Alliance	Hanjin, DSR-Senator, Cho Yang
Maersk Sealand	
Evergreen	

Table 3: Liner Shipping Alliances in 1998–2001

Table 3 presents the relatively stable position of liner shipping alliances around 1998–2001. The Grand Alliance, consisting of Hapag-Lloyd, NYK Line, Orient Overseas Container Line (OOCL) and P&O Nedlloyd, has merged its services with those of CP Ships-owned carriers Lykes Lines and TMM Lines. Similarly, between Maersk Sealand and TNWA carriers like APL, Hyundai Merchant Marine (HMM) and Mitsui OSK Lines (MOL) combined their transatlantic services in 2000.

Approximately three to five years later, the liner shipping market reshuffled to a great extent. Maersk Sealand announced that it had annexed P&O Nedlloyd, ranked third in May 2005. Meanwhile, China Shipping Container Line (CSCL), ranked eighth in terms of capacity in April 2005, acquired Canada Pacific ranked seventeenth at that time. However, Canada Pacific was finally bought by Hapag-Lloyd in August 2005 (Brent, 2005). These business activities show some turbulence and the resulting situation can be summarized in Table 4. On the one hand, the alliances or mergers between large carriers lead to a further concentration of vessel capacity on the long trade lanes. On the other hand, the increased monopoly power of major carriers would lead to large and sustained slots surplus.

The name of alliances	*Members*
Grand Alliance	Hapag-Lloyd, CP, NYK Line, MISC, OOCL
TNWA	MOL, APL, HMM
CKYH	COSCO, K-Line, YangMing, Hanjin
Maersk Sealand P&O Nedlloyd	
Evergreen	

Table 4: Situation from the End of Year 2005–2007

(*Sources*: Compiled from *www.snet.com.cn* and Brent, 2005)

Tables 2–4 can be summarized in Figure 1. We see that members of alliances are not fixed. For example, Nedlloyd originally belonged to the Global Alliance, in about 1998 switched to the Grand Alliance and then in 2005 was purchased by Maersk Sealand. Note that Evergreen, as an independent carrier, has maintained its independence from the main alliance groupings for decades since its establishment (Slack *et al.*, 2002).

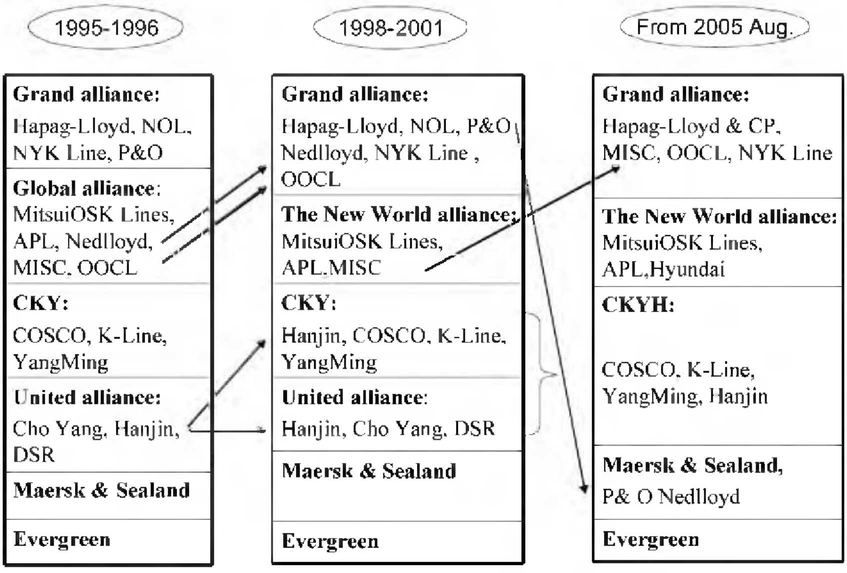


Figure 1: The Changing Membership in the Linear Shipping Industry

2.3 Motivations for Strategic Liner Shipping Alliances Members to Build Cooperations

For liner shipping alliances as well as liner carriers themselves, the most fundamental motivation may be profit maximization. There are several ways to achieve this goal, with the most prominent being revenue exploitation and cost savings. Below we describe ways and outcomes if liner carriers choose to be a member of an alliance.

2.3.1 Revenue Exploitation Aspect

A better transportation network could be achieved when a liner company cooperates with certain partners (Ding and Liang, 2005), which ensure a better transportation service to more coastal ports and inland distribution spots. An increase in revenues may be expected together with a higher customer satisfaction (Doi *et al.*, 2000). The frequency of liner ships' departure could be increased when liner companies cooperate and supply more vessels on the same route. More optional times of departure imply more convenience for forwarder agents and shippers to call upon the shipping service. Agreements and trust among alliance members make common actions such as general rate increases, seal fee collection, etc., much more likely. Those surcharges, just to mention some, could increase freight income.

The bargaining power of suppliers and customers greatly influence the final price of goods or service contracts. Shippers, as the demand side, may face problems regarding shipment, ports, inland transportation as well as ancillary problems (Addico, 2000). Generally speaking, freight rates are negotiated by shippers (or their agents) and carriers (Stewart *et al.*, 2003). To avoid the abovementioned problems, shippers should carefully pursue negotiations. A stronger liner alliance makes it less possible for the shippers to propose varying (e.g. non-profitable loads) and demanding desires when booking slots. Based on Porter's Five Forces Model (Porter 1980, 1991), shippers and forwarder agents have relatively less bargaining power compared to liner carriers regarding negotiations, and prices of the liner services posed by liner carriers are more accepted by shippers rather than shippers controlling the transportation prices themselves. For a discussion of competition policy and pricing see, e.g. Brooks *et al.* (2005).

2.3.2 Cost Savings Aspect

As the most important part of the total cost of ownership of liner carriers, fixed costs could be sharply decreased if a liner company cooperates with others when necessary. Carriers enter operational relationships to increase their service offerings and, at the same time, to reduce their costs (Sheppard and Seidman, 2001). Liner companies would share vessels and slots with each other to meet the sharply increasing freight desire without too large an investment in building new vessels or buying second-hand ships, or even other kinds of ships and then modifying them to carry containerized goods, as what had already happened to combined ships (Douet, 1999). Moreover, "flagging out" is also an adopted means of cutting down the total operation cost (Li and Wonham, 1999; Veenstra and Bergantino, 2000). Privatization or part privatization of state-owned carrier firms could be a possible way also (Roe, 1999). For a detailed and comprehensive quantitive analysis of investments see Veenstra (1999), Goss and Marlow (1997) and McWilliams *et al.* (1995).

Electronic data interchange (EDI) and related information sharing, of course, saves companies' costs. There is a trend in key organizational relationships in the community going along with the emergence of E-business (Martin and Thomas, 2001). EDI offers economic and strategic advances and can be regarded as an advanced tool for modern logistics (Lee *et al.*, 2000). Moreover, more efficient handling and stowage could also result in the ability to handle a considerably larger amount of freight in the same amount of time under the restriction of limited resources (Ambrosino *et al.*, 2004; Steenken *et al.*, 2004). To minimize the total time of stay at port of a vessel an optimized container stowage planning is, without any doubt, necessary, which calculates the suitable placement of containers in a containership (Wilson and Roach, 2000; Steenken *et al.*, 2004). Here we may consider, e.g., space restrictions at many major ports that do not allow for considerable expansion of terminals in many ports worldwide. This may include automatization processes with highly qualified back-office personnel instead of low cost workers for manual handling processes. Furthermore, more and more shipping carriers are willing to share pertinent data with port operator companies. It could save not only the shipping companies' costs but also the operator companies' costs.

Besides information sharing among shipping carriers and port operators, members in alliances sometimes share their port operation services as well. They share the same authorities and rights of fast handling to save total waiting and handling time when container vessels visit ports. A stronger liner alliance pushes port operators towards rethinking and rejudging the bargaining power of the liner carrier companies as they are very important customers. Actually, successfully attracting one liner company does not mean its other cooperators in the alliance would come to visit the port as well, while loosing one liner company may lead to a worse situation of loosing all the liner companies in this alliance as customers. This is one of the reasons why port operators pay a lot of attention to the influence of shipping alliances.

Until now, as shown in Figure 2, we have discussed two main aspects which motivate liner shipping companies to set up short-term cooperations and long-term alliances (see also Shi and Voß (2006)), including revenue exploitation and cost savings as mentioned above. Service sharing and bargaining power are particularly related to port operations. Liner companies (sometimes on behalf of shippers) set forth their desires of vessel visiting, cargo handling, short-time storage and logistics services (Steenken *et al.*, 2004), while port operators undertake great efforts to provide timely and agile services. It is significant for port operators to predict trends of container transportation and analyse the influence of shipping alliances advertently.

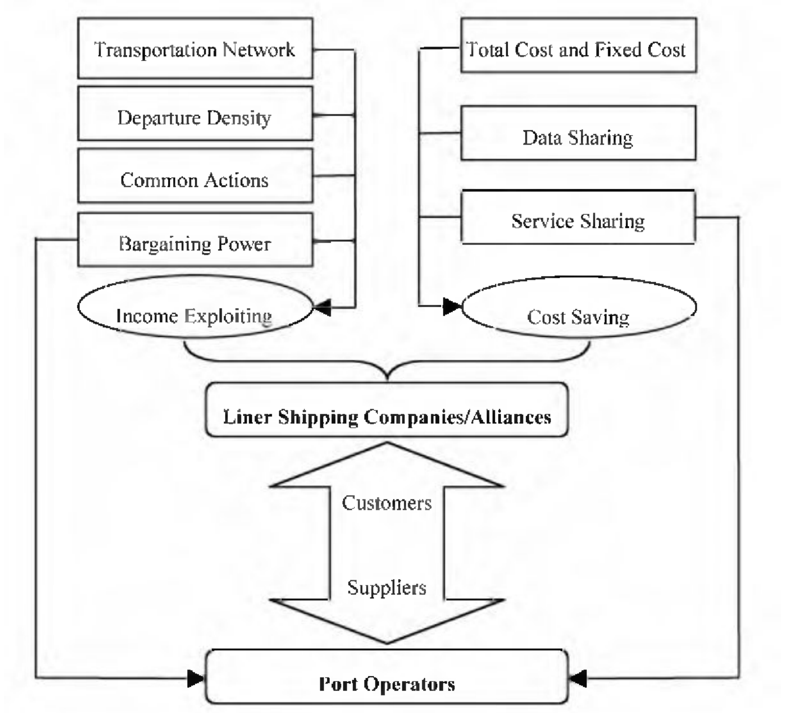


Figure 2: Motivations and Linkages between Liner Carriers and Port Operators

2.4 Resistance to the Strategic Liner Shipping Alliances

Forming an alliance can definitely offer various benefits but at the same time contain some drawbacks due to turbulence, unpredictable circumstances and various objectives (Song and Panayides, 2002). Moreover, risk considerations are of the utmost importance (see, e.g. MacDonald, 2004).

First, overcapacity is blamed for the poor financial performance and economic inefficiency over the long-term history of the liner shipping industry (Yoshida *et al.*, 2001). Some liner carriers differentiate themselves in terms of services offered, low freight price (e.g. China Shipping and MSC) or high quality service (e.g. Maersk Sealand). Integrating these different kinds of liners too tightly into an alliance with the corresponding requirement for "seamlessness" may pose problems. In alliances there is still much uncertainty and ambiguity. Sheppard and Seidman (2001) discuss the fact that liner carriers prefer to gain the benefits without having to ally with or to merge with other carriers. Therefore, the real long-term goal of large carriers is to improve their own service offerings, regardless of whether the improvement is through an alliance or a merger. Furthermore, a series of cross-alliance mergers and acquisitions had forced the alliances to restructure and/or modify their partner base (see above as well as Midoro and Pitto, 2000). Based on this one may conclude that relationships between partners are hard to predict; today's partners may be tomorrow's rivals (Kleymann and Seristo, 2001).

Secondly, even if a liner shipping company becomes a member of an alliance, it might not behave or share profit as fairly as it is supposed to. There are possible factors that make the relationship among members of an alliance "unfair", which could later lead to some turbulence of the membership and the alliance itself. Podolny and Morton (1999) examine whether the social status of an entrant owner impacts the predation behaviour of the incumbent cartels. They show that so-called high social status entrants are significantly less likely (40%) to be preyed upon than low social status entrants. Social status could be regarded as one of those factors which resist the development of liner shipping alliances.

Thirdly, the United States government still regarded shipping lines as a "controlled-carrier" under the Ocean Shipping Reform Act 1999 (Rimmer and Comtois, 2002). As a result, state-owned liner companies have to give 30 days' notice of any changes in freight rates, while other privately-owned liner companies also have to provide a 24 hours' notice to the American Communication Administration. This is a means by which the US government can prevent or reduce monopoly in the shipping industry. Its aim is to build up free and fair market structures all around the world.

Not only the USA but also some European countries claim the anti-cartel authorities to decrease the possibility of cartels, conferences, alliances and other kinds of monopoly. As reported by the OECD "the liner industry is no different than other global industries and, therefore, they require no special protection or privileges particularly in the area of setting prices" (ESC, 2004). In other words, liner conferences are not welcome in the shipping industry if one considers shippers' requirements and governments' regulations. Then, as the successors of liner conferences, consortia and alliances are still under the threat of being challenged by anti-cartel or anti-trust regulations, the existing liner shipping structure would change if those kinds of regulations take effect as strongly as they are expected.

No matter whether there are liner alliances or only independent carriers (suppose the alliances come to an end under anti-cartel regulations) in the liner shipping industry, port operators follow what the carriers and shippers demand. It seems that there are no explicit links between anti-cartel regulations and port operations. However, if we take into account the behavioural differences of liner conferences, alliances, consortia and independent carriers there is an indirect effect, which even comes from regulations on port operators. Usually members of liner conferences want to earn as much revenue as possible by fixing the freight price (ESC, 2004) together with a considerable bargaining power when negotiating with port operators, which causes port operators always try hard to cut down the handling costs (labour and operational). If liner shipping structures were destroyed by anti-cartel regulations, alliances and consortia would turn to individual carriers who should attract shippers not only by cost leadership but also service differentiations. Then port operators would switch to provide specific and agile handling services to carriers and shippers instead of only low handling charges.

However, if anti-cartel or anti-trust regulations do not take effect there would be great threats and challenges to the existing port operators because liner alliances and consortia tend to be much more powerful without barriers of the regulations. Those top liner corporations would like to enlarge their berth investment and maybe even build large dedicated ports all around the world, which make the regional port operation competition much fiercer compared to the current situation. To summarize, port operators should pay attention to those "indirect" regulations as well.

3 LINKAGE BETWEEN LINER SHIPPING CARRIERS AND CONTAINER TERMINAL OPERATORS

Vessel types, port handling methods and cargo characteristics are three vital factors which affect the freight rate and market trend considerably. Those factors even affect each other revealing that port operator company decision makers should be conscious of both of the other two sides simultaneously. Figure 3 shows the triangle connection of carriers, operators and shippers which could be a more comprehensive explanation. Based on this figure, we attempt to deepen our discussion by ordering shipper/cargo, carrier/vessel and operator/handling processes.

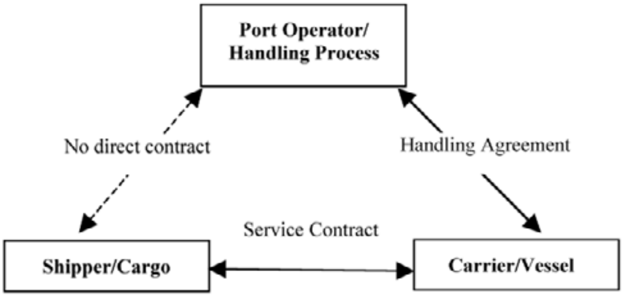


Figure 3: Triangle Connection within the Shipping Industry

The shipper charges the cargo transportation fee and also puts forward the transportation desire. There is an explicit contract between the shipper and the carrier, namely a service contract, which is always represented as bill of lading (B/L). In terms of maritime law the B/L should not be called a service contract itself (Si, 2005), but it is an important certificate of a liner service contract, which notes and defines the port of origin, port of discharge, place of delivery, vessel name, voyage number, cargo description, seal and container number, service type (CY–CY, CFS–CFS, Door-Door, etc.), insurance, risk allocation, payment method (prepaid or collect) and sometimes the freight rate too. Among those, service types and handling processes force container terminal operators to think about an optimal utilization of their instruments and resources.

Even if there is no direct contract between the shipper and the port operators, the shipper informs about his desire regarding a service contract, which is between him and the carrier. Then the carrier signs the handling agreement with the port operator, which means that there is at least an indirect linkage between shipper and port operator. Meanwhile, the handling processes may still be affected by cargo characteristics, such as bulk cargo, chemical cargo, liquid cargo and liquefied gases, etc. Different cargo may require totally different transportation needs and handling processes. For instance, the transportation and handling of oil products are related to local and regional supply/ demand imbalances, refinery inputs, outputs and utilization rates, storage considerations, product quality differences, price differentiation, seasonal variations and port traffic, etc. (Yamaguchi, 1999). Even if we focus on container terminal operations, there are many different kinds of containers which contain a variety of goods, such as normal dry container, hang container, flat container, high cube, open-top container, reefer container and dangerous cargo container, etc.

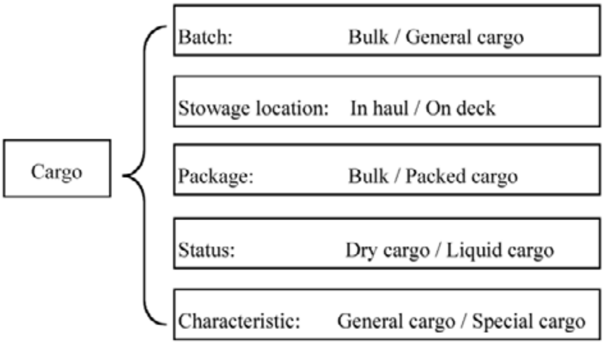

Cargo
Batch: Bulk / General cargo
Stowage location: In haul / On deck
Package: Bulk / Packed cargo
Status: Dry cargo / Liquid cargo
Characteristic: General cargo / Special cargo

Figure 4: Cargo Types

Among the cargo types mentioned in Figure 4, dry and packed cargo, especially if it is clean cargo, would be the most common type transported by container carriers. Some containerized bulk, such as rice and corn, could also be suitable for containerization. Furthermore, fresh cargo needs to be transported in reefer containers, which need special locations with respective equipment. As mentioned by Steenken *et al.* (2004), dangerous cargo in containers is not a common occurrence in every port, and it is more demanding with respect to the temperature control, pressure check-up, manifest location, etc. To be an efficient berth providing satisfactory handling and short-term storage, the terminal operator should first choose its target customers, especially if it does not get enough investment to develop plugs and special yard equipment. Even if it is possible to manage special cargo handling, operational managers still need to estimate and analyse when demanding cargo is going to visit and be handled. Briefly, the linkage between carriers and port operators relies not only on the carriers' vessel, but also on specific transportation desires promoted by shippers and cargos.

The number of ports that a fleet visits depends on the length of trade routes together with the number of vessels in the fleet. Because of the trend in VLCS, the price of new ships increases accordingly which pushes the liner companies to strive towards reducing the number of vessels in a fleet if possible (Yang, 2004). Based on that, the time period of a round voyage is shortened to ensure periodical (say, weekly) services with a reduced number of vessels; the number of port callings decreases, however, the lifts per call increase (Yang, 2004). It is certainly desirable for a port to become one of those reduced from the alliance's former calling of ports, which also leads, to a great extent, to revenue decrease. This is seen as a major linkage between the trend of liner carriers and the future of port operators. In other words, this is why port operators are so concerned about terminal operations under the influence of shipping alliances.

4 CONTAINER TERMINAL OPERATORS: BEHAVIOURS AND TRENDS

Considering the history of port operations, different development stages can be observed: see Table 4. Before the 1950s, ports were acting as centres of transhipment and delivery, also including the storage of cargo. During the 1950s up to the 1980s, ports provided more functions, such as value-added service and commodity export and import clearance, which gave the shippers and carriers more convenient services. Since the 1980s, ports more and more act as distribution centres in the whole logistics network while, at the same time, also serving as information platform.

Generation 1	Before the 1950s	Centre of transhipment, delivery, short time storage
Generation 2	1950s–1980s	Centre of services, value added function, commodity area
Generation 3	After the 1980s	Centre of logistics, distribution and information

Table 4: Port Operations Development

It should be noted that storage is always a function of utmost importance. However, in order to increase berth efficiency, storage functionality should only be available for short-term storage. For long-term storage it seems advantageous for containers to be delivered to special container yards or container freight stations.

The role of ports exceeds the simple function of services to ships and cargo. Apart from their role as the traditional sea/land interface, ports are a good location for value-added logistics, in which members of different channels can interact (Bichou and Gray, 2004). Besides acting as centres of transhipment and services (Generations 1 and 2 in Table 4), the ports of the third generation also act as dynamic nodes in international production and distribution networks (Carbone and Martino, 2003). Furthermore, the separation of responsibility for infrastructure and services and the transfer of regulatory power from landlord ports to independent regulatory authorities are what European and world ports currently face or will face in the near future (Farrell, 2001). Nevertheless, how far a port can develop not only relates to the regulations it has and the ambition of its decision maker, but also depends on the following factors: port tradition and organization; port accessibility; state aids; port productivity; port selection preferences of carriers and shippers; and comparative locational advantage (Fleming and Baird, 1999).

After analysing the existing container terminal operators' behaviours (see Table 4), a brief summary of the cooperations is given. Vertical cooperation with liner companies, horizontal cooperation with other top-standard port operators and other possibilities with 3PL or 4PL are all of great importance. Actually, the liner shipping strategic alliances consist of liner shipping companies; similarly, horizontal cooperations consist of port and terminal operators, such as, e.g. Hutchinson Port Holdings and PSA (port of Singapore Authority). Then there are similarities between those two kinds of cooperations, say, shipping alliances and port operators' cooperation: both of them are set up among those who provide nearly the same services; members all have relatively large capitals to manage; members are partners, to some extent, and competitors as well.

4.1 Vertical Cooperations

We define vertical cooperations as cooperations with other players in a supply chain, e.g., shippers, carriers, freight forwarders, vessel maintenance, etc.

Advantages that could be gained from vertical cooperations are listed and explained below.

Decrease the total service time and waiting time in port

When port operators cooperate with carriers with respect to the sharing of data, e.g. through EDI, and information system integration, remarkable time and cost savings could be expected. For a more detailed and comprehensive literature review see Steenken *et al.* (2004) whose survey focuses on optimization of port operation processes. Note that there may be arguments why mega ships should choose longer routes and visit highly efficient ports in order to save total service time in ports and waiting time in anchorage grounds (Xu, 1996).

Compete with carriers on bargaining power

On the one hand, the more members an alliance has, or the bigger its fleet is, the stronger oligopolistic economic power and competitive advantages it has when negotiating with port operators (Panayides and Cullinane, 2002). Port operators are supposed to accept and offer a lower wholesale price rather than a higher retail handling price; port operators, as any company in general, are not only concerned with short-term profits but also long-term profits. That is, their objective is net present value maximization (Kamien and Schwartz 1971).

On the other hand, we could also view terminal operations as the centre of the Five Forces Model. Certainly this could lead to another competitive structure. But those structures should be interrelated and useful for both the terminal operators and liner alliances. Based on the above discussion, if port operators cooperate with liners and set up a vertical cooperation, which could be a better means to apply common profits instead of contradictory bargaining powers then both liner companies and terminal operators could obtain a "win-win" result (see Table 5).

Fixed Costs	Direct fixed cost	Operating cost	Labour cost Repair & maintenance cost Lubricant storage Administration fee
	Indirect fixed cost	Capital cost	Vessels depreciation Lending cost Loan interests
Variable Costs	Voyage cost		Fuel cost *Port service cost* Others

Table 5: Cost Composition of Carriers

When cooperations exist between carriers and port operators, they could sign long-term handling agreements or even port facilities investment and utilization agreements, which benefit both sides. For example, COSCO and HIT set up a new company COSCO-HIT, which is a typical vertical alliance as they combined the carrier COSCO and its terminal service supplier HIT. Vertical alliances could largely develop international competitive advantages.

Service-oriented district allocation in port

Currently, carriers attempt to provide different transportation services to their customers, shippers, booking agents and cargo owners, including long lane services and short lane shuttling service. Due to the differences between those two services, their service areas should be allocated accordingly in order to reach higher efficiency. Vertical integration between global carriers and terminal operators is regarded as a good means of achieving better financial power and technical capability (Midoro *et al.*, 2005). For example, mega ships should choose deep, long berths and big container yards. But as for the average handling rate, those shuttling vessels are more demanding. That is, all of the berths should first set the oriented target customers and set up their values, versions and missions accordingly. Berths without sufficient depths and without sufficiently large container yards should provide fast handling service to shuttle vessels (for considerations regarding hinterland container terminals see Gronalt *et al.*, 2003). Considering the similarity between the airline industry and the liner shipping industry, we could expect those short lane shuttle services to be as successful as some of the so-called low-cost carriers in the airline industry.

Investment in container building and renting

Most of the top liner shipping companies, such as Maersk Sealand, COSCO, CSCL are stock holders of some container building companies. Liner companies try to reduce cost and achieve stability to defend against the turbulent market by building containers themselves or renting containers from the companies in which they invest. While the capability to defend against the turbulence is an advantage, there are also some disadvantages. The investment and the complex control of container return usually concerns managers of liner companies. Then there may be a good chance for port operators to attract liners by improving empty container renting and returning services. Liner shipping companies, in general, bought a number of containers and provided them to those shippers who do not have containers themselves. Those containers are costly, especially when they cannot be returned in time, delayed in some unknown ports due to inefficient management information systems. To solve this problem to some extent, some of the liner shipping companies, e.g. COSCON and CSCL, even invested in container building factories. On the contrary, the liner shipping companies would save capital if they did not need to pay attention to and invest in the container building industry. The limited capital should be used to build new mega ships and enlarge fleets, which might bring larger revenues.

Port operators already have experience in storing and handling empty containers which makes it more possible and much easier for them to enter the container building and renting sub-industry. Furthermore, experienced storage and handling of full and empty containers make it possible for shippers and carriers to accomplish timely clearance and departure. In short, besides those traditional activities and services (e.g. stores, water, medical aid, telephone service, bunkering, ship waste disposal) (Yahalom, 2002, Vanelslander, 2005), investing in the container building and renting sub-industry might also be a good way for port operators to improve services and attract carriers.

4.2 Horizontal Cooperations

We define horizontal cooperations as those cooperations with other port operators who should actually be competitors and partners at the same time. In other words, two or even more port operators set up a cooperative structure or even invest in a joint company providing handling services, based on regional cooperations or international cooperations, if any.

Regional cooperations

When comparing the regional cooperations among the world's top ports and local governments, some similarities can be found and the incentives of regional cooperations deserve discussion as well. In the survey of Slack *et al.* (2002) there appeared 470 additional ports of call in 1999 compared to 1989, which indicates an intensification of liner service offerings during that decade. As bigger container vessels are launched and deployed, the constraints of berth depth, considering cross-sections of ULCS, become an utmost factor of being regional hubs. Those ports with enough depth aiming at becoming regional hubs are conscious of the importance of distribution networks. They attempt to cooperate with local governments and other ports to ensure fast customs clearing and shuttling services for the feeder lanes. Meanwhile, smaller ports in the same regions welcome this kind of cooperation, otherwise they are loosing future throughput due to their depth limitations. This can be seen as an incentive of regional cooperation among local governments, potential hubs and feeder ports.

As an example (from the USA in 1990; Hershberg, 1995) consider the Philadelphia Regional Port Authority (PRPA), which was created between the State and Bucks, Delaware and Philadelphia Counties. The cooperation proved to be a win-win situation which benefited both the city and the port. For the port aspect, its competitive position was greatly improved by the financial support from the city and the affiliation of PRPA and South Jersey Port Corporation under the auspices of Delaware River Port Authority.

Regional cooperations not only exist between a port city and a port authority, but also among a few port operators who originally compete along the same sea coast and its hinterland. For example, in Europe ports are confronted with a closer integration in the maritime and shipping industry (Heaver *et al.*, 2000). An interesting case happens to be the so-called North Range in Europe. Despite fierce competition between different harbours, e.g., a terminal operator may, in fact, operate terminals in different ports such as Hamburg and Bremen (Germany). Moreover, there is a controversial discussion about whether shares of the HHLA (Hamburger Hafen und Logistik AG) may be sold to regionally close "competitors".

Regional cooperation also happens in the Yangtze River Delta (YRD), mid-east coast of China. Wang and Slack (2004) analyse the competition, cooperation and governance of Shanghai and Ningbo. It is mentioned that the foundation of this cooperation was not enough; lack of good regional port governance, caused by structural problems in administration, was still a burden for larger throughput in YRD.

Realizing the competitive advantages of Shanghai port, Hongkong and Shenzheng port faced the challenges by decreasing throughput (Cullinane *et al.*, 2004). Shenzhen port cooperated with Hong Kong for experienced management skills at the same time. These two ports, certainly with several port operators provide handling services there, set up regional cooperation though they are, as a matter of fact, still competitors to a great extent.

Partners of regional cooperation among ports should be carefully selected. As Thorhus and Lindstad (2006) mention, the difficulties in cooperating with other companies are an important factor that let the cooperations finally split. A better and effective way of keeping the cooperation for a relative long duration is to choose those potential partners with similar characteristics (Pando *et al.*, 2005), who admit similar business values, visions and missions.

International cooperations

Although based on the facts of the increase of ports of call together with intensification of visits of hubs, a very different picture of international cooperations is presented compared to the incentive of regional cooperations. For international cooperations among best practice terminal operators, technology transfer, management skill improvement, risk pooling and profit sharing seem to be reasonable motivations.

PSA engages in mergers and acquisitions and "globalizes" its activities through overseas ownership of port terminals and logistic firms (Rimmer, 1998). In 2004, PSA and SCT (Shanghai Container Terminal Company) gave the port industry a new way of international cooperation by holding each others' stocks instead of cash investment, take over or merger and acquisitions. As shown in Figure 5, the stock exchange ensures that both partners jointly share the profits and benefits in the recently opened Shanghai Yangshang port (*cf. www.nanfangdaily.com*).

From SCT's perspective, cooperation with PSA provides a good chance to learn advanced management skills of top standard terminal operations and newly invented technology. From PSA's perspective, investing in SCT ensures better profits in the future no matter whether Singapore or Shanghai becomes the regional mega hub along the Asian coast.

A crucial foundation to any type of cooperation mentioned above, such as vertical or horizontal, regional or international, are advanced management information systems and appropriate system integration.

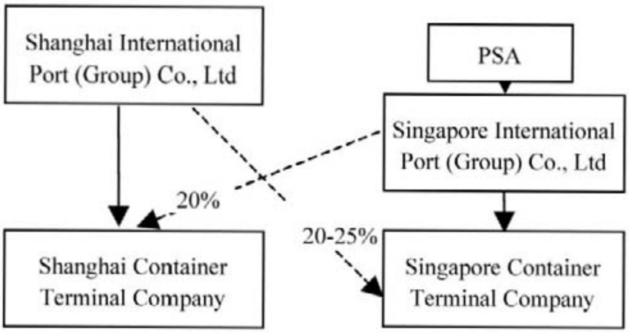

Shanghai International Port (Group) Co., Ltd
PSA
Singapore International Port (Group) Co., Ltd
20%
20-25%
Shanghai Container Terminal Company
Singapore Container Terminal Company

Figure 5: SCT and PSA—Cooperation

4.3 Technology Progress of Port Handling Processes

Outstanding hinterland linkages, super multimodal networks and well structured distribution centres are the usually mentioned points which would make port performance more efficient. Based on the existence of a great variety of newly developed technologies, advanced port operators might be eager to apply newly invented technologies as was the case with any type of innovation (see, e.g., Suh and Lee, 1998; Voß and Böse, 2000; Steenken *et al.*, 2004). APEC, as the largest regional economic cooperation organization in the world, formed by 18 members in Asia and the Pacific region, proposes that its members access and harness the latest transportation technologies (Sun and Zhang, 2000). Although it takes time and risk the outcome may be attractive. For instance, HHLA has experienced benefits while investing in double rail-mounted gantry cranes for efficient yard handling and is going to advance on this when restructuring further. Ningbo Beilun Container Port has kept testing (semi-) automated double rail-mounted gantry cranes since April 2005. Recently, Shanghai Waigaoqiao port conducted a successful trial to accomplish automated crane handling without on-the-spot labour; all moves are controlled from a back office located two kilometres away (*http://www.sjtu.edu.cn/newsnet/newsdisplay.php?id=9457*, access date 20 September 2006). Brisbane (Australia) is experiencing a fully automated straddle carrier system (*http://www.kalmarind.com/show.php?id=1041368*, access date 8 January, 2007).

Last but not least, there is no doubt that port operators should develop management information systems themselves or outsource and cooperate with professional software and IT service providers. Information technology beyond EDI is still seen as the great battleground not just among carriers, but also forwarders, logistics-based integrators and, potentially, pure technology companies (see, e.g. Hans, 2001, *www.dakosy.de*). Most importantly, port operators always face unscheduled incidents beyond any schedule, either by preventive or by reactive strategies. In this case, advanced management information systems (see, e.g. O'Brian, 2002) should be useful.

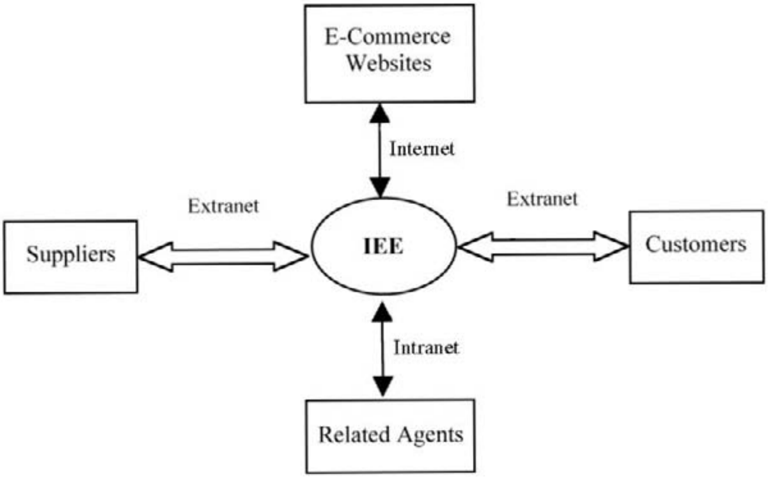


Figure 6: Internet worked e-Business Enterprises (IEE)

Setting an information system shared with customers (in this case, carriers, shippers, customs, forwarders and so on) does not mean that they have the same authorities. Networks should distinguish intranet, extranet and internet to make the information and business efficient and secure (see Figure 6). For instance, the carrier could authorize his forwarder or freight agents by digital signature to issue a B/L on behalf of the carrier himself; customs, carriers and port operators share cargo status and container/seal numbers, etc.

4.4 Possible Restructuring of Transportation Services

A successful port operator, like a successful player in a business game, must be well prepared to constantly meet both the existing desires and adopt the coming new roles in order to cope with the changing market environment (Notteboom and Winkelmans, 2001). Attention has to be paid to the competition of the port in new environments in restructured markets (Heaver *et al.*, 2000) including end-to-end services, pendulum visit lanes (Notteboom, 2005), and hub-feeder/spoke networks (Hayuth and Fleming, 1994). A proper integration of any player in shipping and port economics needs to cope with the recent challenges in globalization and supply-chain management (see, e.g. Wang and Cullinane, 2006). As mentioned by McCalla *et al.* (2005), it is the growth of transhipment that drives the most important developments in port traffic and facilitates the selection of hub ports. It is even speculated that more and more ports could lose existing positions as hub ports until finally only very few mega hubs survive (Payer, 1999 and De Monie, 2001; Baird, 2005).

5 CONCLUSIONS

Shippers are discovering that in today's ever-changing liner industry the question is not where your cargo is but who is carrying it. Furthermore, the carriers are paying more attention to who the port operator is together with the location of the port. As a result, port operators should take into account those shippers' and carriers' desires, improve their handling services by vertical and horizontal cooperations to increase customers' satisfactions and loyalties as much as possible by means of restructuring their service processes, management information systems, etc. Based on related background that we have provided in this chapter our exposition may also be seen as a research outline when discussing the shipping industry as well as port economics. One of the further research directions could be the social status effect on the cooperation among the port operators. Similar to the effects on shipping alliances this factor could affect the relationship, negotiation and development of port cooperations as well. While this chapter cannot be comprehensive enough to touch all possible issues in-depth, we strongly believe that the thoughts as well as the pointers to appropriate literature and the references therein can serve as a helpful entry into this field of research with important real-world implications.

REFERENCES

Addico, M.T., (2000). "African shippers" organizations: the Ghanaian experience". *Maritime Policy & Management* 27(2), 121–132.

Adrangi, B., Chow, G. and Raffiee, K., (1999). "The effects of market structure and technology on airline fleet composition after deregulation". *Review of Industrial Organization* 15, 77–88.

Ambrosino, D., Sciomachen, A. and Tanfani, E., (2004). "Stowing a containership: the master bay plan problem". *Transportation Research Part A: Policy and Practice* 38(2), 81–99.

Baird, A.J., (2005). "Optimising the container transhipment hub location in Northern Europe". *Journal of Transport Geography*, article in press, accessible at *http://www.scapaflowhub.org/ContainerBaird.pdf.*

Bichou, K. and Gray, R., (2004). "A logistics and supply chain management approach to port performance measurement". *Maritime Policy & Management* 31(4), 47–67.

Blauwens, G., De Baere, P. and Van De Voorde, E., (2006). *Transport Economics.* 2nd edn. De Boeck, Antwerp.

Branch, A.E., (1982). *Economics of Shipping Practice and Management.* Chapman and Hall, London and New York.

Brennan, J., (2001). *Measurement approaches: port capacity management.* Paper presented at Marine Board Seminar on Waterway and Harbor Capacity, 23 April 2001, *http://gulliver.trb.org/conferences/2001Waterway%26Harbor/Brennan.pdf.*

Brent, J., (2005). *TUI wins over CP ships for $2-billion. http://www.theglobeandmail.com/servlet/Page/document/v4/sub/Marketing Page?user_URL=http://www.theglobeandmail.com%2Fservlet%2Fstory%2FRTGAM.20050821.wcpcpc0821%2FBNStory%2FBusiness%2F%29&ord=1125892481700&brand=theglobeandmail&force_login=true.* Accessed on 22 August 2005.

Brooks, M.R., Button, K. and Nijkamp, P. (eds) (2005). *Maritime Transport,* Edward Elgar, Cheltenham.

Christiansen, M., Fagerholt, K. and Ronen, D., (2004). "Routing and scheduling: status and perspectives". *Transportation Science* 38(1), 1–18.

Cullinane, K., Wang, T.F. and Cullinane, S., (2004). "Container terminal development in mainland China and its impact on the competitiveness of the port of Hong Kong". *Transport Reviews* 24(1), 33–56.

Cullinane, K., (2005). "Editorial: key themes in shipping economics research". In Cullinane, K. (ed.). *Shipping Economics.* 1–17. Elsevier, Amsterdam.

Czerny, A. and Mitusch, K., (2005). "Cooperation and Competition in the Cargo Liner Shipping Industry", *Internationales Verkehrswesen* 12 (Dec.), 553–557.

De Monie, G., (2001). "Re-evaluating the economics of transshipment". The Terminal Operation Conference & Exhibition.

Ding, J.F. and Liang, G.S., (2005). "Using fuzzy MCDM to select partners of strategic alliances for liner shipping". *Information Sciences* 173(1–3), 197–225.

Doi, M., Ohta, H. and Itoh, H., (2000). "A theoretical analysis of liner shipping conferences and strategic alliances". *Review of Urban and Development Studies* 12(3), 228–249.

Douet, M., (1999). "Combined ships: an empirical investigation about versatility". *Maritime Policy & Management* 26(3), 231–248.

ESC (European Shippers" Council), (2004). *What Shippers Require from Liner Shipping in the Future and Why.*

Farrell, S., (2001). Comment—If it ain't bust, don't fix it: the proposed EU directive on market access to port services, *Maritime Policy & Management* 28(3), 307–313.

Fleming, D.K. and Baird, A.J., (1999). "Some reflections on port competition in the United States and Western Europe". *Maritime Policy & Management* 26(4), 383–394.

Fremont, A. and Ducruet, C., (2005). "The emergence of a mega-port—from the global to the local, the case of Busan". *Tijdschrift voor Economischen en Sociale Geografie* 96(4), 421–432.

Goss, R. and Marlow, P., (1997). "Investment incentives for British shipping: a comment on recent work". *Maritime Policy & Management* 24(4), 389–391.

Gronalt, M., Hartl, R.F. and Reimann, M., (2003). "New saving based algorithms for time constrained pickup and delivery of full truckloads". *European Journals of Operational Research* 151(13), 520–535.

Hans, J.F.P., (2001). "Developments in global seatrade and container shipping markets: their effects on the port industry and private sector involvement". *International Journal of Maritime Economics* 3(1), 3–26.

Hayuth, Y. and Fleming, D., (1994). "Concepts of strategic commercial location: the case of container ports". *Maritime Policy & Management* 21(3), 187–193.

Heaver, T., Meersman, H., Moglia, F. and Van De Voorde, E., (2000). "Do mergers and alliances influence European shipping and port competition?" *Maritime Policy & Management* 27(4), 363–373.

Hershberg, T., (1995). "The case for regional cooperation". *The Regionalist* **1**(3).

Huybrechts, M., Meersman, H., Van De Voorde, E., Van Hooydonk, E., Verbeke, A. and Winkelmans, W. (eds), (2002). *Port Competitiveness—An Economic and Legal Analysis of the Factors Determining the Competitiveness of Seaports*. De Boeck, Antwerp.

Kamien, M.I. and Schwartz, N.L., (1971). "Limit pricing and uncertain entry". *Econometrica* 39(3), 441–454.

Kleymann, B. and Seristo, H., (2001). "Levels of airline alliance membership: balancing risks and benefits". *Journal of Air Transport Management* 7, 303–310.

Lee, T.W., Park, N.K., Joint, J.F. and Kim, W.G., (2000). "A new efficient EDI System for container cargo logistics". *Maritime Policy & Management* 27(2), 133–144.

Li, K.X. and Wonham, J., (1999). "Who is safe and who is at risk: a study on 20 year record on accident total loss in different flags". *Maritime Policy & Management* 26(2), 137–144.

Listes, O. and Dekker, R., (2005). "A scenario aggregation-based approach for determining a robust airline fleet composition for dynamic capacity allocation". *Transportation Science* 39(3), 367–382.

MacDonald, A., (2004) “Ocean Liners: Does size really matter?” *World Trade Magazine*, *http://www.worldtrademag.com/CDA/Articles/Ocean/75ffcf5149af7010VgnVCM100000f932a8c0*, last accessed 8 January 2007.

Martin, J. and Thomas, B.J. (2001). “The container terminal community”. *Maritime Policy & Management* 28(3), 279–292.

McCalla, R., Slack, B. and Comtois, C., (2005). “The Caribbean Basin: adjusting to global trends in containerization”. *Maritime Policy & Management* 32(3), 245–261.

Mc Williams, D., Norwood, P. and Parfitt, A., (1995). “Economitrics testing of investment incentives: update of Marlow model”. *Maritime Policy & Management* 22(3), 201–207.

Midoro, R. and Pitto, A., (2000). “A critical evaluation of strategic alliances in liner shipping”. *Maritime Policy & Management* 27(1), 31–40.

Midoro, R., Musso, E. and Parola, F., (2005). “Maritime liner shipping and the stevedoring industry: market structure and competition strategies”. *Maritime Policy & Management* 32(2), 89–106.

Müller, M. and Schönknecht, A., (2005). “Kapitalrendite von Großcontainerschiffen”. *Internationales Verkehrswesen* 57, 58–60.

Ninnemann, J., (2006). *Seehafenwettbewerb in Europa*. Dr Kovač, Hamburg.

Notteboom, T.E. and Winkelmans, W., (2001). “Structural changes in logistics: how will ports authorities face the challenge?”. *Maritime Policy & Management* **28**(1), 71–89.

Notteboom, T.E., (2004). “Container shipping and ports: an overview”. *Review of Network Economics* **3**(2), 86–106.

Notteboom, T.E. and Rodrigue, J.-P., (2005). “Port regionalization: towards a new phase in port development”. *Maritime Policy and Management* 32(3), 297–313.

O’Brien, J.A., *Managing Information Technology in the E-Business Enterprises*, 5th edn, 2002.

Panayides, P.M. and Cullinane, K., (2002). “Competitive advantage in liner shipping: a review and research agenda”. *International Journal of Maritime Economics* 4(3), 189–209.

Pando, J., Araujo, A. and Maqueda, F.J., (2005). “Marketing management at the world’s major ports”. *Maritime Policy & Management* 32(2), 67–87.

Payer, H.G., (1999). “Feasibility and practical implications of container ships of 8000, 10,000 or even 15,000 TEU”. The Terminal Operation Conference & Exhibition.

Podolny, J.M. and Morton, F.M.S., (1999). “Social status, entry and predation: the case of British shipping cartels 1879–1929”. *Journal of Industrial Economics* 47(1), 41–67.

Porter, M.E., (1980). *Competitive Strategy: Techniques For Analyzing Industries And Competitors*. Free Press, New York.

Porter, M.E., (1991). “Towards a dynamic theory of strategy”. *Strategic Management Journal* 12, 95–117.

PC (Productivity Commission), (2004). *Review of Part X of the Trade Practices Act 1974: International Cargo Liner Shipping*. Draft Report.

Rimmer, P.J., (1998). "Ocean liner shipping services: corporate restructuring and port selection/competition". *Asia Pacific Viewpoint* 39(2), 193–208.

Rimmer, P.J. and Comtois, C., (2002). "China's transport and communications firms: transforming national champions into global players". *Asia Pacific Viewpoint* 43(1), 93–114.

Roe, M.S., (1999). "The commercialization of East European liner shipping: the experience of Poland". *Maritime Policy & Management* 26(1), 69–79.

Ryoo, D.K. and Thanopoulou, H.A., (1999). "Liner alliances in the globalization era: a strategic tool for Asian container carriers". *Maritime Policy and Management* 26(4), 349–367.

Sheppard, E.J. and Seidman, D., (2001). "Ocean shipping alliances: the wave of the future?" *International Journal of Maritime Economics* 3(4), 351–367.

Shi, X., (2000). "The study on the compilation of the China container freight index". *Maritime Policy & Management* 27(3), 303–308.

Shi, X. and Voß, S., (2006). *Non-cooperative Games in Liner Shipping Strategic Alliances*. Paper presented at EURO XXI, Reykjavik, Iceland.

Si, Y.Z., (2005). *Maritime Law* (in Chinese). Law Publishing House, China.

Slack, B., Comtois, C. and McCalla, R., (2002). "Strategic alliances in the container shipping industry: a global perspective". *Maritime Policy & Management* 29(1), 65–76.

Song, D.W., (2002). "Regional container port competition and cooperation: the case of Hong Kong and South China". *Journal of Transport Geography* 10, 99–110.

Song, D.W. and Panayides, M., (2002). "A conceptual application of cooperative game theory to liner shipping strategic alliances". *Maritime Policy and Management* 29(3), 285–301.

Steenken, D., Voß, S. and Stahlbock, R., (2004). "Container terminal operation and operations research—a classification and literature review". *OR Spectrum* 26, 3–49.

Stewart, H.G. and Inaba, F.S., (2003). "Ocean liner shipping: organizational and contractual response by agribusiness shippers to regulatory change". *Agribusiness* 19(4), 459–472.

Suh, M.S. and Lee, Y.J., (1998). "A hierarchical expert system for integrated scheduling of ship berthing, discharging and material transport". *Expert Systems* 15(4), 247–255.

Sun, G.Q. and Zhang, S.P., (2000). "The APEC future maritime policy and its evaluation". *Maritime Policy & Management* 27(2), 209–213.

Thorhus, R.H. and Lindstad, H., (2006). *An Evaluation of a Joint Seaborne Transport System Based on a Strategic Alliance*. Accessible at *http://www.idefondet.ntnu.no/vedlegg/Thorhus_paper_Nofoma.pdf*, accessed 3 November 2006.

Vanelslander, T., (2005). "The Economics Behind Cooperation and Competition in Sea-Port Container Handling", PhD thesis. Faculty of Applied Economics, University of Antwerp.

Veenstra, A.W., (1999). "Quantitative Analysis of Shipping Markets", PhD thesis. Delft University Press, Delft, The Netherlands.

Veenstra, A.W. and Bergantino, A.S., (2000). "Changing ownership structures in the Dutch fleet". *Maritime Policy & Management* 27(2), 175–189.

Voß, S. and Böse, J., (2000) "Innovationsentscheidungen bei logistischen Dienstleistern—Praktische Erfahrungen in der Seeverkehrswirtschaft". In: Dangelmaier, W. and Felser, W. (eds) *Das reagible Unternehmen*, HNI, Paderborn, 253–282.

Wang, J.J. and Slack, B., (2004). "Regional governance of port development in China: a case study of Shanghai international shipping center". *Maritime Policy & Management* 31(4), 357–373.

Wang, J.J., Ng, A.K.-Y. and Olivier, D., (2004). *Port Governance in China: A Review of Policies in an Era of Internationalizing Port Management Practices, Transport Policy.* Elsevier, Oxford.

Wang, T.F. and Cullinane, K., (2006). "The efficiency of European container terminals and implications for supply chain management". *Maritime Economics & Logistics* 8, 82–99.

Wang, Y.Y. and Zeng, K., (1997). *Ocean Transportation Operation* (in Chinese). Transportation Publishing House of People's Republic of China, Beijing.

Wilson, I.D. and Roach, P.A., (2000). "Container stowage planning: a methodology for generating computerised solutions". *Journal of the Operational Research Society* 51(11), 1248–1255.

Xie, X.L., Wang, T.F. and Chen, D.S., (2000). "A dynamic model and algorithm for fleet planning". *Maritime Policy and Management* 27(1), 53–63.

Xu, T.F., (1996). *Management and Operation of Shipping Company* (in Chinese), Publishing house of Dalian Maritime University.

Yahalom, S., (2002). *Intermodal Productivity and Goods Movement-Land Access to Port and Terminal Gate Operations.* University Transportation Research Center.

Yamaguchi, N.D., (1999). "Asian product trade". *Maritime Policy & Management* 26(4), 327–336.

Yang, C.H., (2004). *The Impact of Bigger Vessels on Shipping & Ports.* Accessible at *http://www.kmi.re.kr/english/data/publication/k2004_02.pdf*, accessed 27 October 2006.

Yoshida, S., Yang, J.H. and Kim, K.H., (2001). "The network economy of the alliance in the liner shipping". In: *Proceeding of International Associate of Maritime Economics Conference 2001*, 333–343.

http://www.dakosy.de/en/#. Accessed 6 October 2006.

http://events.simplywebcast.com/maersk/may_2005/index.html. Accessed 12 May 2005.

http://www.globalsecurity.org/military/systems/ship/container-types.html. Accessed 6 November 2006.

http://info.jctrans.com/wl/hy/hyzs/2006726279397.shtml. Accessed 12 September 2006.

http://www.sjtu.edu.cn/newsnet/newsdisplay.php?id=9457. Accessed 20 September 2006.

http://www.smg.cn/news/content.aspx?NewsId=110888. Accessed 20 September 2006.

This page intentionally left blank

PART III

FRAMEWORKS FOR MANAGING THE SECURITY OF GLOBAL TRADING AND SUPPLY-CHAIN SYSTEMS

This page intentionally left blank

CHAPTER 10

VOLUNTARY SUPPLY-CHAIN SECURITY PROGRAMME IMPACTS: AN EMPIRICAL STUDY WITH BASC MEMBER COMPANIES

Ximena Gutiérrez, Philippe Wieser and Juha Hintsa

Ecole Polytechnique Fédérale de Lausanne, IML International Institute for the Management of Logistics, HEC Lausanne

Abstract
Protecting global supply chains against illegal acts is receiving increasing attention both within the trade community and the governmental authorities. Various recent voluntary programmes and mandatory regulations are currently being introduced to reduce the vulnerability of the global supply chains faced with international crime, drug smuggling, terrorism, etc. However, there is little empirical evidence about the impacts of these programmes for the companies that have implemented them. BASC (Business Alliance for Secure Commerce) is a private-origin voluntary security programme, created in Latin America in 1996. This programme, initially designed to prevent legal cargo from being used to smuggle drugs, has evolved towards a complete security management system, which covers multiple security issues within the supply chain. This study presents the result analysis of a 20-question survey, answered by 102 BASC member companies. The study identifies which supply-chain security standards have been implemented by security leading companies in Latin America, establishes which are the most and least efficient implemented security measures, provides a qualitative analysis of the relationship between cost and effectiveness of these measures and presents some of the benefits acquired through the programme implementation. Based on the overall findings and observations the study provides recommendations and conclusions for governmental and company decision makers in relation to "future win-win supply-chain security programmes".

1 INTRODUCTION

Companies have always dealt with disruptions that affect the efficiency of their supply chains. Disruptions can arise from a number of sources which can be unintentional such as natural disasters and accidents, or intentional such as terrorist attacks and theft. To protect their personnel and physical assets, companies have traditionally relied on internal safety and security programmes. However, the tremendous damage caused by the emergent international terrorism against developed economies has highlighted the vulnerability of current global supply chains and has placed the security issue at the top of the agenda of several governments and international organizations around the world. Enhancing global supply-chain security has shifted from being a pure public or private concern to a public–private joint objective.

Several voluntary security initiatives which link business and governmental actors through partnership schemes have been and are still being created. Most of them are mainly being promoted by Customs administrations around the world and they consist of a set of security measures which should be implemented by the participants of the supply chain in order to be granted the status of "security compliant" partners. Companies which can demonstrate that their whole supply chain is secure are expected to receive some kind of facilitation when crossing the borders.

On the surface, these programmes seem to be a new set of international trade regulations that will have to be implemented by the business sector. However, studied in depth, they consist mainly of measures that have been traditionally used by companies dealing with risky products or operating in risky environments. In spite of this fact, there is low empirical evidence of the implications of adding or integrating these measures to the supply-chain operations.

The aim of this chapter is to contribute to filling this gap by gathering information on the costs of implementing and maintaining this type of programme, and identifying the most effective security measures and the realized benefits. Following a complete analysis of nine voluntary security initiatives worldwide that appear to have significant impact on supply-chain security development, BASC (Business Alliance for Secure Commerce[1]) member companies were selected as an appropriate sample community for the following reasons.

BASC is a private-origin voluntary security programme created in Latin America in 1996. This programme, initially designed to prevent legal cargo from being used to smuggle drugs has evolved towards a complete security management system which covers multiple security issues within the supply chain. The 1,500 companies which have or are currently implementing the programme are headed by the World BASC Organization, a non-profit organization whose mission is to "facilitate and stimulate agile international trade through the implementation and management of security standards and procedures applied to the international supply chain".[2] The BASC programme is one of the few private-origin international supply-chain security initiatives, the only one with several years of experience in the implementation of supply-chain programmes in Latin American countries.

[1] Formerly: Business Anti-Smuggling Coalition.

[2] *http://www.wbasco.org/espanol/quienessomos.htm*.

The research involved a survey available to all BASC members, which gathered information on the characteristics of participating companies, the costs of implementing and maintaining the programme, the effectiveness of the security measures and the realized benefits. Section 2 presents a brief description of the BASC programme and how it is positioned relative to other security programmes worldwide. Section 3 describes the research methodology and the basic characteristics of the sample companies. Section 4 presents the study findings divided in four subsections including the concrete security measures implemented by BASC member companies, the cost of certification and maintenance of the programme, the qualitative obtained benefits and a discussion about the obstacles in carrying out a cost benefits analysis for security investments. Section 5 explores the potential connections between the number, type and cost of the security measures and the number and type of obtained benefits. In addition it provides some examples of connections between certain security measures and certain benefits. Section 6 analyses the current attitude of the company managers regarding the vulnerability of their supply chains after the implementation of the programme security measures, their awareness of the new supply-chain security environment and their concerns and recommendations regarding the new security regulations. Finally, based on the overall study findings and observations some conclusions and recommendations for supply-chain security programme designers and users are made.

2 THE BASC PROGRAMME AND THE INTERNATIONAL SUPPLY-CHAIN ENVIRONMENT

Currently the international supply chain environment presents a great variety of security initiatives ranging from country specific operational regulations to global research programmes. These initiatives have different origins, degrees of enforceability and target multiple security related specific goals (Hintsa *et al.*, 2006). Among these initiatives, voluntary supply-chain security programmes are of special interest for several reasons (Gutierrez *et al.*, 2006): (i) they are volunteer-based but the cost of not being involved can be very high; (ii) identical certifications can be obtained through different implementation strategies, therefore companies are confronted with the challenge of identifying the best strategy for their own needs; and (iii) there is a generalized need to guarantee compatibility between programmes and to establish mutual recognition among governments and border agencies from different countries. The researchers identified at least nine voluntary programmes originating from different countries providing a complete reference guide of security standards for certified companies. Examples of these programmes are presented in Table 1.

Type of Programme	*Examples*
Customs compliance programmes to which the security layer has been added	PIP (Canada), StairSec (Sweden), ACP & Frontline* (Australia), AEO (European Union)
Government origin, pure security programmes	C-TPAT (USA), Secured Export Partnership (New Zealand)
International organization origin, security standards programmes	WCO framework of standards, ISO (International organization for standardization)
Private sector origin, pure security programmes	BASC (Latin America), TAPA (technology companies)

Table 1: Examples of Supply-chain Security Programmes and their Type (Gutierrez *et al.*, 2006)

Among these examples, PIP, BASC and TAPA are the oldest and have been in operation since 1994, 1996 and 1997, respectively. However, as shown in Table 1 they differ in origin, main goals, type of companies and certification procedures. For instance, PIP has no certification scheme, TAPA was initially designed for technology companies and BASC was initially intended to reduce the risk that legal cargo would be used to smuggle drugs into the US. In contrast, programmes such as the WCO framework of security standards, ISO 28000/1, and EU AEO are still under development.

BASC is an organization with member companies from 13 different countries and chapters in seven countries or regions (Colombia, Ecuador, Peru, Costa Rica, Pacific region and Dominican Republic). Only companies providing logistics services or carrying out manufacturing or international trade related activities are eligible to participate in the programme. The process starts when the company submits an application to the corresponding BASC chapter (if no chapter exists in the country, the request for affiliation goes directly to the World BASC Organization together with legal documents which must prove the origin and legal status of the company. The designated commission or board will study these documents and decide whether the company is eligible to enter into the certification process. Once this step has been approved, the company is subject to a security audit and, if necessary, will receive an improvement recommendation report. Depending on whether the company fulfils the minimum BASC security requirements, it is certified or it is pre-selected to implement the missing standards before a certain deadline (during this process the company can receive some support from BASC). Upon certification, the company commits to follow the BASC policies. The certification is valid for one year, after which the company is evaluated again to verify its security compliance.

Certified companies can benefit from certain World BASC Organization events and agreements such as personnel training on security and international trade related subjects, participation in annual BASC seminars, certification audits and follow up, collaboration agreements with local authorities, support to establish contacts with port authorities and Customs administrations and information exchange with other BASC chapters.

3 STUDY DESCRIPTION

3.1 Methodology

This study involved a five-page questionnaire, addressed to 800 BASC member companies in 10 different countries. The survey was written in collaboration with BASC management and fined-tuned in a validation exercise with five BASC chapter directors from different countries. The final document contains 20 questions which follow the structure presented in Figure 1.

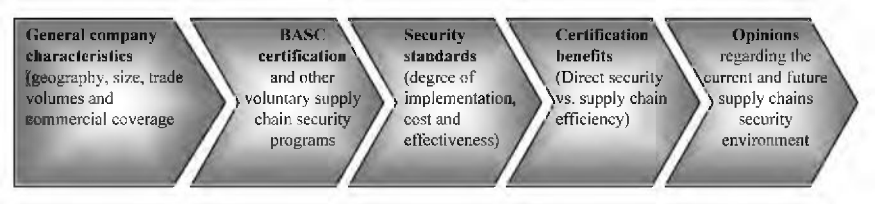

General company characteristics (geography, size, trade volumes and commercial coverage
BASC certification and other voluntary supply chain security programs
Security standards (degree of implementation, cost and effectiveness)
Certification benefits (Direct security vs. supply chain efficiency)
Opinions regarding the current and future supply chains security environment

Figure 1: Summary of Questionnaire Structure

3.2 Sample Characteristics

Out of 800 companies contacted, 102 completely answered surveys were received for a response rate of 13% and sample error of 10%.[3] The survey covers 78% of the member countries, represents companies involved in different international trade-related operations (i.e. manufacturers, traders, port operators, logistics services providers[4] and others providing support services such as security monitoring, rental cargo vehicles etc.), covers different sizes, and annual turnovers and includes companies which were certified during different years. Figure 2 presents the distribution of respondent companies in

[3] *Sample error* = $\sqrt{\frac{t^2 \star p \star q}{n}}$ where t = 1.96 from t-student distribution table, p and q estimated both as = 1/2, n = 102.

[4] Freight forwarders, carriers, and Customs brokers were included in this group.

terms of four different categories: Country of main operations, commercial activity, size and annual turnover.

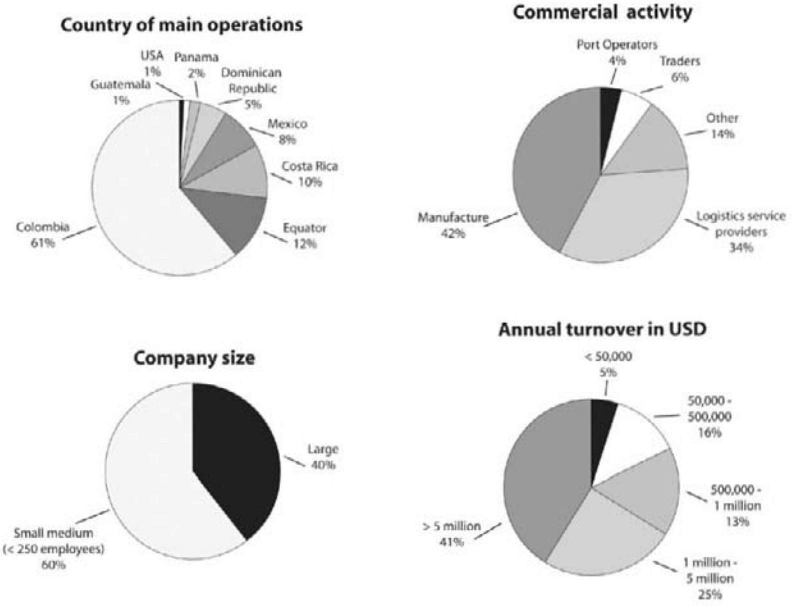


Figure 2: Distribution of Respondents

In addition, respondents were asked to explain the company's main motivation for seeking BASC certification. Three main declared reasons for applying for certification were mentioned: to fulfill market requirements (either because the certification was required by clients or suppliers or to differentiate service offers); to improve or establish internal security standards; or to reduce the probability of cargo contamination by illegal activities. Even though the programme is volunteer-based, for a large proportion of the sample (40%) it is considered more a minimum requisite for participating in international trading activities. The multiple answers were classified into seven main categories and are presented on Figure 3.

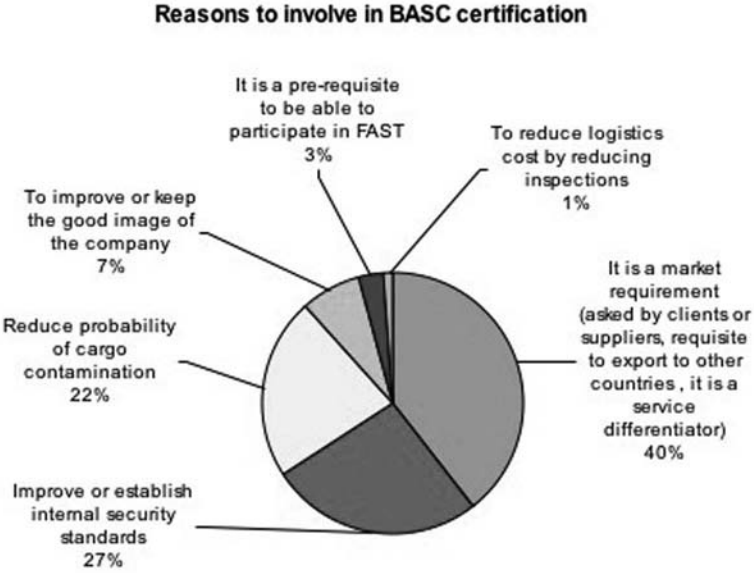


Figure 3: Distribution of answers of companies' motivations to involve in BASC

3.3 Study Findings

3.3.1 Security Measures Implementation

Most of the existing voluntary supply-chain security programs comprise general guidelines which describe the security measures that should be implemented to become a certified company. However, there is much variability regarding the level of detail in which these measures are presented. For instance, BASC is a programme with one of the most highly detailed security standards lists (approximately 100 security measures). Nevertheless, researchers believe that most of the security measures can be implemented in different manners. There still is a great degree of freedom in the implementation of security standards. However, this freedom depends on each company's particular situation (Gutierrez *et al.*, 2006).

A consolidated list of security measures which summarizes the most recurring measures in nine different security initiatives worldwide was established. The resulting 25 measures where classified into the following five categories: facility management; cargo management; human resources management; information management; and business network and company management systems. It should be noted that the list contains some measures that are not explicitly required in BASC security standards guidelines (i.e. the use of cargo inspection and tracking technology, the use of international standards for data management, etc.). However, they may contribute to create an appropriate supply-chain security management system within companies or as part of other existing or future/planned security programmes. This situation was intentionally created for two reasons: (a) to evaluate whether companies only implement the security measures required by the programme or if the certification process stimulates the implementation of additional measures considered as necessary by the company; and (b) to evaluate how far or close BASC members are from being compliant with other recent security programmes.

Respondents specified which security measures from the consolidated list were implemented by their companies. For each implemented measure, they were asked to explain if it was done as a requirement for obtaining BASC certification, or if it was in place prior to the certification process. For each of the non-implemented measures, respondents were asked to explain if they had plans to implement them in the near future or if the measures were not applicable for their company.

Figure 4 presents the implementation reasons and the future plans for each security measure and ranks them from the most to the least implemented by BASC companies. It shows that the most popular measure is the *employee hiring/exit process*, which includes activities such as checking worker background, interviewing leaving or fired employees and other related activities to guarantee the reliability of company staff. The least implemented measures appears to be the *exploitation of cargo inspection technical solutions*, which could consist of the use of various scanners: nuclear/chemical/biological sensors etc.

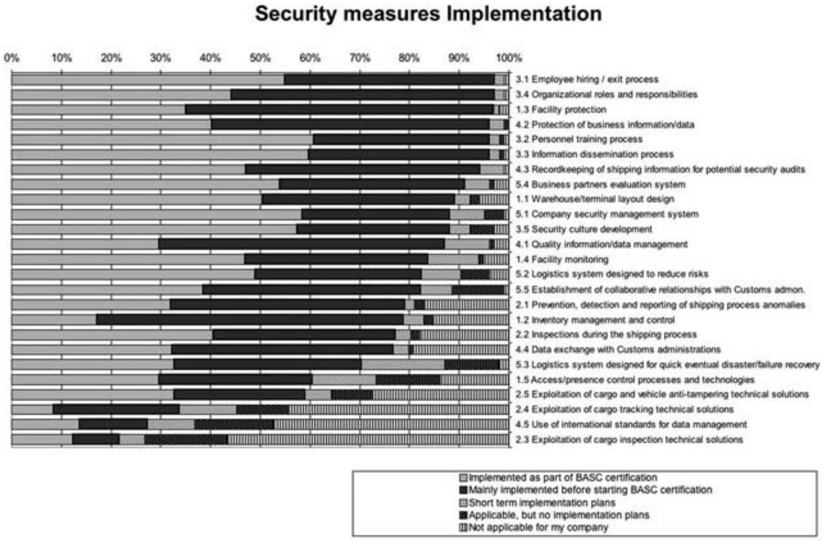


Figure 4: State of Implementation for Set of Security Measures (sample size 102)

3.3.2 BASC Costs

Respondents were asked to estimate the total cost incurred to implement the security measures required by the BASC certification and the annual cost of maintaining these measures. These costs include expenses caused by the implementation of the security measures themselves (i.e. security training courses, investments in technology or facility reinforcement, etc.), and the administrative fees that the World BASC Organization charges their members for covering organizational running costs. These administrative fees can vary from US$800 to US$2,500 for the certification and from US$800 to US$2,000 for the annual maintenance. The tariff varies according to the socio-economic situation of the country and the economic sector to which the company belongs. BASC certification is valid for one year and can be renewed after passing a second security audit. Table 2 presents the average certification and annual maintenance cost for companies with different turnovers.

		Average value in US$			
Annual turnover US$	Number of companies	Implementation cost	Annual maintenance cost	Maintenance/ certification cost	Certification cost/ turnover
< 50,000	4	28,625	2,888	10%	≥ 57%
50,000–500,000	13	17,176	8,539	50%	3%–34%
500,000–1 million	13	13,585	6,698	49%	1%–3%
1 million–5 million	25	61,820	15,826	26%	1%–6%
> 5 million	35	52,742	28,484	54%	≤ 1%
Total	**90**	**34,790**	**12,487**	**38%**	

Table 2: Certification and Maintenance Average Cost for Different Turnovers (sample size 90)

Except for companies with a turnover between US$50,000 and US$500,000, the average cost of certification appears to be positively related to turnover (increase in turnover, higher cost of certification). However, the increase in the cost of certification is not proportional to the increase in turnover. For instance, for companies with an annual turnover of less than US$50,000 the certification cost was on average more than 57% of their turnover, while for companies with a turnover between US$50,000 and US$500,000 this percentage decreases drastically to a range between 1% and 34%. One more relevant result is that the maintenance cost in relation to the certification cost (see column: maintenance/certification cost) appears to be smaller (10%) for companies with turnovers of less than US$50,000 per year and higher (on average 45%) for companies with higher turnovers. It could be then concluded that the certification cost appears to be more expensive for companies with small annual turnovers (less than US$50,000) while the maintenance cost is proportionately more expensive for more affluent companies.

The potential opportunity costs generated by the deviation of company resources from the daily operational activities to work in the certification process were not quantified in US$. However, this potential opportunity cost was measured in terms of time and human resources required. Table 3 presents the average value for some measures of time and resources.

Time	*Average values*
Months necessary for certification process	8
Total hours of work for certification	2,337
Resources	
Number of employees involved in certification process	48
Number of employees involved/Total employees	23%
Time per resource	
Hours per person	49 (~ 6 working days)

Table 3: Measures of Time and Resources Required to Implement BASC (sample size 90 complete answers)

3.3.3 BASC Benefits

Based on an exhaustive supply-chain security literature review, 16 potential benefits related with voluntary supply-chain security programmes were identified and classified in the following three categories: (I) direct security benefits; (II) benefits for the company's efficient functioning under normal conditions; (III) benefits for the company's efficient functioning under high alert or post-disaster conditions. Respondents were asked to evaluate the degree of importance of these benefits for their companies. Figure 5 presents the list of benefits ranked from the most to the least important based on the respondents answers.

There was a general agreement between the companies regarding the most and least important benefits. More than 70% of respondents considered that the top five most important benefits belong to categories (I) (direct security benefits) and (II) (benefits for the company's efficient functioning under normal conditions). An average of 60% companies considered the direct, indirect cost savings and the reduction of insurance premiums benefits as of medium or low importance. On the contrary, there is certain disagreement concerning benefits such as quick recovery from general disasters and better Customs regulation and processes compliance, where 50% of respondents believe that these are highly important and the other half believes that their importance is medium, low or not applicable for their company.

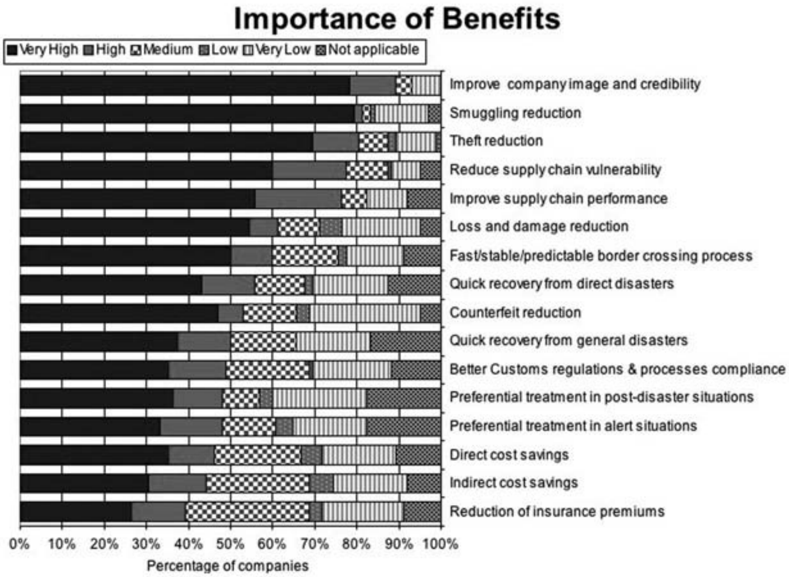


Figure 5: Potential Security Programme Benefits Ranked by Importance (sample size 102)

Furthermore, respondents were asked to explain which benefits they were expecting when the company embarked on the certification process and was indeed certified. Figure 6 presents the benefits percentage of companies that expected and obtained each of the benefits.

Figure 6 shows that attainments were higher or very close to expectations for almost all the security direct benefits (except for reduction of insurance premiums), for some supply-chain efficiency related benefits (such as the reduction of the supply-chain vulnerability and the improvement of the supply-chain performance) and in particular to improve company image and credibility, which was the most expected and the most attained (expected by 85% and obtained by 90% of the respondents). In contrast, it seems that benefits related with cost savings (direct and indirect), efficiency under high alert/post disaster conditions and facilitation of border crossing operations (fast/stable/predictable border crossing process and better Customs regulations and process compliance) were on average less attained than expected.

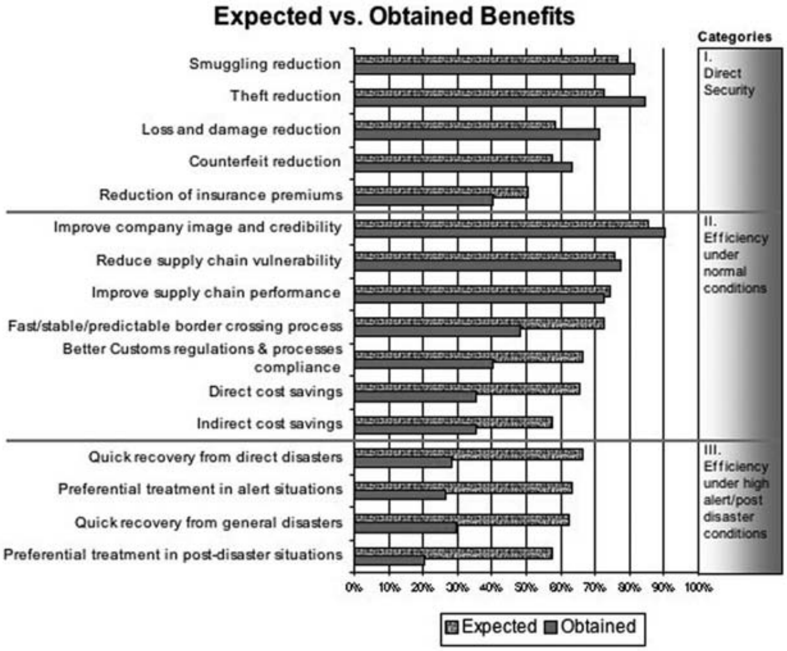


Figure 6: Voluntary Supply-chain Security Programmes Expected versus Obtained Benefits (sample size 102)

These results show that although the implementation of BASC programmes has been extremely useful in increasing security and as a consequence in improving corporate image, it has been difficult to translate this apparently less risky situation into cost savings. For instance, only 40% of the companies were able to obtain a reduction in their insurance premiums as recognition for their investments in reducing their exposure to risk. It seems that insurance companies are still not recognizing this type of programme as an important criterion for defining their premiums even though the insurance cost is a significant component of the security cost of an international trade transaction and is directly related with the risk exposure of the cargo.

For those benefits where attainments meet expectations the main interest is to understand which security measures contributed to achieve them. Section 5 provides some insights for solving this question by establishing some potential connections between benefits and security measures.

For those benefits where the attainments did not meet expectations there are three potential explanations: (a) the attainment of these benefits requires further efforts in addition to the security measures, therefore, companies that were not able to implement these additional efforts did not obtain all the expected benefits; (b) some security measures are not appropriate for producing the expected benefits, therefore, they should be changed or improved in order to achieve them; (c) companies claim that they did not get these benefits because they had not been exposed to disruptions or alert situations where they would have been able to prove the effectiveness of the security measures.

The first explanation may be valid for those benefits related with cost reduction. It is possible that security measures may have improved operational performance but not necessarily reduce their cost. Further efforts or changes may have to be enforced in order to achieve cost savings. The second explanation could be valid for benefits related with cross-border operations facilitation. For instance, having fast/stable/predictable cross-border operations not only depends on how security compliant the shipper is to the regard of Customs administrations; it also depends on how effective or complex the clearance process is, on the use of technology and human resources, on the coordination between border agencies, etc. Implementing security measures only at the shippers' functional level is not an appropriate measure for obtaining fast/stable/predictable border crossing. To get this benefit it might be necessary to use a holistic approach which could imply changes not only for the shippers operations but also for Customs administrations, port operators and for the coordination activities amongst these actors. Finally, the third explanation could be valid for those benefits related to efficiency under high alert/post disaster conditions, given that most of the companies might not have been exposed to such situations and therefore cannot prove whether they have obtained such benefits. Understanding which of the proposed hypotheses explains each result could be the object of future case studies in the field.

3.4 BASC Cost-Benefit Analysis

It is not a simple task to measure the cost-benefit relation of security investments. Implementing a supply-chain security programme can be compared to paying an insurance premium to be covered against the potential costs of suffering from an undesirable event (such as cargo contamination, border closure, cargo theft, etc). While in both cases the costs can be clearly identified (for the insurance it is the premium value and for the security programme it is the cost of implementing and maintaining the security measures), the benefits can be the result of one or more of the following reasons: (i) cost savings from reducing the probability or avoiding the occurrence of undesirable events (i.e. decrease in theft, counterfeit, loss or damage rates, reducing supply-chain vulnerability, avoiding Customs fees, loss of goodwill, etc.); (ii) secondary positive effects on existing operations (i.e. improving supply-chain efficiency due to better control and traceability, indirect cost savings, etc.); and (iii) improving the company's situation in relation to external actors (i.e. acquisition of new clients, preferential treatment at borders, etc.). Benefits for the first category result of avoiding costs; therefore, their quantification requires calculating the potential costs that could be incurred if an undesirable event occurs. For the third and fourth categories quantifiable benefits should be the result of more income, due to an increase in turnover or a decrease in operational costs. In both cases, the quantifiable benefits are not easy to estimate. In the first case the estimated benefits will never be exact if the undesirable event never occurs, and in the second case the benefits will be the result of other interacting variables (i.e. marketing function of the company, product quality, etc.) so it will be difficult to identify which part of the increased income corresponds to the security investments.

BASC member companies illustrate the existing difficulty in quantifying security investment benefits: while 93% of the respondents were able to estimate the total cost of implementing and maintaining BASC, only 40% were able to quantify some benefits and very few were able to explain where they originate.

Large variations where found when comparing the value invested in security with the value of the obtained benefits in companies that quantified their benefits. Out of this set of 34 respondents, half obtained benefits which were inferior or equal to their investment and the other half obtained benefits which varied from double to ten times the total cost of implementation and maintenance. Additionally, although several companies invested similar amounts of money in security they obtained significantly different quantifiable benefits. Even if some respondents were able to explain the reasons for such benefits, it did not sufficiently explain why companies making apparently the same effort obtained very different results. In spite of these difficulties the researchers provide some explanations for the variation in the results.

There are significant obstacles when quantifying benefits stemming from the prevention of an undesirable event. The estimation of these benefits depends on the perceived degree of risk faced by the company and the programme's capacity to reduce the probability that this risk will occur. For instance, the same security measure *will reduce* the probability that an undesirable event will occur within companies facing high risks and others facing low risks *to the same extent*. However, the companies most at risk will perceive higher benefits, because the potential savings from preventing undesirable events are higher than for the low risk companies.

There might be important differences in the items that were considered to calculate the cost of implementation and maintenance by each company. The relation between costs and benefits might depend on the situation of the company. For instance, a company where several security standards were implemented prior to starting the certification process will incur reduced cost in comparison to one which starts from zero.

Finally, the size of quantifiable benefits can depend on many variables—for instance, on the implemented security measures, on the maintenance activities or on the execution of any additional efforts. Better understanding of the connections between such variables could provide important insights to analyse the relationship between cost and benefits for security investments.

3.5 BASC Lessons

As discussed in the previous section, there are multiple barriers to quantify and explain the potential benefits derived from the investments in security programmes. Not being able to quantify the benefits creates obstacles to justify the investments. Not understanding the connections between cost, security measures and benefits prevents the possibility of creating cost-effective security programmes. In this section researchers assess this problem by exploring if there is any relationship between the number, type and cost of the implemented security measures with the number and type of obtained benefits.

In simple terms a security programme consists of a list of security measures. Given that in principle each security measure reduces the probability of occurrence of a certain identified risk, it could be argued that the more security measures are implemented the more benefits will be obtained. BASC companies have followed this same logic because they have tried to implement as many measures as possible. To test this hypothesis the number of implemented measures was graphed against the number of obtained benefits for each company in Figure 7. The graph shows that it is not possible to explain the number of benefits by the number of implemented measures. For instance there are several companies which implemented the same number of measures and while one obtained the maximum number of benefits (16) the other obtained zero. In order to avoid the potential bias given by the fact that not all the benefits and not all measures are applicable for all the companies[5] the following two percentages where graphed one against the other: (i) the number of implemented measures out of the total applicable for each company; and (ii) the number of obtained benefits out of those that were expected by each company. Figure 8 shows that neither in this case it is possible to say that the number of obtained benefits can be explained by the number of implemented measures.

[5] For instance, a company whose product is not counterfeited might have answered that the benefit of counterfeit reduction has not been obtained because they don't actually have this security problem. However, this doesn't mean that the programme cannot contribute to this benefit for companies which suffer from counterfeit.

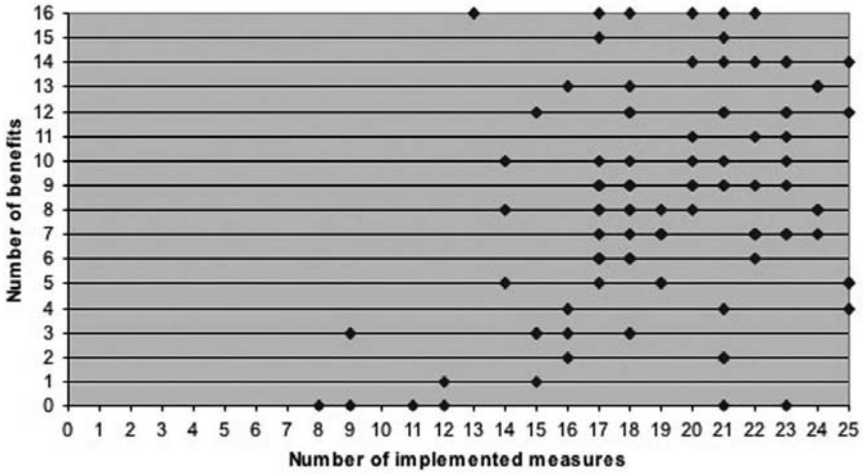


Figure 7: Relationship between Security Measures and Number of Obtained Benefits

The same graphic was done adding several control variables such as company's main activity (logistic service provider or manufacturer), size (large or SME), main reason to implement the programme (security or image), commercial relationships with US and/or EU and number of measures implemented from each category (facility, cargo, human resources, information and business partners management). Once again it was not possible to establish any significant pattern for any of the analysed groups of companies.

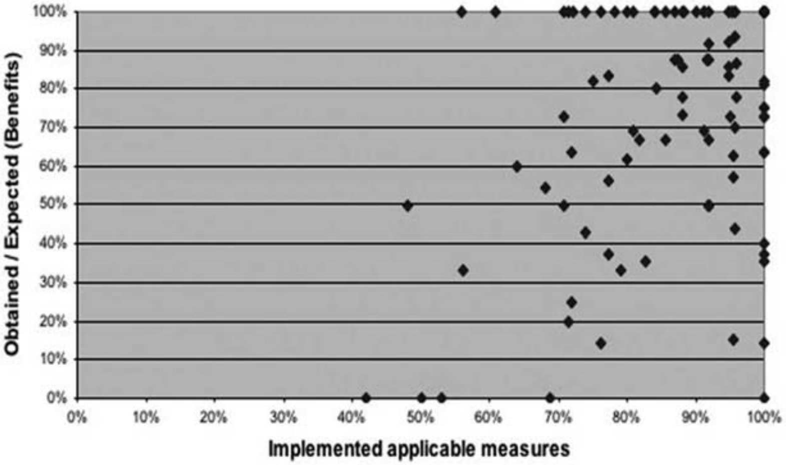


Figure 8: Relationship between Implemented Applicable Measures and Obtained Benefits

Given that it was not possible to establish any robust connection between the global efforts made with regard to security (represented as number of implemented measures) and the global effectiveness of these efforts (represented as the number of obtained benefits), it was decided to analyse the potential connection between effort (represented as cost of implementation) and effectiveness for each security measure independently. Respondents were asked to qualify each measure in terms of their implementation cost and efficiency in improving security. Two five-point Likert scales were used by respondents to qualify each security measure in terms of these two properties. Table 4 presents the different values and the corresponding meaning.

Implementation cost	*Effectiveness to improve security*
1 = 0–2,000 US$	1 = Very low effectiveness
2 = 2,001–10,000 US$	2 = Low effectiveness
3 = 10,001–50,000 US$	3 = Medium effectiveness
4 = 50,001–100,000 US$	4 = High effectiveness
5 = > 100,000 US$	5 = Very high effectiveness

Table 4: Qualitative Scales to Qualify Security Measures in Terms of Cost and Effectiveness

Once each measure was evaluated separately in terms of cost and effectiveness, analyses were carried out to establish which type of relationship exists between the cost of implementation and the effectiveness of security measures. Providing answers to this question could provide essential insights to designing cost effective security programmes. For instance, if effectiveness is positively related with the cost of the measure, companies with higher investments in security will be more likely to enhance security. On the contrary, should such relationships not exist, the creation of a cost effective supply-chain security programme would only require implementing low cost and effective security measures. Most of the answers indicated that all the 25 measures are cheap and highly effective. Figure 9 shows the percentage of answers for each possible combination between cost and effectiveness for all the 25 measures. It can be observed that 74%[6] of the answers point that all the measures cost between US$0 and US$10,000 and are high or very highly effective.

The analysis of joint cost and effectiveness answers doesn't provide much information about the differences in cost and effectiveness for the 25 security measures. However, by studying the cost and the effectiveness separately it was possible to establish how cost-effective each security measure is in relation

[6]. 74% = 14.7% + 9.1% + 13.6% + 24.3% + 3.6% + 7.5% + 1.4%.

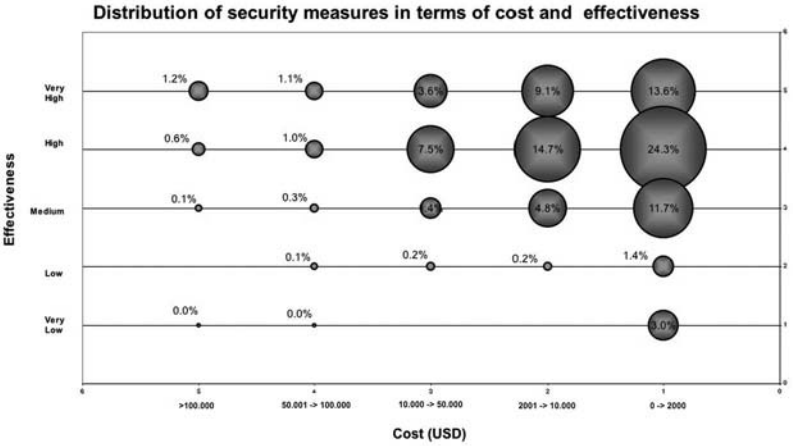
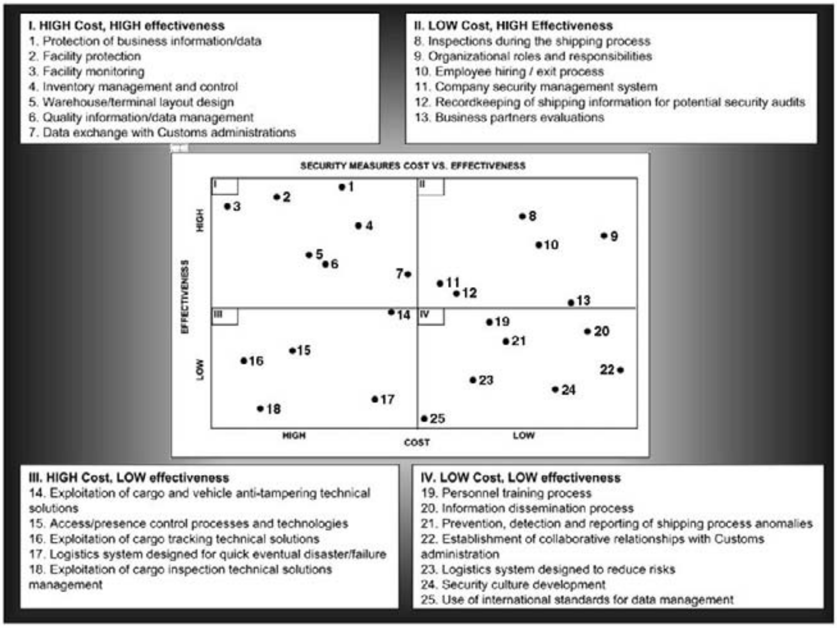


Figure 9: Number of Answers per Possible Combinations of Cost and Effectiveness

to the others. In order to do this, each security measure was ranked in terms of cost (from the one which was considered more expensive to the one whichwas consider cheaper by the higher percentage of companies) and effectiveness (following the same logic as for cost). Then these two ranks were combined in Figure 10, where the measures are classified into two levels of cost (low and high) and two levels of effectiveness (low and high).

No linear positive relationship between cost and effectiveness was found. On the contrary, four main groups of security measures which account for inverse and identical combinations of cost and effectiveness levels were identified. For instance, there are six of the 25 security measures which present a LOW implementation cost and HIGH effectiveness in relation to the others (for details see measures in group (II). In contrast to this group five of the 25 measures present the opposite combination: HIGH implementation cost and LOW effectiveness (for details see measures in group (III).



I. HIGH Cost, HIGH effectiveness
1. Protection of business information/data
2. Facility protection
3. Facility monitoring
4. Inventory management and control
5. Warehouse/terminal layout design
6. Quality information/data management
7. Data exchange with Customs administrations

II. LOW Cost, HIGH Effectiveness
8. Inspections during the shipping process
9. Organizational roles and responsibilities
10. Employee hiring / exit process
11. Company security management system
12. Recordkeeping of shipping information for potential security audits
13. Business partners evaluations

III. HIGH Cost, LOW effectiveness
14. Exploitation of cargo and vehicle anti-tampering technical solutions
15. Access/presence control processes and technologies
16. Exploitation of cargo tracking technical solutions
17. Logistics system designed for quick eventual disaster/failure
18. Exploitation of cargo inspection technical solutions management

IV. LOW Cost, LOW effectiveness
19. Personnel training process
20. Information dissemination process
21. Prevention, detection and reporting of shipping process anomalies
22. Establishment of collaborative relationships with Customs administration
23. Logistics system designed to reduce risks
24. Security culture development
25. Use of international standards for data management

Figure 10: Classification of Measures in Terms of Cost and Effectiveness

A closer analysis of the type[7] of measures that compose each of the identified cost-effectiveness groups, shows that there are certain types of measures which predominate for some groups or on the contrary are completely absent. For instance, the HIGH cost and HIGH effectiveness group is composed only of facility management and information management measures. The LOW cost and HIGH effectiveness, as well as the LOW cost and LOW effectiveness groups are composed of measures from all categories, except from facility management. Finally, the HIGH cost and LOW effectiveness group is composed mainly of measures related to cargo management, and some related to business networks and management systems and facility management. Figure 11 presents the percentage of different types of measures that compose each cost-effectiveness group.

[7] The type of measure refers to the previously described categorization of security measures: facility management; cargo management; human resource management; information management; and business network and company management systems.

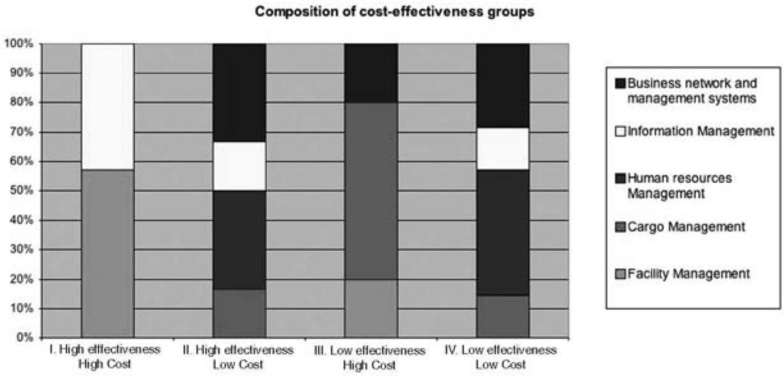


Figure 11: Types of Measures Composing each Cost-effectiveness Group

It is interesting to see that those groups where the cost is high, have higher concentrations of measures from the same type, on the contrary those for which the cost is low tend to have measures from almost all the categories. These results suggest that measures related to facility management are more likely to be costly to implement and less effective than the others. In addition, understanding why certain measures are less effective or more expensive than others and establishing if it is possible to transform them into better security measures could provide important insights to design cost effective supply-chain security programmes. Figure 12 illustrates the potential strategies to enhance a set of measures which compose a security programme.

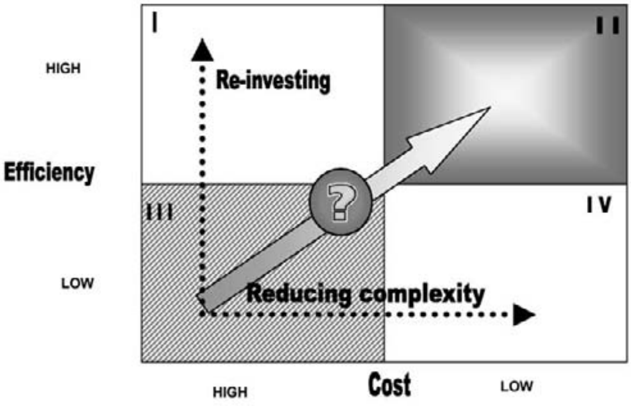


Figure 12: Identification of Low Cost Effective Security Measures

Up to this point some insights have been achieved regarding the relationship between the effort (cost) and effectiveness of the investments in security. However, the successful implementation of a supply-chain security programme should not only aim to identify the cheapest and most effective security measures; it should also give priority to those measures that can contribute to create the benefits that are highly important for the company. In order to achieve this goal it would be desirable to identify any existing strong connections (statistically significant associations) between certain benefits and measures. Should such connections exist, the necessary statistical analysis to study it is not included in the scope of this report. However, in Table 5 we present some potential connections that were reported by respondents when asked about the most important benefits obtained by their companies and the corresponding measures that were implemented to achieve them.

These results suggest that supply-chain efficiency related benefits are the result of certain security measures which contribute to security and at the same time create operationally desirable conditions that are conducive to improving efficiency. For instance, some respondents explained that certain security measures reduced the time and variability of some of the company's logistics operations and improved cargo visibility and control, which all together contributed to reduce the vulnerability of the supply chain. Others reported an improvement in logistics processes and level of service, which contributed to the improvement of supply-chain performance. In spite of these examples, which connect certain measures and benefits, there were several respondents who argued that the obtained benefits were the result of all the implemented measures and were not able to establish any relevant connections.

Measures implemented	*Obtained benefits*	*Type of benefit*
Logistics process control, information management on-time and collaboration with authorities	Anti-smuggling and anti-theft	**Direct security**
Supply chain traceability, identification and control of process responsibilities (knowing who does what at what moment)	Anti-loss and damage	
Document revision and training employees to detect and report anomalies	Decrease containers theft	

Measures implemented	*Obtained benefits*	*Type of benefit*
Documents protection and processes supervision	Better process control, processes bottlenecks and mistakes reduction	**Supply chain efficiency**
Use of security seals, supervision of deviations in vehicles travel times, access control with bar code system	More control over operations, personnel, documents and cargo	
Access control (working with closed doors), registration of visitors, adequate information management, monitoring of vehicles 24 hrs, use of security seals	Improve internal organization, decrease disruptions and hence insurance premiums	
Creation of strategic alliances, risk evaluation of clients and suppliers, adequate employees selection process, establishment of security best practices agreements with clients	Increase of 24% of the business, increasing the turnover by around $2 million	**Company image**
Inspection of containers and vehicles while in storage (this company has used this extra security activity to sell their clients a corporate image which promotes very high security standards)	Client recognition of improved security level. Differentiation from other competitors	

Table 5: Samples of Connections between Benefits and Measures Identified by some Respondents

3.6 Attitude and Awareness with New Supply-Chain Security Environment

There are two significant concerns regarding the future development of the supply-chain security environment. For companies which are not involved in security programmes, the main issue relates to the real benefits that are to be obtained through the programme's implementation and whether they justify the cost of going through the process of certification. For companies which are already certified, such as BASC members, the immediate issue is whether there will be a supplementary effort involved in being certified by another programme. In this section we try to illustrate this situation by highlighting some opinions of BASC participant companies regarding the incentives that governments should provide for companies involved in security programmes and the recommendations and concerns about the future development of new supply-chain security initiatives.

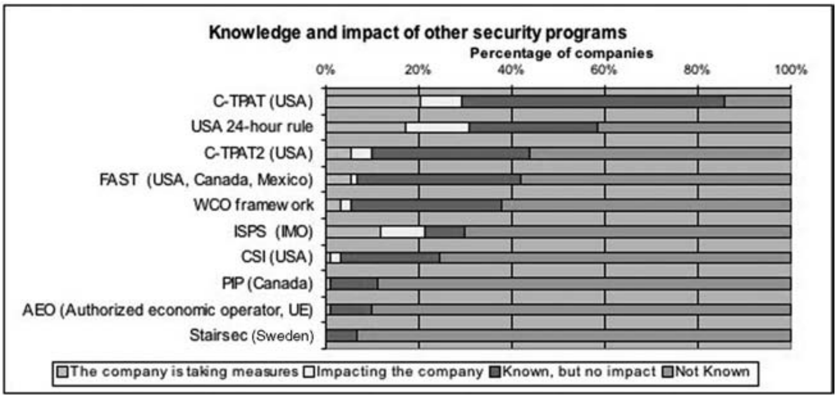


Figure 13: Respondent Awareness of other Supply-chain Security Programmes (sample 102)

To highlight the importance that *other* supply-chain security initiatives have for BASC member companies, the researchers measured the degree of awareness and current impact in relation to 10 other existing/emerging initiatives. BASC member companies tend to be more aware of US initiatives. For instance, the only initiative that is known by about 85% of the companies is C-TPAT which is the US initiative to strengthen overall supply-chain and border security management. The remaining most well known initiatives are the 24-hour rule, C-TPAT2, FAST and the WCO framework of security standards. Ninety per cent of the initiatives exert an impact on only a small percentage of companies and in some cases even stimulate the implementation of some measures to deal with them. Figure 13 presents the distribution of the responses.

Respondents were asked to indicate which incentives they believe governments should provide for companies in order to be involved in voluntary security programmes. They identified 11 potential incentives that are presented in Table 6 ranked from the most to the least commonly cited.

Proposed incentives for companies involved in security programmes	*Percentage of companies*
1. Provide preferential border-crossing treatment: simplified procedures, reduced physical inspections and clearance time, stability and consistency and information transparency concerning customs regulations	39%
2. Reduce taxes proportionally to security investments and/or payment facilitation	28%
3. Provide security training courses or finance them	14%

Proposed incentives for companies involved in security programmes	*Percentage of companies*
4. Reduce tariffs for security related products (e.g. cameras, CCTV systems etc.)	5%
5. Finance projects to develop or implement technological solutions for security	4%
6. Ensure flexibility (when things go wrong in spite of the implemented security measures (i.e. reduce customs penalties)	4%
7. Provide operational cost reductions (i.e. energy, water, property tax, communication, port services)	3%
8. Support for new foreign market acquisitions	1%
9. Publicize the company's commitment to security	1%
10. Permit global certification for multinationals	1%
11. Make more efficient the process to obtain a security certification	1%

Table 6: Potential Government Incentives for Companies Involved in Security Programmes (sample size 102)

In addition respondents provided some general recommendations for the current security policy makers and programme developers. In the following section, their most relevant ideas are presented classified into 10 main categories.

I. Enforceability and certification recognition

- Seek government support for companies involved in security programmes.
- Make voluntary security programmes a minimum requirement for participating in international trade operations.
- Remain strict when granting certification.
- Stimulate increasingly intensive collaboration with local and international authorities.

II. Programme design

- Keep it simple: stimulate the implementation of simple and effective systems.
- Try not to spend excessive amounts on security. The key is to focus on the weak spots.
- Find a balance between security imposed controls and the need for free movement of people and merchandise.

III. Sharing information

- Stimulate sharing: experiences, best practices and results. Security is highly based on experience. However, there is a lingering tendency to disclose this type of information.
- Reinforce communication between certified companies through meetings, presentations of real cases by Customs and authorities.
- Look for effective mechanisms to update knowledge in security issues (i.e. e-learning).

IV. Promote alliances to create end-to-end security

- Create strategic alliances along the supply chain (security associations etc.).
- Promote the creation of alliances between suppliers and clients to work with the same security policies.

V. Exploit the programme's potential for creating more benefits

- Convince companies that such programmes are genuinely beneficial for operations; programmes should not be only about obtaining certification. Presently, it is difficult to see results because not all the actors interacting in supply chains have the same level of security.
- Develop the certification to become a working tool to create real benefits for companies. It should not be seen only as a way to improve the company image, a commercial brand or as a client-based market requirement.

VI. Programme implementation

- Raise management decision-making security issues.
- Emphasize employee security awareness and enforce supervision to guarantee real implementation of security policies and procedures.
- Facilitate the certification process to eliminate unnecessary transactions and inspections. Promote the integration/mutual recognition of different programmes (ISO, TAPA, BASC, WCO).

VII: Globalization and standardization

- Avoid multiple programmes while they mean dispersed efforts and duplicate information.
- Stimulate the creation of agreements with other countries to obtain recognition for BASC certification in foreign countries.
- Globalize and generalize security programmes to unify security standards.

- Aim to use BASC as a starting point to obtain other certifications such as C-TPAT.

VIII. Programme cost—Open access

- Note that the cost of security programmes can be very low compared to the benefits.
- Reduce the participation cost for small- and medium-size enterprises (SMEs).
- Provide economic support to help companies implement these programmes.

IX. Awareness of the risks involved in these programmes

- Aim to mitigate the risk that those who carry out illegal activities can use certified companies to attain their objectives.

X. General security issues

- Security results in monetary benefits, lower risks and fewer problems.
- Security sometimes leads to a general feeling of confidence.
- Security should not be considered an ultimate goal but as a means to obtain better results.

4 CONCLUSIONS

BASC is a successful example of a private initiative that has become a consolidated organization promoting supply-chain security standards amongst its members.

This study presents for the first time empirical data about the cost, efforts required and effectiveness of supply-chain security programmes. One of the two most relevant results are that the benefits of a supply-chain security programme are not likely to depend only on the number of security measures and that security effectiveness is not linearly and positively related with the cost of security measures. Although it was not possible to establish any significant connection between the type, cost or quantity of security measures and the obtained benefits, it was possible to identify security measures which appear to be high effective and low cost in comparison with the others and vice versa.

While the cost of the programme has been quite accurately estimated, there were significant difficulties in quantifying the benefits. Qualitative benefits were proven to exist, but respondents were hardly able to establish the quantifiable gains of these achievements. This problem should be further studied, but in this study we provide the first identification of low cost high effective measures.

BASC members' experience provides important guidelines for the future development and globalization of supply-chain security standards. Even though most of the sample companies decided to become involved in BASC because it was required by the international trade market, results show that they benefited from it in multiple ways, including contributions to supply-chain efficiency. Despite this positive experience, most of the certified companies did not receive preferential border treatment, especially not at foreign borders. The capacity of Customs administrations and other government agencies in providing such benefits will lead to two possible future scenarios: (i) security certification becoming a true "secure" and "non-secure" trader differentiator; or (ii) security certification becoming a minimum requirement for companies to participate in international trade. Future research should clarify the various parameters around these two scenarios.

It is also pertinent to highlight that businesses expect significant incentives from governments for participating in these programmes, such as special border treatment and tax reductions proportional to investments in security. Companies involved in private initiatives much like BASC members generally assume the entire cost of enhancing security within their supply chains. Future research should also help to determine whether new programmes should be primarily promoted and financed by the public sector or whether the efforts and the costs should be spread between the private and the public sectors.

Acknowledgements

BASC: Ms Mayra Hernández de Cavelier, World BASC Organization president.

Mr Diego Castillo, BASC Chapter Pichincha, Mr Stephen R. Tiernay, BASC Dominican Republic, Jose Luis Hernández Valentino, BASC Chapter Carabobo and John Reinberg, BASC Chapter Ecuador; plus all BASC member respondents to the study.

EPFL and IML: Dr Philippe Wieser, Executive Director of Master in Management of Logistical Systems; Prof Michel Bierlaire.

HEC Lausanne and CBRA: Mr Juha Hintsa, Mr Vladlen Tsikolenko.

HEC University of Lausanne: Prof Ari-Pekka Hameri; Prof Erkko Autio.

HEC—IUMI: Prof Jean-Claude Usunier, Mr Vincent Vandersluis.

REFERENCES

Bodner, N. (2003), The Weakest Supply Chain Link, five categories of food manufacturing supply chain risks, *Food Logistics*, pp. 42(1).

Christopher M. (2001), An integrated Model for the Design of Agile Supply Chains, *International Journal of Physical Distribution & Logistics Management*, Volume 31, Number 4, pp. 235–246(12).

Gutierrez, X. and Hintsa, J. (2006), Voluntary Supply Chain Security Programs: A Systematic Comparison, *ILS 2006 The International Conference on Information Systems, Logistics and Supply Chain*, Lyon, France. May 15–17, 2006.

Hintsa, J., Gutierrez, X., Wieser, P. and Hameri, A. (2006). Supply chain security management: a general overview, *ILS 2006 The International Conference on Information Systems, Logistics and Supply Chain*, Lyon, France. May 15–17, 2006.

Schneier, B. (2003), Beyond Fear: Thinking Sensibly about Security in an Uncertain World, New York: Copernicus books, 2003.

Official program documents

European Commission (2005), The Authorized Economic Operator, TAXUD/A4/SA D(2005). March 2005.

ISO TC 8/SC 11(ISO/WD 0, ISO TC 8/SC 11/WG 1), Custody Best Practices to enhance Supply Chain Security: 2 May 2005.

New Zealand Customs Service, Secure Exports Partnership, Important Information for applicants. December 2003.

Partners in Protection (PIP) Importer security recommendations [online]. Available at: http://www.cbsa-asfc.gc.ca/general/enforcement/partners/imp_recommend-e.html.

StairSec®, White Paper on Accreditation of Operators and the Supply Chain Security, A way forward—Proposal to connect national customs accreditation systems and create an authorized supply chain security (pilot).

TAPA 200-2005, Freight suppliers' minimum requirements, January 2005.

US Customs and Border Protection, C-TPAT validation process guidelines. January 2003.

World BASC Organization, BASC standards, 2002.

World Customs Organization, Framework of Standards to Secure and Facilitate Global Trade. June 2005.

CHAPTER 11

TRADE DISRUPTION INSURANCE: AN EFFECTIVE FORM OF RISK MANAGEMENT IN SUPPLY-CHAIN SECURITY?

Risto Talas

Cass Business School, City University, London, UK

Abstract
The chapter evaluates the effectiveness of trade disruption insurance (TDI) as a form of risk management in supply-chain security. The chapter examines how TDI works, how it complements ISO/PAS 28000 and argues that a mandatory introduction of TDI could accelerate the introduction of standards in supply-chain security technologies.

1 INTRODUCTION

Lee and Wolfe in their article "Supply Chain Security Without Tears" were instrumental in being one of the first to draw the parallel between the quality movement and the newly enforced security regimes visited upon the world by the security initiatives of the 2002 US Maritime Transportation Security Act (MTSA). The Customs-Trade Partnership Against Terrorism (C-TPAT) initiative featured for its parallel with the emphasis on prevention; the Container Security Initiative (CSI) similarly featured for its parallels in source inspection; and identifying, tracking and improving quality translated into container tracking and supply chain visibility.

The temptation to draw the parallels must have been overwhelming in early 2003 when the article first appeared as many of us struggled to fathom the impact that the introduction of the ISPS Code and the MTSA would have, and supply-chain security was a phrase which made many appearances at conferences where delegates would solemnly nod their heads about the need for "improved 'intel' post 9/11" while not really knowing what it was all about.

Three years on, the International Organization for Standards has introduced ISO 28000:2005 Publicly Available Specification "Specification for security management systems for the supply chain" (ISO/PAS 28000), the first comprehensive attempt to tackle supply-chain security threats.

This chapter is in three parts. In part one, I will show that trade disruption insurance (TDI) is effective in insuring a company's net profit and additional costs and expenses against the risk of an act of terrorism directed at the company's supply chains. In part two, I will show that TDI complements ISO/PAS 28000 in managing supply-chain security risk. In part three, I will argue that by mandating TDI cover for C-TPAT members, it may be possible to solve the problem of standardization of supply-chain security technologies.

2 TDI AS AN EFFECTIVE SOLUTION AGAINST SUPPLY-CHAIN SECURITY RISK

Trade disruption insurance (TDI) protects against loss of profits and extra expenses arising from an insured event in the assured's supply chains. The uniqueness of TDI is that it will respond even if the assured's property is not damaged, unlike traditional forms of insurance cover.

Christopher (2005) lists seven steps of supply-chain risk management. First, the organization must understand the supply chain; secondly, it must improve the supply chain; thirdly, it must identify critical paths and nodes; fourthly it must manage the critical paths; fifthly, it must improve network visibility; sixthly, it must establish a supply-chain continuity team; and finally, it must work with suppliers and customers to improve supply-chain risk management procedures. TDI features in the fourth step. It is effective as a risk management tool by mitigating the effects of the threats to the organization's critical paths and nodes (as well as the supply-chain overall). I will describe two examples of TDI. For purposes of confidentiality, I am unable to disclose more than the outline details.

(A) The first is a TDI policy bought by a company where the majority of their business relied upon certain specific roads and rail lines into a major port city remaining open at all times. The insurance cover they purchased protected their supply chains into and out of the city from being blocked owing to an act of terrorism, or by the order of the local or national authorities.

The insured events were defined as:

> "Partial or total closure by the appropriate authorities or unintentional physical blockage of any berth, port, bridge, channel, canal, waterway, road or railway line . . . by, under, or by the lawful order of the police, local or national authority or government . . . "

An act of terrorism was defined as follows:

> " . . . an Act of Terrorism means an Act, including the use of force or violence, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organisation(s), committed for political, religious or ideological purposes including the intention to influence any government and/or put the public in fear for such purposes."

The insured events also included strikes, riots, civil commotion and malicious damage.

The overall sum insured was $100,000,000 for each and every loss and in the aggregate in the policy period. The period of the policy was 12 months and the excess was five days commencing with the date of the occurrence of an insured event. The policy was designed to respond to the insured event by paying the net loss which was defined as the assured's net profit lost during the period of indemnity relating to that proportion of the insured's revenue which is lost by the occurrence of an insured event provided such revenue was connected to a contract at the time of the occurrence of the insured event.

(B) The second example concerns an importer in a Latin American country whose businesses were based in four named ports. The policy is similar to the one above in that it also covered acts of terrorism and included strikes, riots and civil commotion as well as malicious damage. However, the policy also included:

> " . . . physical damage or physical destruction to/at the scheduled ports and/or key transport infrastructure within a ten mile radius of the scheduled ports directly caused by war, civil war, revolution, rebellion, insurrection or civil strife arising there from or any hostile act by or against a belligerent power."

In addition, the policy covered

> " . . . Physical damage or physical destruction or Physical loss to/at the scheduled ports and/or key transport infrastructure within a ten mile radius of the scheduled ports from: Fire, lighting, explosion, looting, natural phenomena, overflowing water courses, pipe breakage, flood, rain filtration, avalanche, aluvion, landslide, weight of snow or ice, hail, wind, sea swell, sea quake, tsunami, sprinkler leakage, volcanic eruption, earthquake and/or fire following, storm, aircraft and/or objects falling therefrom, smoke, spontaneous combustion, vehicle impact, debris removal, collapse of buildings, subsidence, impact with fixed or floating objects including vessel impact, port blockage, spillage or general, bulk or IMO cargo."

The overall sum insured was $10,000,000 each and every loss and in the annual aggregate with each of the businesses in the ports having their own maximum daily loss amount.

Both of the examples of trade disruption insurance above demonstrate that the threats to supply chains can be insured, even in the absence of physical loss or damage to the insured's property.

It is effective in insuring a company's net profit and additional costs and expenses against the risk of an act of terrorism directed at the company's supply chains, and as such is an effective form of risk management for supply-chain risk managers.

3 TDI AND ISO/PAS 28000: COMPLEMENTARY TOOLS IN MANAGING SUPPLY-CHAIN RISK

In a recent article in *Telematics Update* magazine (Telematics Research, 2006), I asked (without proposing an answer) how are the interests of supply-chain managers served by the raft of new supply-chain security initiatives and legislation on both sides of the Atlantic? Their job is concerned as much with dealing with all forms of supply-chain risk as with the environmental risks where the supply-chain security risks fall.

Christopher (2005) refers to five potential sources of risk to business disruptions which supply-chain risk managers face. In supply risk, they must consider how vulnerable their business is to disruptions in supply. In demand risk, the key is volatility and the bullwhip effect possibly causing demand amplification. In process risk, the supply-chain manager is confronted with process resilience and identifying the bottlenecks in the supply chain. In control risk, the issues concern the company's own internal control systems and their effect on demand.

Only when considering environmental risk are the impacts of external events on the supply chain directly assessed. In short, in only two of the five categories are supply-chain security risks overtly considered: supply risk and environmental risk. What then does this say about the attitude of supply-chain managers to the risks of supply-chain security? In my opinion, they feel that their role is not about saving the world, but ensuring that they can continue shipping, sourcing, replenishing and reaching markets before the competition.

Lee and Wolfe's article highlights the parallels between the quality movement and supply-chain security. These same parallels are clearly apparent between ISO/PAS 28000 and ISO 9001 (quality management systems) and Annex A of ISO/PAS 28000 describes the correspondence between them. There are many grounds for basing ISO/PAS 28000 on ISO 9001.

First, the security risk assessment process set out in 4.3.1 shall

> " . . . consider the likelihood of an event and all of its consequences which shall include physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action . . . operational threats and risks etc."

The emphasis is on identifying all of the threats to the organization's supply chains, not only the upstream and downstream threats. The equivalent in ISO 9001 concerns customer focus, determination of requirements related to the product and review of requirements related to the product.

Secondly, in section 4.4.7 "emergency preparedness, response and security recovery", the organization shall

> " . . . establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them."

Again, the procedures are concerned with preventing and mitigating the likely consequences from any security incidents and emergency situations. The equivalent in ISO 9001 concerns control of nonconforming product.

However, section 4.4.6 "Operational Control" is concerned that the organization shall ensure that the operations and activities listed in 4.4.6 (a) to (f) are carried out under specified conditions by

> “ . . . evaluating any threats posed from upstream supply chain activities and applying controls to mitigate theses (sic) impacts to the organisation and other downstream supply chain operators . . . ”

Notwithstanding that the risk assessment process described in section 4.3.1 and the emergency response and recovery planning in section 4.4.7 address all possible threats to the organization’s supply chain, the key section on operational control of those threats refers only to threats upstream and downstream in the supply chain. While threats external to the supply chain are considered in the risk assessment process, their mitigation and control are absent from the key part of ISO/PAS 28000. This is explained, at least in part by the equivalent sections of ISO 9001 which are concerned with product quality and design and not by external influences.

The question that then arises is how effective ISO/PAS 28000 is at addressing external threats to the supply-chain, notwithstanding that they may have been identified in the risk assessment process (section 4.3.1) but not tackled in the key section on operational control (section 4.4.6)? The answer, I believe, is that ISO/PAS 28000 is not designed for this purpose. The translation of quality management into supply-chain security has resulted in the issue of drafting procedures to tackle threats external to the supply chain being left out. Operational control is concerned solely with risks from within the supply chain, upstream and downstream.

If we use the analogy of a water main as our supply chain and the Water Board as the organization that is ISO/PAS 28000 compliant, the Water Board’s risk assessment (section 4.3.1) states that there is a risk of cowboy workmen digging up the road and putting holes in the water main. Furthermore, the Water Board’s emergency preparedness, response and recovery plan lists the procedures for shutting off the mains and sending out a team to repair any leak caused by cowboy workmen breaching a water main. However, the Water Board’s day-to-day operational control (section 4.4.6) of the water mains is concerned solely with identifying and plugging any leaks or dealing with contamination that arise from corrosion of the pipework, flanges or the introduction of any unwanted foreign bodies by the sewage treatment works upstream. That is, the Water Board does not patrol the streets looking for cowboy workmen and reporting them to the local council authorities if they do not have the necessary permits to dig up the road. This role is reserved for the council workers with clipboards—for this read national intelligence agencies.

To extend the analogy further, the International Ship and Port Facility Security Code (ISPS Code) helps to tackle any potential break-ins at the Water Board’s pumping stations and protects the pipework in between (i.e. the ports and on international sea voyages between ports). C-TPAT aims to protect the sewage treatment works, pumping stations and pipework that serve the local community of America, but is a voluntary neighbourhood watch scheme.

In order to tackle the cowboy workers (terrorists) from digging up the road and putting holes in the pipes (attacking supply chains), the ISO/PAS 28000 compliant Water Board has two organizations to which it can turn. The first is the council workers with clipboards (intelligence agencies) who are tasked with tracking down the cowboy workmen. The second is the TDI underwriters who will pay for the loss of net profit and the costs and extra expenses suffered by the Water Board.

The purpose of the analogy is to demonstrate that an ISO/PAS 28000 compliant organization will have conducted extensive risk assessments and drawn up comprehensive emergency response plans to tackle supply-chain security threats, but that the management of the threats external to its supply chains is effectively achieved through the use of TDI. TDI complements ISO/PAS 28000 by mitigating the effects of external threats to the supply chain not sufficiently tackled by section 4.4.6.

4 TDI AS AN EFFECTIVE TOOL FOR STANDARDIZING SUPPLY-CHAIN SECURITY TECHNOLOGIES

Mandatory regulation through legislation is one of the many banes of the followers of liberalism. However, from time to time it has its uses. I will attempt to argue that mandatory introduction of TDI cover for C-TPAT members will solve the problem of standardization of supply-chain security technologies.

The first question to ask is: why TDI in particular? The answer to this is that, as mentioned in part one, TDI cover protects C-TPAT members from the effect of a supply-chain security incident, regardless of whether their property was damaged by the security incident. One set of underwriters protects the insured's net profit and extra expenses from an event which affects his or her entire supply chain, even the parts not under the insured's control.

The second question to ask is: why is having only one set of underwriters such a crucial factor? I will return to this later.

If TDI were to be mandated, let us look first at the immediate effects. Insurance business created through legislation is much desired among underwriters. Insurers are gifted with a new class of business: they immediately set to work on drafting the terms and conditions of the insurance cover, identifying their target market, arranging reinsurance cover and then pricing the risk so they can make a net profit based on forecast premiums and claims after allowing for reinsurance costs. Another effect is also very noticeable: many insurers will enter the market.

If TDI cover were to be mandated for C-TPAT members, then overnight almost 10,000 potential policyholders require insurance cover. They would be inundated with offers of cover by their existing insurance brokers who in turn would very quickly assess which underwriters are providing TDI cover. The pricing of TDI insurance would crash from its current levels owing to the enormous influx of TDI underwriting capacity.

In a matter of six months to a year as the claims come in, underwriters will realize that TDI is being underwritten at uneconomic levels. There are two options open to underwriters at this point: raise the premiums or introduce alternative mandatory forms of risk management. Raising the premiums on the first renewal (12 months after the introduction of TDI as a mandatory class of insurance) will cause C-TPAT members to shop around for a better deal, the switching costs being naturally low for mandatory TDI cover. This will continue to keep pressure on TDI premium levels.

The only alternative is for underwriters to introduce further mandatory measures which are not premium-related. These additional measures relate to how the supply chains are protected. In particular, the measures relate to the technical specification and operation of radio frequency identification (RFID) technology and its deployment. Further measures along the lines of GPS tracking and monitoring technology will be introduced to reduce the risk profile and claims record for underwriters.

The power of underwriters is not to be underestimated. In July 2005 the Joint War Committee (JWC) of the London insurance market decided to declare the Malacca Straits a war zone for additional premium charging purposes, as recommended by their security advisers. Marine war insurance cover is underwritten on a worldwide basis, subject to certain excluded areas which attract payment of an additional premium. The effect of the decision by a handful of insurance professionals in London was (amid uproar from southeast Asian shipping associations) to force the navies of the littoral states to work together to reduce the effects of piracy in their territorial waters.

Mandatory TDI could have similar effects if the leading underwriters were to demand that C-TPAT members adopt certain RFID tracking and monitoring technologies. Standardization would quickly ensue as underwriters pushed for adoption of certain minimum standards. This answers the question: why is having only one set of underwriters such as crucial factor?

The final two questions to ask are: why would the Customs and Border Protection (CBP) Agency wish to mandate TDI for C-TPAT members and how could it do it? The answer to the first is that CBP has for a long time made the case for not mandating security standards for C-TPAT to ensure that best practice is adopted by all members. However, if TDI underwriters were to mandate the minimum security standards, they do so against their own insurance loss records related to security incidents. The minimum mandated security standards are not theoretical but are borne out of actual underwriting experience, and more importantly, mandated by industry itself, independently of government, in order to protect itself.

The answer to the final question of how TDI could be mandated for C-TPAT members, is that the US Congress already has form in this area. In the aftermath of 9/11, the Bush Administration signed into law the Terrorism

Reinsurance Act (TRIA). TRIA established a temporary Terrorism Risk Insurance Programme of shared public and private compensation for insured commercial property and casualty losses arising from an act of terrorism, as defined in the Act. The main effect was that it forced the reinsurers of US property and casualty business, who were mainly outside the United States, to provide capacity for terrorism insurance cover for US citizens.

By the very nature of trade disruption insurance, its worldwide reach and the quirks of the insurance industry, the introduction of mandatory TDI could help introduce the minimum standards of supply-chain security technologies that industry is waiting for and accelerate their adoption.

5 CONCLUSION

Trade disruption insurance is unique among insurance products. It has been shown to be versatile in responding to events where no physical damage to property has occurred, and thus will respond where other insurance products do not. As a risk management tool for supply-chain managers, its importance cannot be underestimated. It has been shown to be a complementary tool to ISO/PAS 28000 for tackling the risk management of external security threats to supply chains. Finally, its mandatory introduction for C-TPAT members could help to accelerate the standardization and adoption of supply-chain security technologies that industry and nations require to secure their supply chains.

Acknowledgements

I would like to express my gratitude to John Eltham and Rupert Sawyer of the Special Risks Unit of Miller Insurance Services for their kind assistance during the preparation of this chapter. However, the views expressed within it are entirely my own and I take full responsibility for its content.

REFERENCES

Christopher, M. (2005), *Logistics and Supply Chain Management: Creating Value-Adding Networks*, FT Prentice Hall.

International Standardization Organization, *ISO/PAS 28000/2005: Specification for Security Management Systems for the Supply Chain*, ISO: Geneva.

Lee, H. and Wolfe, M., 2003, "Supply Chain Security without Tears", *Supply Chain Management Review.*

Telematics Update On-line, 2006, *http://www.telematicsresearch.com/PDFs/telematics_update_magazine_35.pdf*, Issue 35.

CHAPTER 12

THE CO-EVOLUTION OF SAFETY CULTURES AND CRISIS MANAGEMENT CAPACITIES IN MARITIME TRADING SYSTEMS

Paul Barnes and Richard Oloruntoba

Queensland University of Technology, Brisbane, Australia

Abstract:
This chapter investigates an alignment of issues in security, risk and vulnerability analysis to present a comprehensive framework for designing an integrated safety-crisis culture across maritime supply chains and associated workplaces. The framework examines systems and processes for training, including needs analyses, covering crisis management capacities that enhance vulnerability analysis in maritime trading systems and the security assurances of supply chains. A combination of primary and secondary data sources from maritime and related industries in Europe and the Asia-Pacific region will be applied in a comparative analysis of practices and theoretical approaches to safety and crisis response. The scope of the chapter is limited to the requirements for designing, developing and implementing safety and crisis management cultures in organizations across maritime supply chains. The study reinforces the unique security challenges in the maritime operating environments and in regional port settings. It also details a selection of innovative strategies for mitigating these issues and challenges and in generating a capacity to anticipate some types of crisis. In summary, the authors find the need for development of flexible—yet specific practices—that must be embedded in the operational and managerial repertoire of commercial participants of maritime supply chains internationally. These practices (via the organizational culture) must be adaptive to emergent conditions yet grounded in professional knowledge.

1 INTRODUCTION

It has been observed that organizations in the maritime industry need to operate faster, better and be more cost-effective than in the past. In fulfilling this need managers must constantly develop and operate strategies and policies enabling such prosperity (Panayides, 2006). Each transaction or movement of goods across a supply chain occurs within a regulatory regime consisting of commercial and national regulations, and enforcement mechanisms governing the structure and operation of the supply chains for air and ocean-based trade. The focus of these regulations has shifted in recent years from safety and trade facilitation to include security outcomes (Willis and Ortiz, 2004). To this end what were once recognized as trading boundaries have become "security" boundaries (Suárez de Vivero and Rodríguez Mateos, 2004).

In parallel with this global "securitization" a range of emergent risk-related phenomena such as climate change, public and animal health crises, invasive pests and inter-dependencies within and across systems of infrastructure, create significant problems of governance for the private and public sector alike (OECD: 2003, 2006). Unmitigated disturbances from such sources are likely to generate cascading impacts propagated along unexpected pathways and fault lines throughout commercial and institutional segments of established and establishing economies. The potential for rapid spread of consequences, geographically and virtually, can render a comprehensive understanding of a crisis's context beyond the grasp of competent authority.

Maritime industries are not immune to crises both from natural causes and human intent. An absence or underdevelopment of effective crisis management capability within many organizations has been noted extensively in the literature covering industrial disasters in addition to business and organizational failure.[1] Crises often create situations that cannot be anticipated, so "warning sign" detection is critical as is a tested ability to respond to emergencies quickly and effectively (Boin and Lagadec, 2000). The need to have trained and responsive crisis management systems, personnel and related capacities seems obvious.

The degree of forewarning of such crises available to management may be dependent on the sophistication of existing organizational awareness and monitoring systems, both formal and informal. Often tacit knowledge embedded within organizations (and across industries) forms a critical aspect of such capacities and constitutes important cultural and human capital. Organizations with the capacity to detect the onset of crises, or react to them faster and thus mitigate impacts, have been termed crisis prepared (Pearson and Mitroff, 1993). Functioning safety systems may also aid in preventing crises and attenuating consequences, however they do not guarantee safe practices in workplaces. In practice safety systems may also be constrained by being designed, or at least focused, on known hazards or specific categories of loss causing events. Given the nature and variability of the emergent threats alluded to above, overly specified safety systems may be ineffective in the face of asymmetric conditions.

This chapter investigates generic aspects of safety cultures and crisis management relevant to ongoing needs of maritime trade security. It promotes a conceptual basis for integrating safety and crisis management capacities across maritime supply chains, ports and associated networks (including operators

[1] See, for example, Turner and Pidgeon, 1997; Pearson and Mitroff, 1993; Mitroff and Alpaslan, 2003.

and commercial participants) consistent with the need to support the implementation of risk management as a core enabler of secure global trade. A starting premise is that the effort required in sustaining safety cultures can equally support development of crisis management capacities in maritime industries. Detail about safety as a cultural phenomenon is followed by an examination of complexity inherent in maritime settings and opportunities merge safety and crisis-related practices. A key issue for discussion is consideration that while safety remains a core aspect critical to commercial and industrial outcomes, evolution of needs towards a combined safety-crisis management goal makes clear sense from an effectiveness and efficiency perspective.

2 THE ENCULTURATION OF SAFETY

Processes of socialization are phenomena common to all human cultures as a means by which [they] recreate and perpetuate themselves through time. Socialization processes as discussed here, focus on how employees are inducted into normally expected occupational and professional practices, that is, "learning the ropes". A "safety" culture may be interpreted to be a stable characteristic of an organization which—through the socialization of new workers—imprints generic approaches to dealing with critical safety issues (Ek and Akselsson, 2005). If, for example, danger is a salient variable within an occupation or industry, workers (over time) could be expected to respond to such a condition by creating a culture that functions as an insulative and adaptive mechanism promoting the value of safety and motivating workers to achieve it (Fitzpatrick, 1980). Such creations have been found among submarine crews, squadrons of fighter pilots, military units and construction crews (Vaught and Smith, 1980; Manning, 1984) and arguably, within workforce participants in the port and maritime segments of supply chains.

The importance of social integration in dangerous workplaces is highlighted also by Haas (1977), who in reference to the high-rise construction industry suggested that a fearful or unknowing worker adds a measure of unpredictability to the work situation and therefore makes it potentially more dangerous. Haas further noted that, in the high-rise construction industry, a worker who is afraid cannot be trusted to act correctly. Fear or lack of knowledge may cause the worker to act rashly because of concern about his own protection and by being unsure about how to respond in dangerous circumstances. Fitzpatrick (1980) identifies eight norms regulating behaviour in dangerous situations involving underground miners. Miners are expected to: (1) do their share; (2) meet reciprocal obligations; (3) act with moderation; (4) act responsibly; (5) protect the interests of others; (6) attempt actions within their level of skill and experience; (7) be accommodating; and (8) respect dangerous situations. The first four identify primary requirements for group membership. The second four are regulatory behaviours within the small two or three man work groups. Each norm is directly related to safety. Similarly, Håvold (2000)[2] suggests that the aim of a safety culture is to reduce human error by seeking the reduction of any likelihood of error, trapping errors before they have an operational effect, and mitigating the consequences of error.

Ek and Akselsson (2005)[3] suggest that a safety culture expresses itself in observable outputs in the form of safety management practices. Thus, a safety culture can shape safety-related behaviours that, among many things, are incorporated in the development of safety management systems. In the maritime settings, the International Safety Management Code (ISM Code) is an instrument that has been developed in order to provide an international standard for the safe operation of ships (IMO, 1997). Characteristics of an existing safety culture may then determine, in part, how well any regulation (such as the ISM Code) is implemented across maritime trading industries, including aboard ships (Ek and Akselsson, 2005).

Håvold (2000) also suggests that many large fatality maritime accidents during the last few years have focused public, institutional and regulatory attention on issues of maritime safety with accident investigation revealing that large numbers of these incidents have human related causes. Håvold further suggests that by looking at [workplace] cultural aspects, an understanding of the underlying mechanisms leading to accidents might increase understanding of cause and effect. Talley, Jin and Kite-Powell (2006) also identify human factors as being more of a significant causal factor for incidents on passenger vessels than either mechanical failure on the ship itself or wider environmental sources. The importance of effective ongoing training on safety practices, and in particular new employee induction, is therefore obvious. Problems with a safety culture can manifest at a wide organizational level also. A number of precursor factors to the Piper Alpha accident were retrospectively identified to be present in the culture, structure and procedures of Occidental Petroleum and other segments of the oil and gas industry (Håvold, 2000).

Accident causes related to human factors and/or issues of organizational culture are obviously not the only factors requiring consideration. Assurance of security goes beyond organizational practice with both operational and systemic complexity being significant factors for both safety and efficiency.

3 MARITIME SYSTEMS: COMPLEXITY AND SECURITY

It has been suggested that, from the perspective of trade in general, the world has become a system of maritime pathways in which individual ports are linked into intricate patterns of dependency and end-to-end shipping linkages reflecting trade dependencies among regions in broad competitive regional environments (Robinson, 1998). Bateman (2003) refers to these key locations

[2] Referencing Helmreich and Merritt (1996).

[3] Derived from Kirwan (1998).

as "hub ports" which, due to their size and capacity, have become essential to the efficient functioning of the global supply chain. Such ports have become pieces of critical infrastructure within trading systems especially in relation economic performance at the national and international level.

A crisis (or series of multiple concurrent incidents) could occur at any time in such large, highly complex systems. Incidents might occur in a number of ways: by emerging suddenly due to the interaction of previously separated system elements or by "cooking" slowly (without recognition) until they appear. The scale of potential port-related incidents is significant. An economic impact analysis of a one-week shutdown of the ports of Los Angeles and Long Beach on the US west coast indicate significant losses in container trade. Costs to the US economy from the port closures for the week were estimated to range from $65 million to $150 million per day (Congressional Budget Office, 2006). If such an event did occur, vessels would usually re-route around such a chokepoint with added costs in terms of time.

The socio-economic importance of large trading ports and their nearby hinterland areas is a major driver for an expansion beyond mere emphases on safety to incorporate wider regulatory, commercial and analytical perspectives. Crisis management theorists have emphasized for some time the need for an extension of conceptual thinking applied to commercial strategies that change from seeing the *world as a simple machine* to one of the *world as a complex system* (Mitroff and Kilmann, 1984).

Critical to this position are the circumstances under which expected organizational functioning "transitions" from normality to crisis: a concern that is beyond the scope of standard safety management. A full appreciation of such transitions can derive from seeing an analogue of moving from *regularity* (familiar—expected functioning) to the edge of chaos (unmanageable complexity). Maritime supply chains fit well into this pattern because of their open nature nationally and globally, and their complexity (Van de Voort *et al.*, 2003). The US Government Accounting Office has suggested that difficulties in coordination among public and private sector entities with an interest in port security and active at a port may make effective security programmes hard to establish (Hecker, 2002). Further, the complex organization and unique vulnerabilities of ports and associated support components are not easily appreciated or understood (Harrald, Stephens and van Dorp, 2004).

Strong opinion exists that the sea itself can barely be policed (even though there is a critical need to enforce relevant law and international treaties) with anarchy as a domain issue (Langewiesche, 2003). Piracy is a well-noted security issue internationally with known geographical areas of concern in the southeast Asian region and other locations (Richardson, 2004a; Anonymous, 2004; Jarvis, 2003; OECD, 2003). The International Maritime Organization (IMO) reported a total of 45 instances of piracy (forced boarding, cargo hi-jacking and violent assault on crews) in the Far East reporting category in the second quarter to June 2003 (Jarvis, 2003). Over the 10-year period 1993 to 2003, a total of 3,254 acts of piracy have been recorded in this geographical category. Even with the increased emphasis on protective interdiction at sea by relevant naval and police forces, and other multilateral efforts this trend may be likely to continue. It has been noted also that the influence of the nation state on control of transnational economic business flows has weakened considerably in recent times (Suárez de Vivero and Rodríguez Mateos, 2004).

Supply-chain specific factors also add variability. The nature of doing business in this modern form itself generates vulnerability due to the mutual interdependencies of stakeholders within the supply networks: both up and downstream. The fragility of these interdependencies creates reduced resilience in the wider systems and can lead to an unexpected or surprising juxtaposition of causal elements, and thus, possible failure. Just-in-time manufacturing, quick response, single sourcing and reduced inventory strategies are standard approaches to logistics and supply-chain management. They work more effectively, however, in times of market stability but less so in times when the volatility of demand increases (Home Office, 2002). Within maritime trading systems (as a significant component of a trading network) a form of "normal" accident[4] (Perrow, 1984) might be expected but not necessarily predictable.

Barnes and Oloruntoba (2005) presented a conceptual framework encompassing the notion of interactive complexity between the ports and maritime supply chains. This interaction generates two distinct classifications of vulnerability: namely Type 1 and Type 2. These are defined as:

- type 1—a factor emerging from the operational complexity within a port (encompassing the transport node infrastructure and onsite operators); and
- type 2—an attribute of the maritime movements themselves (with ports as nodes of the system) and global logistics management practices that underpin the supply chains themselves.

The type 1 vulnerability might be contributed to by "loose" organization and coordination mechanisms (including risk management and/or corporate governance) resulting in a reduced capacity to detect evidence or signs of an impending crisis or to understand the meaning of such evidence. Boin and Lagadec (2000) suggest that such a reduced capacity might also be contributed to by inflexible cultural factors or belief systems within an organization itself promoting notions of invulnerability or indifference to external or internal threats.

As noted above, processes at ports and in related systems can be difficult to coordinate. Cargo and passengers are transferred to and from the maritime mode connecting them with other transportation modes (e.g. rail, road, or

[4]. Perrow provides an analytical view of how accidents in large, extremely complex organizations or institutions are more likely due to inherent complexity and capacities of human operators to not understand what is going on within the system(s) and therefore being unable to manage or respond to unexpected events effectively.

pipeline). Although individual modes (as stand-alone systems) may be tightly connected, the functional links to other systems within a port can be relatively loose. A container facility may be "tightly coupled" with the intermodal rail yard and tightly scheduled container vessels, but only loosely connected with the adjacent petroleum facility or cruise terminal. A crisis, however, may generate circumstances where geographical distance is negated quickly.

Together ports and the maritime routes that connect them constitute a "system of systems" exhibiting strong potential for interactive complexity.[5] On the high seas the system components include the ship (and other ships depending on sea lane traffic), radio and networked communication, the weather, the commodities being transported and orders from ship owners (Perrow, 1984). Even with the benefit of modern navigation technology, as well as satellite communications and geographical positioning systems, the physical reality of the variable weather conditions across open oceans and in littoral areas, remain important considerations. An important factor to be considered is where the system boundaries exist between the maritime and port regimes and how crisis and safety management issues can be dealt with across this divide.

4 SAFETY AND CRISIS MANAGEMENT

A key argument in this chapter is that the effective convergence of the benefits of a positive safety culture and effective crisis management capacities is logical and will lead to resilience in maritime trading systems. The literature on complex systems failure in organizations and institutions has much to offer the understanding of the safety and security issues in maritime systems. This body of knowledge consistently details the presence of "signs" that a crisis was emerging from organizational "noise" before an incident occurred (Perrow, 1984; Turner and Pidgeon 1997; Boin and Lagadec, 2000; Comfort *et al.*, 2001, Rijpma, 1997). Such incidents might be seen as being caused not just from the failure to notice of signs but also from a failure of organizational systems to respond to them. Equally, there are situations where, as a result of extreme systems complexity, warning signs may not have been visible or, if detectable, not understood. This latter category may be the result of totally new systems behaviour or some other source of perturbation. A deeper factor is the nature of the organizational culture that existed before the crisis emerged. While not clearly explicated in this literature organizations with dysfunctional safety cultures also are crisis prone.

An important factor in maritime security is that major actors comprise both the public and private sectors with interaction across regional trading blocks.

[5]. Interactive complexity as used here relates to unfamiliar, unplanned or unique operational sequences that might not be visible or comprehensible to users of the system and could cause or contribute to errors or loss events (see Perrow, 1984).

Recent activities of the Asia Pacific Economic Cooperation (APEC) are useful examples of multilateral efforts to generate resilient maritime trade and supply chains by focusing on operational activities. APEC, a dialogue group of 21 economies possessing shoreline contact with the Pacific Ocean, has developed an active programme of engagement on protecting maritime cargo and the movement of goods and services. Member economies are seeking to implement an agreed framework for the security and facilitation of global trade, which is based on the World Customs Organizations (WCO) Framework of Standards to secure and facilitate global trade and to create an environment for the secure and efficient movement of goods, services and people across the borders (see generally *www.apec.org*).

This includes the adoption of international standards for securing and facilitating the global trade supply chains within the APEC region via implementing where possible common standards for electronic customs reporting developed by the WCO that provide data to target high-risk shipments and facilitate trade. Considerable emphasis is placed on implementing arrangements for "Customs to Customs" communications including: harmonization of in-advance electronic cargo information; the application of a consistent risk management approach to address security threats; and the use of non-intrusive detection equipment for cargo examination. Additional consideration of "Customs to Business" engagement includes the realization of benefits to businesses that meet minimum supply-chain security standards and other high-level practices.

There is a specific goal to enhance cooperation between APEC economies on training to enhance ship and port security in the region and the continued implementation of enhanced critical information infrastructure protection and cyber security. This latter point is enforced by the goal of establishing national computer security incident response teams to help prevent cyber attacks and minimize damage and recovery time from incidents, and to participate in domestic and cross-border information sharing arrangements.

Key factors in much of the APEC-related dialogue, and in particular a 2005 review of counter-terrorism action plans (including capacity building needs) developed by member economies, is joint training and familiarity with systems and practices used by member economies. Other training issues are detailed but a strong focus remained on aligning operational (and social) differences as they apply to work settings with commonly understood and practiced security risk management techniques (Barnes, 2005).

Expanded economic development in southeast Asia is a global trend that is expected to continue. Sustained rapid growth along with rising living standards in China and India have been accompanied by a dramatic increase in Asia's shares of world exports and in particular raw material consumption (UNCTAD, 2005). This continued growth has concomitant impacts on the APEC capacity building activities mentioned above.

An example of the type of capacity-building processes in place includes targeted desktop exercises and exchanges on issues of prevention and preparedness for security incidents.

Exercise *Pacifika,* for example, involving Australia, New Zealand, Papua New Guinea and a number of Oceanic nations, aimed at identifying mechanisms for internal and regional intelligence support and information exchange, including the outlining of roles, capabilities and contact-points for relevant regional organizations. Coverage of information shared included outlining security measures in place to reduce vulnerabilities and existing arrangements that will assist preparation for managing the consequences of a terrorist incident (APEC, 2006).

It is interesting to contrast the intent of the APEC capacity building and the functionality of the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT). Both the CSI and C-TPAT focus on border and trade security; in particular regarding strategies for container security and whole-of-supply chain issues. While involvement in these initiatives is voluntary, there is arguably a degree of commercial inevitability that participation will enhance throughput of imported goods at US ports. Not to expect some degree of unilateral action by the US to enhance security coverage of maritime and land-based containerized trade following the 9/11 crisis would of course be short sighted. This is particularly acute in the absence of a transnationally mandated supply-chain security framework.

It is, however, important to contrast the investment in social capital as well as the cultural and working-level familiarity generated by the APEC practices against assurance generated predominantly by regulation and enforcement at ports and borders. Without consideration of the issues being worked on in the APEC dialogue, adoption of CSI or C-TPAT initiatives may not be widely successful. An issue of note is an appreciation that the CSI and C-TPAT initiatives by themselves do not constitute a global maritime security regime (Frittelli, 2003) even if they are adopted more broadly in international settings.

Other problematical issues are raised by Pysden and Perez-Goldzveig (2003) who note the absence of any legal framework in place ahead of promotion of the CSI especially in relation to data protection issues, liability for delays arising from processing errors, or damage to cargo during inspection.

Alignment to and compatibility with international standards and mandated international codes of practice are required, and a uniform implementation of the International Maritime Organization International Ship and Port Facility Security Code (Piersall, 2006). Of note also is the International Standards Organization (ISO) "Specification for security management systems for the supply chain" (ISO 2800) that will assist in this regard. The clear need to integrate all these factors into any globally adopted and supported trade security framework has been identified by the United Nations also (UN, 2006).

5 EVOLVING NEEDS AND OPPORTUNITIES

Understanding failure in infrastructure systems requires appreciation of the complexity and inter-connectedness of components, whether concentrated or geographically dispersed. These factors, in concert with required command, control, coordination and communication elements embedded within infrastructure systems, often make effective governance and sustained availability of reliable essential services problematical.

Commentators in the early 1990s, however, suggested that many institutional crises may replicate in a number of common ways, albeit never in exactly the same manner (Anderson, 1991). The suggestion that there are repeatable and recognizable stages in major socio-technical failure is supported by findings grounded in the analysis of industrial and organizational settings over a number of years. Key findings summarized by Stead and Smallman (1999) identify five recognizable stages in organizational failure:

- pre-conditions (where indicators of dysfunction were ignored or buried in background noise);
- trigger (an escalation factor internal or external to an organization or setting);
- crisis (an emergent process of confusion, uncertainty and loss);
- recovery (recovery of the organization and normalization of functions); and
- learning (identification and changes to functional capacities of organizations).

A capacity to apply such an understanding entails the presence of a number of capabilities, namely:

- timely recognition of counter-intuitive loss-causing incidents;
- access to vulnerability analysis capacities within and between complex and critical systems; and
- continuity planning methodologies for effectively recovering the functioning of complex infrastructure systems.

Additional capabilities should also support effective crisis coordination and decision-making that are separate to routine business decision-making structures (Barnes, 2001). The absence of a crisis management capability within organizations has been noted as a critical factor in literature covering industrial disasters and business and organizational failure.[6] The benefits of such embedded skill sets has been recognized within specific industries internationally but how they might be established at the level needed for consistency across the maritime trading industry is yet to be determined. What is evident

[6] See, for example, Turner and Pidgeon, 1997; Pearson and Mitroff, 1993; Mitroff and Alpaslan, 2003.

is the strong potential for merging the expected outcomes of effective safety enculturation with specific crisis management capacities.

6 FUTURE STEPS

A number of options exist that will assist progress towards greater understanding of how to create secure and resilient maritime trading systems: all entail collaboration among stakeholders new and old. Two overarching elements are needed within this enhanced participation: (1) the application of ideas and concepts across-paradigms, and (2) break-through thinking about how social and cultural realities can be helpful to the application of modern security and risk-related practices.

Håvold (2000), for example, encourages sustained collaboration between industry and academic institutions as a clear and present need with emphasis on organizational culture and organizational climate in maritime safety: an area where little research has been done. Work suggested in this area includes:

1. transfer of findings from industry and air safety to maritime safety;
2. determining the most important cultural factors affecting maritime safety; and
3. investigating the effects of culture on risk aversion and risk taking, and how cultures can influence safety in times of increasing production pressures.

Of equal importance to the notion of paradigm breaking is the incorporation of historical learning from organizational failures detailed earlier. They too emphasize the cultural factors inherent in systems accidents.

Beyond this parallel trading system exchange two broad investigative terrains need to be explored, both of which are likely to produce a positive return on the investment that is required. The first is enhanced and ongoing collaboration among trading partners on delivering secure trade. Using the APEC example, increased exchanges on capacity-building needs are both logical and effective. Similar activities among members of other trading blocs are likely to be beneficial also. While this style of involvement is notable in the European Union (Paixão Casaca, 2006) for example, expanded efforts should be attempted elsewhere.

The second is research at an international level of the degree of realignment (if any) that may be needed between relevant global institutions to make secure maritime trade more easily achievable. This outcome would rely on sustained coordination in the development of international standards on security and risk management and detailed guidance under mandated treaty obligations (including those directly impacting on maritime trade and those with peripheral involvement). This latter factor involves engagement of a number of United Nations affiliated bodies that have standing across the maritime trading regimes.

7 CONCLUSION

This work has investigated relations between generic aspects of safety cultures and crisis management within organizations and institutions as they are relevant to the ongoing needs of maritime trade security. From examining key factors in crisis causation—as they emerge from the human activities within organizations—it has attempted to align the social and cultural factors of workplace cultures with crisis management capacities as they are applied to complex networks. It has also suggested that a degree of paradigm busting (at best sharing) needs to be pursued in order to make accessible the potential benefits from combining knowledge bases and conceptual schema.

A core issue within the chapter has been that enhanced safety outcomes and crisis management capacities are by logic "two sides of the same coin" and should be developed together. It has also examined, through the example of APEC secure trade initiatives, how such collaborations encourage and enhance safety and crisis management capacities within and across trading blocs.

REFERENCES

Anderson, A. (1991). "Making a Success out of a Museum of Failure", *New Scientist*, 130, 54.

Anonymous (2004) *The Rising East: Pirates and Terrorism*, Editorial (www document) *http://www.koreaherald.co.kr/SITE/data/htnl dir/2004/03/05/20403050015.*

APEC (2006) *Report on Exercise Pacifika*, Counter Terrorism Task Force Meeting, Ho Chi Minh City, Viet Nam, 2006/SOM2/CTTF/024. Accessed from: *www.apec.org.*

Barnes, P. (2001) "Crisis Management Needs in the Public Sector", in: *Proceedings of the, Institute of Public Administration Australia Queensland Division Conference*, 24 August.

Barnes, P.H. and Oloruntoba, R. (2005) "Assurance of Security in Maritime Supply Chains: Conceptual Issues of Vulnerability and Crisis Management", in a special edition of *The Journal of International Management,* 11, 4.

Barnes, P.H. (2005) *Report of interim results of a Cross-analysis of Counter-Terrorism Action Plans—Asia Pacific Economic Cooperation Economies (Gaps, Capability Enhancements and Needs)*, Asia-Pacific Economic Cooperation (APEC) Counter Terrorist Task Force meeting, Seoul, Korea (11–12 September).

Bateman, S. (2003) "Maritime Security: A New Environment Following September 11", in the *Symposium of Maritime Experts to Assist in Implementation of the STAR Initiative*, Melbourne, 18–20 June.

Boin, A. and Lagadec, P. (2000) "Preparing for the Future: Critical Challenges in Crisis Management", *Journal of Contingencies and Crisis Management*, 8(4): 185–191.

Comfort, L. *et al.* (2001) "Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments", *Journal of Contingencies and Crisis Management*, 9(3): 144–157.

Congressional Budget Office (2006) *The Economic Costs of Disruptions in Container Shipments*, 29 March.

Ek, A. and Akselsson, R. (2005) "Safety culture on board six Swedish passenger ships", in *Maritime Policy & Management*, 32(2), 159–176.

Fitzpatrick, J.S. (1980) 'Adapting to Danger (A participant observation study of an underground mine)', in *Sociology of Work and Occupations*, 7(2), 131–158.

Flemming, D. K., (1999) "A geographical perspective of the transhipment function", in: Proceedings of the *IAME Conference*, Halifax, Canada, 14 September.

Haas, J. (1977) "Binging: educational control among high steel workers", in: *American Behavioural Scientist*, 16 (Sept.), 27–34.

Harrald, J.R., Stephens, H.W. and van Dorp, J.R. (2004) "A Framework for Sustainable Port Security", in: the *Journal of Homeland Security and Emergency Management*, 1(2):1–13.

Håvold, J.I. (2000) "Culture in maritime safety", in: *Maritime Policy & Management*, 27(1), 79–88.

Hecker, J.Z. (2002) *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, US General Accounting Office, 1 August.

Helmreich, R.L. and Merritt, A.C. (1996) "Cultural issues in crew resource management training", in: a paper presented at the *ICAO Global Human Factors Seminar*, Auckland, New Zealand.

International Maritime Organization (1997) *International Safety Management Code (ISM Code), Guidelines on the Implementation of the ISM Code* (London: IMO).

Janis, I. (1982) *Groupthink*, Little Brown, Boston.

Jarvis, D.S.L. (2003) *The Arc of Instability: Regional Security Challenges for Australia and the Asia Pacific*, Centre for International Risk, University of Sydney.

Kirwan, B. (1998) "Safety management assessment and task—a missing link", in: *Safety Management (The Challenge of Change)*, Hale, A. and Baram, M. (eds), Oxford: Elsevier Science, pp. 67–91.

Lagadec, P. (2004) "Crisis: A Watershed from Local, Specific Turbulences, to Global, Inconceivable Crises in Unstable and Torn Environments, Future

Crises, in the International Workshop", in: *Future Agendas: An Assessment of International Crisis Research.*

Langewiesche, W. (2003) "Anarchy at sea", *The Atlantic Monthly* (Sept.), 292(2) 50–70.

Manning, F.J. (1984) "Critical Commentary", in *The Boys in the Barracks: Observations on American Military Life*, The Institute for the Study of Human Issues, Philadelphia.

Marais, K., Dulac, N. and Leveson, N. (2004) "Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems". Presented at *the Engineering Systems Division Symposium*, MIT, Cambridge, MA, 29–31 March.

Mitroff, I.I. and Alpaslan, M.C. (2003) "Preparing for Evil", *Harvard Business Review*, April: 109–115.

Mitroff, I.I. and Kilmann, R.H. (1984) *Corporate Tragedies: Product Tampering, Sabotage, and other Catastrophes*, Praeger, New York.

OECD, 2003. *Emerging Systemic Risks: An Agenda for Action*, OECD, Paris.

OECD, 2006. *Denmark (Assessing Societal Risks and Vulnerabilities)*, OECD Studies in Risk Management, Paris.

Paixão Casaca, A.C. (2006) "Insights into the Port Training of the New European Union Member States", *Maritime Policy Management*, 33(3), 203–217.

Panayides, P.M. (2006) "Maritime policy, management and research: role and potential", *Maritime Policy & Management*, 33(2), 95–105.

Pearson, C.M. and Mitroff, I.I. (1993) "From Crisis Prone to Crisis Prepared: Framework for Crisis Management", *Academy of Management Executive*, 7(1), 48–106.

Perrow, C. (1984) *Normal Accidents: Living with High Risk Technologies*, Basic Books, New York.

Piersall, C. (2006) *Developments at the International Standards Organisation, Total Supply Chain Security Symposium*, Singapore, 6–7 July 2006, APEC Doc. 06/CTTF/TSCS/017

Pysden, K. and Perez-Goldzveig, S. (2003) "Problems ahead for security initiative", *Freight Transport Review*, 2003, 150, 152.

Richardson, M. (2004a) "A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction", *Viewpoint*—Institute of Southeast Asian Studies (www document) *www.iseas.edu.sg/viewpoint.*

Rijpma, J.A. (1997) "Complexity, Tight-coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory", *Journal of Contingencies and Crisis Management*, (5)1, 15–23.

Robinson, R. (1998) "Asian hub/feeder nets: the dynamics of restructuring", *Maritime Policy & Management*, 25(1), 21–40.

Shaw, G.L. and J.R. Harrald, J.R (2004) "Identification of the Core Competencies Required of Executive Level Business Crisis and Continuity Managers", In: the *Journal of Homeland Security and Emergency Management*, 1: 1.

Stead, E. and Smallman, C. (1999) "Understanding Business failure: Learning and Un-learning Lessons from Industrial Crises", *Journal of Contingencies and Crisis Management*, 7(1), 1–18.

Suárez de Vivero, J. and Rodríguez Mateos, J.C. (2004) "New Factors in Ocean Governance: From Economic to Security-based Boundaries", *Marine Policy*, 28, 185–188.

Talley, W.K., Jin, D. and Kite-Powell, H. (2006) "Determinants of the severity of passenger vessel accidents", *Maritime Policy & Management*, 33(2), 173–186.

The Home Office (2002) *Supply Chain Vulnerability*, Research Report prepared by the Cranfield University School of Management.

Turner, B.A. and Pidgeon, N. (1997) *Man-made Disasters* (2nd edn), Butterworth Heineman, Oxford.

UNCTAD (2005) *Trade and Development Report*, UNCTAD/TDR/2005.

United Nations (2006) *Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment*, UNCTAD/SDTE/TLB/2005/4.

Van de Voort, M., *et al.* (2003) *Seacurity (Improving The Security of the Global Sea-Container Shipping System)*, RAND Europe, MR-1695-JRC.

Vaught, C. and Smith, D.L. (1980) "Incorporation and Mechanical Solidarity in an Underground Coal Mine", *Sociology of Work and Occupations*, 7(2), 159–187.

Wiegmann, D.A., Zang, H., Von Thaden, T.L., Sharma, G. and Mitchell Gibbons, A., (2004) "Safety culture: an integrative review", *International Journal of Aviation, Psychology*, 14(2), 117–134.

Willis, H.H. and Ortiz, D.S. (2004) *Evaluating the Security of the Global Containerized Supply Chain*, RAND Corporation.

This page intentionally left blank

CHAPTER 13

MARITIME CONTAINER SECURITY: A CARGO INTEREST PERSPECTIVE

Mary R. Brooks

Faculty of Management, Dalhousie University, Halifax, Canada

Kenneth J. Button

Centre for Transportation Policy, Operations and Logistics, School of Public Policy, George Mason University, Fairfax, VA, USA

Abstract

The 9/11 attacks brought to the forefront long-standing concerns that terrorists could severely disrupt the global supply chain using shipping containers or vessels as a weapons platform. In response, new maritime security requirements were initiated. It has been difficult to quantify the economic impacts of these measures because of the reluctance of those involved in the global supply chain to share data for proprietary and security reasons and because of difficulties in quantifying costs. This chapter, by making use of interviews with senior US executives in manufacturing and retail operations, looks at how cargo interests involved in US waterborne container trade have responded to the new environment. A number of issues are addressed. What were the strategic responses of key manufacturing and retail concerns to the container security requirements? What did they conclude about the costs of imposed security requirements and did they see any benefits? What do they expect to happen in future and what would they like to see in future? What will this mean for companies in developing countries that do not have the benefits of scale and scope that large US corporations have?

1 INTRODUCTION

Achieving a secure container supply chain poses significant policy challenges given the international nature of much of the business. For example, the US does not have jurisdiction over foreign firms, containers or vessels until they reach US waters. It also does not have the resources to guarantee the security of every container arriving at a US port. The response of the US government, like all others, to global terrorism must, therefore, be measured and coordinated. There is, however, a trade-off between security and efficiency. Programmes involving full inspection of containers are, given current technology, highly resource-intensive and the US General Accounting Office (2004) has taken Customs and Border Protection (CBP) to task for its failure to perform a comprehensive assessment of the risk faced by maritime containers. Excessive emphasis on security can offset the economic benefits gained from trade liberalization, containerization, container tracking technology and management information systems.

It is this challenge of ensuring appropriate levels of security at an acceptable cost that lie at the foundation of this chapter. It is concerned with the reactions of actors in the international supply chain to the institutional changes that are taking place and affect their ability to act freely. In this sense, it is a micro-analysis that does not address some of the crucial broader issues of the optimal amount of national resources that should be committed to security, or the meso-questions of how these resources should be allocated across various sectors or types of threat.[1]

2 THE ISSUES

Maritime containers are the primary mode of transport for international trade in manufactured products and parts. Some 303 million containers were handled in world ports in 2003; 20 ports alone accounted for 166.62 million containers handled in 2004 (United Nations Conference on Trade and Development, 2005). Of these ports, three were in the US—Los Angeles, Long Beach and New York New Jersey. Port congestion has, however, become an issue, with delays on the US West Coast creating problems for US cargo interests. As rigorous security programmes suggest there will be even more delays as port congestion grows, the views of cargo owners with respect to security programmes and costs become relevant for risk management programme planning.

Not only is global trade involving containers focusing on specific routings, the business is continuing to consolidate in the hands of a few lines. The Top 10 container carriers offered 45.7% of the slots available in 2003 (the Top 20 offered 64.4%), and concentration of the market has continued with more mergers and acquisitions; in 2004 the Top 20 offered 70.5% of the slots available (*Containerization International Yearbook*, 2006). Although it looks as though the number of actors is small, this is far from the case. A European study concluded that 21 different actors are involved in a container chain in addition to the buyer and seller (European Conference of Ministers of Transport, 2004). Container integrity is key to the success of containerization in the post-World War II era; prior to its advent, theft from ports, terminals and ships was a significant commercial risk, as was damage to cargoes. Today, shipping lines face the additional uncertainty that terrorists will use the vessel or the container as a weapon of mass destruction, while ports face, at minimum, congestion in anticipation, during or after an incident, and at worst, devastation.

[1] Some of these larger issues are addressed in Spich and Grosse (2005). European Commission (2001) provides an initial assessment of the macroeconomic impacts for Europe of post-9/11 security measures.

In response to the terrorist acts of 9/11, multilateral regulators and the US implemented new maritime security requirements. In December 2002, the International Maritime Organization (2002) developed the International Ship and Port Facility Security Code (ISPS Code) and added it as an amendment to the Safety of Life at Sea, 1974 (a widely-adopted UN Convention) to address concerns about vessel safety. The Code sets forth mandatory security requirements to be taken by governments, ports, shipping companies and terminal operators to enhance the security of the world's maritime transportation system. The US implemented the ISPS Code by passing the Maritime Transportation Security Act of 2002 with effect 1 July 2004.[2] The International Labor Organization passed the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185) so that standards are set for a biometric feature—a fingerprint—on this globally recognized document and national security agencies can ensure these mobile workers are who they say they are.

On the cargo side, the World Customs Organization (WCO) (2002) adopted the Resolution of the Customs Co-operation Council on Security and Facilitation of the International Trade Supply Chain. Since the adoption of this resolution, the WCO Task Force was established and developed a package of measures, including: an amended WCO data model and a list of essential data elements for identification of high risk consignments; customs guidelines for Advance Cargo Information to enable the pre-arrival electronic transmission of customs data (Integrated Supply Chain Management Guidelines); WCO Guidelines for Co-operative Arrangements between Members and private industry to increase supply-chain security and facilitate the flow of international trade; and a new International Convention on Mutual Administrative Assistance in Customs Matters to assist Members in developing a legal basis to support these initiatives. The objective of the WCO's efforts, from a cargo perspective, was to develop a framework of standards that would encourage the facilitation of trade so as to be seamless, and that could be applied consistently across customs jurisdictions; this framework was published in June 2005 (World Customs Organization, 2005). It is too early to assess if the intentions are likely to be achieved.

To supplement these multilateral efforts, the US implemented advance notification rules, and launched a series of programmes, including Operation Safe Commerce, the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) and Free and Secure Trade (FAST) (US General Accounting Office, 2003a). Operation Safe Commerce acts as a test bed for piloting new procedures and technologies throughout the supply chain. The CSI focuses on the container; through bilateral agreements with other countries, it places US customs officials in foreign ports as part of pre-

[2] The Act, however, has two requirements that exceed the minimum requirements of the ISPS Code. First, it requires the establishment of transport worker identification cards for domestic port personnel (still not completed and the subject of on-going internal debate). Secondly, it requires that the US government not only assess the security plans of foreign ports, but also the effectiveness of a foreign nation's security oversight.

screening processes, and allows container inspection to US standards to occur in foreign ports, thereby moving the border offshore. There were, as of 29 March 2006, 26 countries and 44 ports participating in the CSI (US Customs and Border Protection, 2006); CSI participating ports accounted for 62.48% of all US destined containers as of 31 May 2005 (United Nations, 2006). FAST complements C-TPAT by streamlining border movements by truck between the US and Canada and Mexico for C-TPAT members. The primary programme of interest to cargo owners is C-TPAT, but it is by no means the only programme influencing the flow and processing of internationally traded goods.

The purpose of the C-TPAT programme is to make security a cooperative activity throughout the cargo supply chain. Guidelines, developed by US Customs and Border Protection in consultation with cargo interests, are implemented by registered companies and built into their contracts with their trading partners. By 25 January 2005, 8,355 businesses had registered in C-TPAT and 4,515 were certified. Only US companies, however, may belong. The sole exception is Mexican manufacturers in *maquiladoras*; other foreign companies have been certified by virtue of getting their US operations certified.[3] There are several benefits associated with C-TPAT participation. Participating firms are subject to faster and fewer inspections at US ports and land border crossings and are five to eight times less likely to have imports examined for enforcement reasons (SITPRO, 2004). In the event of a container-based terrorist incident participants in C-TPAT will be allowed to resume operations faster than non-participants. The programme, however, has come under scrutiny for its inability to process applications in a timely manner, audit existing members adequately, and generally deliver the benefits promised (US Government Accountability Office, 2005; Ojah, 2005). Furthermore, the automated targeting system CBP uses to identify the highest risk containers for inspection (which likely uses C-TPAT membership as one of the “green light” mechanisms in the container screening process) continues to attract criticism from the Government Accountability Office (2006a).

These programmes have evolved as new organizational learning has developed. All also have their flaws. For example, participation in C-TPAT is voluntary and was originally not costed (Organization for Economic Cooperation and Development, 2003). With respect to the ISPS, all compliance is enforced by the responsible national government agency, and violations are dealt with at a national level. There is no black list published by IMO and, therefore, the ISPS security system is only as good as the national flag government is serious or as shipping lines and the ports are compliant.

Security is not just about programmes and business processes. Traditionally, container seals provided evidence of cargo integrity but are not regarded by cargo owners as a barrier for sophisticated thieves or for stowaways.

[3] Other countries have implemented similar programmes; Canada’s Partners in Protection Program mirrors C-TPAT but many Canadian companies have acquired C-TPAT certification through US parent operations.

Therefore, cargo interests have sought to define appropriate standards to achieve the purposes they desire; if a manufacturer supplies Wal-Mart or another such large retailer, it is likely to be the large multinational with the economic power that will define the security standard to be met by industry. Manufacturers of high value goods experimented with GPS tracking and internal condition monitoring equipment long before 2001 and radio-frequency identification (RFID) is increasingly being adopted as part of inventory control management. While electronic seals were proposed by the Department of Homeland Security (DHS) in January 2002 as the "frontline" technological solution to security, there has been no subsequent agreement on electronic seal standards and DHS has recently concluded that the integrity of the seal still does not guarantee that the contents of the container are what they are stated to be; therefore, CBP has decided to focus its resources on cargo data and scanning technologies (Edmonson, 2006). The problem with RFID technology is that it can be used for illicit tracking. The supply chain is only as secure or as strong as the weakest link.

Booz Allen Hamilton (2003) argue that security can seldom be viewed as point problem but rather one that involves protecting a flow, in this case the flow of international trade. While Figure 1 illustrates the classic supply chain, with circles representing nodes and the heavy, solid lines representing links, the supply chain in which maritime containers move is not, partly for institutional reasons, so simple. Links, for example, are usually controlled by one corporate entity—ship, rail line, road—and vulnerability is perceived to be greater at the nodes, the ports. This is because containers are most vulnerable at rest, and least vulnerable in motion, particularly on the high seas where they may be inaccessible. Land border delays increase vulnerability for trucks that must sit and wait. As a result, ships are generally perceived to be more secure than railways; they, in turn, are seen as more secure than trucks. Thus, the heavy downward arrows in Figure 1 identify those weakest links.

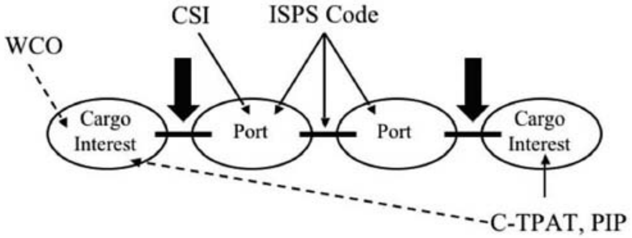


Figure 1: Security Programmes in Place

The actors in the supply chain can also be very different, not only between the various elements in the chain but also within each element. The large players—the multinational enterprises—have diverse objectives, resource bases and structures, and their detailed involvement in the supply chain may vary considerably. In consequence their approach to security requirements are likely to differ (Li *et al.*, 2005) At the other extreme, suppliers of first mile or last mile links—those involving collection and distribution—are often small players that enter and leave markets and thus have unknown track records (e.g. an unknown driver in a developing economy).

Finally, if a container is determined to be at risk and it is deep in the hold of a ship, how is it to be accessed without putting a port at risk? It is not surprising, therefore, that the US has moved the problem of identifying containers at risk offshore through the CSI and advance notification requirements built into the Maritime Transportation Security Act, 2002.

In broad terms, there are three types of reactions to terrorism that cargo interests need to consider: the prevention and deterrence of an incident; the short-term response to an incident; and the longer-term remediation and recovery from an incident when one does occur. Targeting and prevention are only part of securing the supply chain. To date, it appears that most of the focus of government has been on the first of these, although inevitably the need for security prevents a full assessment. To quote Willis and Ortiz (2004):

> "Both public and private sector initiatives to improve the security of the global supply chain have focused largely on preventing and deterring smuggling and terrorist attacks. . . . Few initiatives have focused on improving the fault tolerance or resilience of the system, which could be a fruitful area for new security measures."

Added to this there are some significant differences between safety, as normally understood and for which many previous policies were established, and security. Safety has traditionally been treated as the need to protect individuals or consignments from accidental malfunctioning of the system; this may be due to poor design or some so-called act of God. Security involves protection against deliberate acts to injure or damage for whatever reason. This inevitably implies a degree of game playing in the setting and modifying of regulations and standards to meet the ever-changing challenges posed by those wishing to disrupt the system. Since, by definition, the actions of these individuals and groups depend on their motivations, ingenuity and resources at any particular time they are rare events and not easily brought within actuarial calculations.

The industry response to safety issues was to develop risk management techniques and processes, built on incidents with measurable probability for the private insurance market to assess in setting premiums. The new post-9/11 security environment must still address these, as they have not disappeared, but companies and governments must now prepare for and remediate terrorism, in a climate of uncertainty and one with insufficient incidents for measuring probability. A regulatory policy of "implement and amend", as currently exists in the US, adds to, rather than reduces, the uncertainty that cargo owners face. Add to this the US approach of mandating action without allocated funding and more uncertainty is created. Security is not only a private good; the part that is a public good mandates public sector participation in some form. As Gorman (2005) notes, private markets lead to public vulnerabilities. Security generally needs to focus on both what the government will do and what private companies will do; private markets alone can lead to under-investment if there are not full property right allocations.[4]

This greater complexity also leads to greater difficulty in analysing the success of any policies to enhance security. Since by its nature, a successful strategy will prevent a security breach it is almost impossible to define the appropriate counterfactual. This makes quantitative assessments difficult. Quasi-efficiency analysis may look at the costs of meeting various security requirements, either within a company or at a more macro-governmental level, but these requirements themselves may be poor proxies for actual security. In the absence of adequate quantitative methods, more qualitative approaches are unavoidable and are used here. In particular, the knowledge of some of those closely associated with the creation and implementation of security measures is drawn upon.

The attitudes and the approaches of the private sector are important in influencing how official policies are formulated—affecting the *de jure* element—and in the ways they will work in practice—affecting the *de facto* element. We limit ourselves to three specific questions within this context.

- What were the strategic responses of key manufacturing and retail concerns to the imposed container security requirements?
- What did manufacturing and retail concerns conclude about the costs of imposed security requirements and did they see any benefits?
- What do manufacturing and retail concerns expect to happen in future and what would they like to see happen?

Based on the answers to these three, we attempt to answer a fourth:

- What will this mean for companies in less developed countries that do not have the benefits of scale and scope that large US corporations have?

3 FINDINGS

To look at these questions, companies in the Top 100 that imported goods to the US or Top 100 that exported goods from the US in 2004 were targeted and those recommended by an industry association as actively participating in

[4]. There are also the public good elements of some aspects of security—those elements with a degree of non-rivalness and non-excludability—that, even with full property right allocation, would lead to under-provision.

cargo security standards development were approached. Interviews were conducted by telephone, mail, e-mail or site visits using a common survey instrument. The data collection took place between February and May 2005. Senior US executives in both manufacturing and retail operations were approached (36 companies) and 10 in-depth interviews with companies took place. This was supplemented by interviews with three cargo industry associations. All persons interviewed stated that they expressed the official viewpoints of their company or their industry trade association. Most of the respondents, however, provided additional security insights on condition of confidentiality.

3.1 Strategic Responses to Container Security Requirements

Of particular interest here[5] is the issue of strategic changes in transport decisions as a result of the events of September 2001 and the consequent new security requirements. The personnel of the companies contacted were very vocal on the issues of how they altered their transportation and distribution arrangements after September 2001. Many had already reduced the number of transportation suppliers or contracted with carriers offering larger geographic scope in the 1990s, in an effort to gain greater control or minimize supply-chain costs. One manufacturer had reduced its transborder trucking suppliers to one. Particularly interesting was the comment by one company that the need to raise international security standards had also resulted in the implementation of the same programme for domestic security, but that this was all in progress before 2001. After September 2001, supplier reduction programmes continued for many of the respondents. Cargo interest concerns, however, also turned to security compliance and transport network capacity constraints.

For manufacturers and retailers, the key focus before 2001 was the integrity of the supply chain to deal with issues of both intrusive theft and theft of the container as a whole. For many of the manufacturers and retailers, cargo theft had already driven logistics processes in a direction that the new security requirements after 9/11 extended. Therefore, it is not surprising to find that, when companies were asked whether they had switched to outsourcing distribution/logistics or changed terms of sale, nine out of the 10 answered neither and only one responded that a change in terms of sale occurred (Table 1). Some of those who had not changed terms of sale indicated that they had preferred to control the transport decisions prior to 2001 for risk, cost control, or other reasons, and so no change was necessary. The one large retailer that changed its terms of sale did so “to ensure that origin trucking is controlled by our company or a trusted 3PL, as an increased security measure”. Only one

[5]. The findings are part of a larger research programme. The findings of the interviews with shipping lines and ports are reported in Thibault *et al.* (2006).

of the companies responding to the question about security responses indicated that it had dropped a market because of security concerns.

Strategic response	*n*	*Frequency*
Require C-TPAT of transport suppliers	10	7
Added requirements to transport contracts	10	6
Outsourced transported and distribution	10	0
New terms of trade	10	1
Neither outsourced nor new terms of sale	10	9
Dropped market(s)	9	1

Table 1: Strategic Responses to Changed Security Environment

On the issue of making changes to their transport contracts, opinions were divided. Some felt that all suppliers must be C-TPAT compliant and that all request for quotations and purchase orders must include supply chain security clauses. Others felt that this formality was not necessary, that expectations could be conveyed to suppliers, and that encouragement and coaching were appropriate roles for their companies.

Seven respondents indicated that they require their transport companies to be C-TPAT participants. One of the other three indicated that they encouraged it, a second felt they had insufficient clout to demand it, and the third believed it was more important to measure performance but that companies have a role in educating their transportation suppliers on security matters.

Companies also reported concerns about capacity constraints, raising questions about whether security has reduced the rated capacity of existing infrastructure. Such capacity constraints have some seeking to introduce supplier variety and routing options. One consumer goods manufacturer noted that it has instituted a port diversification plan to reduce the concentration of cargo through one particular port.

3.2 The Costs and Benefits of Security Requirements

It is difficult to quantify the economic impacts of regulations within global supply chains as companies have been either reluctant to share their data for proprietary and security reasons or have not been able to quantify costs. Only five companies were willing to discuss the cost of enhanced security, four claiming it to be less than 1% and one claiming it to be 1%. The others noted that it was hard to quantify but as requirements become standardized, it will be a cost for all companies, thus producing a level competitive playing field.

The cost of security, however, was not a key pressure point for many of the companies.

This finding provides a contrast to those of Thibault *et al.* (2006). In that study, shipping lines stated that it was costly to meet initial compliance with the new container security requirements, as they had to make significant expenditures to hire new personnel and purchase equipment. However, several executives stated the 24-hour rule was beneficial because it required that a container's documentation be in order prior to shipment, thereby reducing the amount of time that their companies had to spend resolving documentation issues with their customers.

On the other hand, Thibault *et al.* (2006) found that the opinions of small container ports and lines diverged from those of their larger counterparts. These actors indicated that their small scale of operations made it easier for them to make the investments they needed to comply with the new security requirements. Some indicated, however, that it was expensive to maintain certain types of continuing security activities such as vehicle checks, and they questioned why they should be held to the same physical security standards as ports whose scale of operations were several orders of magnitude larger. They found it harder to spread fixed costs across a smaller business base.

While not all cargo interests saw the benefits of streamlined logistics processes, there were mixed reviews on whether the costs were outweighed by the benefits. Security was noted as slowing the supply chain down, although one company noted that this was being partially mitigated by the implementation of new technologies.

When asked what would make transport security more cost effective, there were numerous suggestions ranging from tax incentives for the adoption of new security technologies or for participation in pilot programmes. The cargo owners generally focused on three issues: (1) the development of a common data set and requirements; (2) the desirability of a CBP-rated country-risk index so that companies would know where to place priorities; and (3) continued collaboration between industry and government. To elaborate further on the first, it was recognized by the cargo interests that implementation of the automated commercial environment will help to achieve this goal, and that this programme can be of benefit to both carriers and cargo owners. One manufacturer said: "The economic benefit is to the carriers in the form of asset control, and to the shippers in the form of data accuracy." There is for cargo owners the positive benefit of better planning for inventory in transit.

Companies also called for US Customs and Border Protection to work with their counterparts in Mexico and Canada to employ Free and Secure Trade (FAST) type programmes for all modes between the three countries. Not all crossings have FAST lanes, diminishing the benefit of ramping up to the higher-level programme. It was noted that security costs are likely to continue to go up (e.g. because of smart containers and RFID tags) but that these costs may be balanced by recovery of theft of items and better control practices.

3.3 Expectations and Hopes for the Future

The cargo industry has been very supportive of US security initiatives, both within the US and in international forums like the WCO. The World Shipping Council, the International Mass Retail Association and the National Industrial Transportation League, and their member companies have supported the Maritime Transportation Security Act, 2002 and its 24-hour rule, the CSI, and the C-TPAT programme as well as the "development and implementation of analogous efforts at the international level through the World Customs Organization. . . . The industry strongly supports the governments of trading nations establishing predictable and transparent, and mutually consistent, security rules governing these issues" (World Shipping Council *et al.*, 2003). It was noted by one of the associations interviewed that a two-way system of communication between industry and government does not appear to exist.[6]

It appears that temporary changes to national policy, like cabotage regulations, have not been considered as part of incident response and this would allay some of the cargo owners' concerns about current government policy in the US. The belief that "restoration is almost as important as prevention" was reported. This belief is only now being echoed by DHS (Blenkey, 2006).

Finally, there was discussion about the level of communication between government and industry. Associations representing cargo interests felt that they have intelligence capability on the ground and can contribute; they have access to the companies with the most to lose from poorly implemented security programmes. They also believe that government where possible needs to share more of its concerns with industry.[7]

3.4 Discussion

What does this mean for companies in less developed countries? Large companies were already working on seamlessness and supply-chain process improvements before 9/11. Their focus on security before then was to prevent theft, but after the attacks, they expanded the responsibilities of the senior supply-chain executive or chief information officer to include new security responsibilities. Security took on a higher profile within the senior management team. While all companies interviewed are supportive of security programmes, if business process benefits are clear, some want to "do what's right" or "execute to a higher standard" and do more. In other words, for some, their

[6] The Thibault *et al.* (2006) analysis of shippers came up with a somewhat different conclusion, namely that there was a feeling that mechanisms and working relationships between the US government and the maritime industry that did not exist prior to 9/11 were now in place, and that has improved security.

[7] The Government Accountability Office (2006b) notes that it concluded in April 2005 that the major barrier hindering information sharing was the lack of federal security clearances for non-federal members of committees or centres; by June 2006, about 40% of those individuals had received security clearances.

interest is still driven by a concern about theft (as well as continuing piracy and human smuggling) while others see prevention of terrorism and incident contingency planning as a part of the company's corporate social responsibility mandate.

Most of the company personnel interviewed were concerned about the uncertainty around regulation (e.g. with respect to e-seals, security and investments). Advanced manifest notification seems to be acceptable for the big companies; as we only interviewed large or relatively large companies, the impacts for small- and medium-sized enterprises, and particularly those in developing countries, cannot be easily commented upon.

Regulations often serve as a "fear factor" for small companies with limited resources and the Internet-based paperwork can mean problems for those in rural or remote communities (Darby, 2004). Add to this the uncertainty of continuously revised regulations under an implement and amend approach, and it is not hard to reach the conclusion that security can drive away the faint-hearted supplier. Micro-businesses and artisans, the path to economic development in many developing countries, will see security as a barrier to growth. Collaborative partnerships can go some way to supporting these types of companies.

The operational driver for retail activities is, for traditional reasons, supply-chain control and security. The power of large retailers is substantial; they are setting the standards and influencing the agenda. Small and medium enterprises would do well to align with large retailers and seek collaborative improvement of their business processes and joint investment in logistics equipment as many of those interviewed indicated that the foreign partners of large US manufacturers and retailers will be assisted. SITPRO (2005) has concluded that the cost of implementing compliance with the ever-increasing volume of regulations is escalating. While developed countries have the ability to provide companies with some financial assistance, as is currently the case with Canada's Export Development Canada Security Compliance Loan programme (Brown, 2006), the cost of implementing security programmes and maintaining their validity may simply be impossible to achieve in poorer countries. This raises the question about whether such support should be expanded under the umbrella of World Bank funding.[8] Those who opt out of available security programmes will be flagged. Those who cannot participate in such programmes will also be flagged (C-TPAT is a domestic programme for US firms and their subsidiaries). This implies that shipments from the poorest of nations are most likely to be flagged for increased scrutiny by security agencies. The cost for foreign small and medium enterprises may be

[8] The World Bank already gives limited funding to help some countries meet international security commitments—e.g. in 2006 two International Development Association credits and two grants for a combined total of $33.57 million Burkina Faso, Cameroon, Guinea and Mali for this purpose.

too high resulting in a reduction in their contribution towards realizing economic development potential.

4 CONCLUSIONS

As with most areas of security, the private market has an inherent tendency to under-supply. This is in part because of potential free-rider problems—protection for a port or intermodal facility protects all users—but also the lack of complete property rights, and *de facto* contracts, for the open sea means that large parts of the "infrastructure" are essentially commons. Added to this, many terrorist acts, because of their infrequency, are more a matter of uncertainty than actuarial risk and this precludes the development of an effective private sector insurance market. Cargo interests, therefore, cannot be expected to carry the full cost of maritime container security. They do have an interest in ensuring that what is provided as a public good continues to also facilitate trade, albeit it a more secure manner. Hence, it is not surprising that the focus of those interviewed is forward looking, with a greater concern for ensuring that if standards for electronic seals are introduced that they are too prescriptive, that lines of communication between security officials and industry remain open and are effective, and that "one size fits all" solutions are not imposed.

A few shipping and rail companies have considerable power and influence through their security programmes. While concerns about chemical, biological, radiological or nuclear weapons in a box ("Trojan Horse" scenarios) drive current security measures from a government perspective, most companies agree that by the time the box arrives in the port, it is too late if the container is the weapon (or the ship the weapon). While they are generally supportive of measures that push back the border nearer to the source, the companies interviewed are much more concerned about incident management and remediation.

There is general acceptance of the necessity to have a layered and targeted risk management approach as companies believe that to inspect every maritime container would be too costly. The question is how much security is enough. The two weakest links for the US-bound maritime containers are: the US domestic trucking link as the Oklahoma bombing revealed the "enemy within"; and foreign domestic trucking still provides the Trojan Horse opportunity. Terrorists have imagination; the next incident is highly unlikely to reflect similar patterns to the last. Small companies, and those in developing countries, would do well to align with large cargo interests who seek to ensure security throughout the chain and are prepared to invest, educate and assist their partners.

Acknowledgement

This chapter is based on work conducted while Mary Brooks was a Canada-US Fulbright Scholar at the School of Public Policy, George Mason University. The Critical Infrastructure Protection Project at George Mason University supported the work of Kenneth Button. The research assistance of Diana Dennis, Denise Napoliello, Henry Vega and Marc Thibault is much appreciated.

REFERENCES

Booz Allen Hamilton (2003) *Port Security War Game: Implications for US Supply Chains*, New York: Booz, Allen, Hamilton.

Blenkey, N. (2006) "Port Security: New Emphasis on Recovery", *Marine Log*, 31 August.

Brooks, M.R. and Button, K.J. (2006) "Market Structures and Shipping Security", *Maritime Economics and Logistics*, 8, 100–120.

Brown, B. (2006) "C-TPAT: Security Compliance Loan Program", *Exportwise* (Ottawa: Export Development Canada), Spring, 6–7.

Containerization International (2006) *Containerisation International Yearbook 2006*, London: Containerization International.

Darby, J. (2004) "Myths and Realities: The Shipper View", Presentation to the Atlantic Provinces Transportation Forum, Halifax, Canada, 29 October.

Edmonson, R.G. (2006) "On the Back Burner". *The Journal of Commerce*, 14 August, 19.

European Commission (2001) *Overview of EU Action in response to the Events of 11 September and Assessment of their Likely Economic Impact*, Commission of the European Communities, Brussels.

European Council of Ministers of Transport (2004). *Security in Transport: Report on Container Transport Security Across Modes* (CEMT/CM(2004)22), European Council of Ministers of Transport, Paris.

Gorman, S.P. (2005) *Networks, Security, and Complexity: The Role of Public Policy in Critical Infrastructure Protection*. Northampton: Edward Elgar.

International Maritime Organization (2002) *The Safety of Life at Sea, 1974, As Amended Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention For the Safety of Life At Sea, 1974, As Amended*, IMO, London.

Li, S., Tallman, S.B. and Ferreira, M.P. (2005) "Developing the Eclectic Paradigm as a Model of Global Strategy: An Application to the Impact of the Sep. 11 Terrorist Attacks on MNE Performance Levels". *Journal of International Management*, 11, 479–496.

Ojah, M. (2005) "Securing and Facilitating US Land Border Trade: A Critical Analysis of the C-TPAT and FAST Programs", *Transportation Research Record*, 1938, 30–37.

SITPRO (2004) *Summary Notes from the Meeting of the 7th SITPRO Security Forum*, 4 November, *http://www.sitpro.org.uk/policy/security/secfor7.html*, last accessed 10 August 2006.

SITPRO (2005) *Summary Notes from the Meeting of the 8th SITPRO Security Forum*, 20 April, *http://www.sitpro.org.uk/policy/security/secfor8.html*, last accessed 10 August 2006.

Spich, R. and Grosse, R. (2005) "How Does Homeland Security Affect US Firms' Competitiveness". *Journal of International Management*, 11, 457–448.

Thibault, M., Brooks, M.R. and Button, K.J. (2006) "The Response of the US Maritime Industry to the New Container Security Initiatives", *Transportation Journal*, 45, 5–15.

United Nations (2006) *Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment.* United Nations, New York.

United Nations Conference on Trade and Development (2005) *Review of Maritime Transport, 2005.* United Nations Conference on Trade and Development, Geneva.

US Customs and Border Protection (2006). *Ports in CSI*, 29 March. *http://www.customs.gov/xp/cgov/border_security/international_activities/csi/* last accessed 10 August 2006.

US General Accounting Office (2003a) *Container Security: Expansion of Key Customs will Require Greater Attention to Critical Success Factors*, GAO-03-770, GAO, Washington DC.

US General Accounting Office (2003b) *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*, GAO-04-325T, GAO, Washington, DC.

US General Accounting Office (2004) *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T, GAO, Washington, DC.

US Government Accountability Office (2005) *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security* (D-05-404). GAO, Washington, DC.

US Government Accountability Office (2006a) *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System* (GAO-06-591T). GAO, Washington DC.

US Government Accountability Office (2006b) *Maritime Security: Information-Sharing Efforts Are Improving* (GAO-06-933T). GAO, Washington DC.

Willis, H.H. and Ortiz, D.S. (2004) *Evaluating the Security of the Global Supply Chain*, RAND Corporation, Arlington.

World Customs Organization (2002) *Resolution of the Customs Co-Operation Council on Security and Facilitation of the International Trade Supply Chain*, June. *http://www.wcoomd.org/ie/En/en.html*, last accessed 10 August 2006.

World Customs Organization (2005) *Framework of Standards to Facilitate and Secure Global Trade*, June. *http://www.wcoomd.org/ie/En/en.html*, last accessed 10 August 2006.

World Shipping Council, the International Mass Retail Association, and the National Industrial Transportation League (2003) *In-transit Container Security Enhancement* (Working Paper), 9 September, *http://www.retail-leaders.org*, last accessed 12 May 2005.

CHAPTER 14

MANAGING SECURITY THROUGH QUALITY MANAGEMENT: A CASE STUDY TO IMPLEMENT THE 24-HOUR RULE IN A LINER SHIPPING COMPANY

Khalid Bichou

Port Operations, Research and Technology Centre (PORTeC), Centre for Transport Studies, Imperial College London, UK

Kee-hung Lai, Y.H. Venus Lun and T.C. Edwin Cheng

Department of Logistics, The Hong Kong Polytechnic University,
1 Yuk Choi Road, Hung Hom, Kowloon, Hong Kong

Abstract
This chapter introduces a quality management framework for implementing and managing the 24-hour Advance Manifest Rule based on a case study for a liner shipping company. The chapter starts by investigating the relationship between quality management and maritime security in the context of international shipping and port management before outlining the need for a case research application of quality management principles into the emerging field of maritime security. Throughout the case study, we demonstrate how the proposed framework has been successfully applied to ensure regulatory compliance and quality assurance for the 24-hour rule. The case research objective is to achieve a balance between the regulatory framework and the quality management framework so that the requirements of both regulators and customers are equally met.

1 INTRODUCTION

Following the events of 9/11, fundamental shifts have taken place in the way policy and regulatory instruments are being drafted and implemented. In the field of maritime security, this has led to a raft of compulsory and voluntary security programmes, but more importantly to a different approach to security risk assessment, management and mitigation. Traditionally, the shipping and port community has for long considered security almost solely during times of wars and political conflicts when the latter meant huge claims and insurance premiums. Even with increased warnings of the danger and consequences of the new security threats such as piracy, drug smuggling, human trafficking, etc. neither the perception of the security risk nor the response to it had nurtured a proper security culture until new security regulations came into force.

Early and effective compliance with the new security regulations is usually presented as a successful tool for competitive advantage, such as in terms of exclusive certification and fast-lane treatment. Even though few empirical evidences of a positive correlation between best-compliance practice and commercial rewards exist. Empirical investigations in the field of maritime security are extremely sparse and their undertaking for the purposes of exploratory research and theory building are even more sparse. Much of the available literature on the subject has sought to examine the new security regulations and their macro-economic, trade, social and policy implications (OECD, 2003; Kumar and Vellenga, 2004). The remainder is either largely descriptive (King, 2005) or predominantly conceptual (Harrald *et al.*, 2004), with only a few studies explicitly investigating maritime security issues at the spatial (Prokop, 2004), sectoral (Tzannatos, 2003) or regulatory programme (Babione *et al.*, 2003) level. Two separate but distinctive areas of literature are, however, worth mentioning in this regard. The first is an established body of literature in which much of the attention has been focused on the interface between quality management and supply-chain management (Beamon and Ware, 1998; Lai *et al.*, 2005) since the two management approaches share a common theoretical background and are similar in their strategic orientations. The second is a new stream of literature linking maritime security to supply-chain vulnerability, with a strong emphasis being placed on sea-container shipping systems (Van De Voort, 2003; Russel and Saldana, 2003) and on the appraisal of new security regulations in view of supply-chain management (Harrington, 2002; Bichou, 2004).

In a similar vein, the interface relationships between security regulations and quality management systems also appear to be overlooked in both academia and the profession, in particular for the 24-hour rule. On the one hand, little empirical or applied research has sought to link the benefits of quality management to regulatory compliance with maritime security (Lee and Whang, 2005; Bichou, 2006), and we are not aware at the time of writing of any research being applied to the 24-hour rule. On the other hand, much of the industry's attention has been paid to the deadlines and prescriptive mechanisms for compliance, with no quality or industry standard being developed prior to the entry into force of new security regulations. As with maritime safety and environmental management, quality practices in maritime security did not emerge from a firm-centric or product-based mindset but only came to light through regulation.

This chapter presents a case study and a framework in a step-by-step manner for the implementation of the 24-hour advance vessel manifest rule (hereafter abbreviated to the 24-hour rule) within the framework of quality management. Our contribution is to demonstrate that the current security framework can be perceived, managed and implemented in line with the quality management approach. The conceptualization of the current maritime security framework in terms of a quality assurance system translates various security regulations into a series of interrelated quality standards, the achievement of which would benefit intra- and inter-organizational relationships between various members of the maritime and port community. A second contribution of this paper is the use of case study research to investigate areas so far uncovered by the literature. We believe that conducting empirical research through using case study methodology is particularly relevant to the content and objective of this inquiry, and in general to inquiries based on exploration and aimed at gaining an in-depth knowledge of how in practice quality management principles can be applied in shipping companies to ensure compliance with maritime security regulations. The remainder of the chapter is structured as follows. Section 2 briefly reviews the origin and the requirements of the 24-hour rule. Section 3 examines the historical relationships between quality assurance and regulatory management in shipping and ports, followed by the development of a conceptual framework that identifies a need for taking the quality management approach to managing security through legislation. Section 4 presents the case study and the developed framework for the implementation of the 24-hour rule. Section 5 concludes with summaries and suggestions for future research.

2 THE 24-HOUR RULE: FRAMEWORK AND BACKGROUND INFORMATION

Following the terrorist attacks in the US in September 2001, several frameworks aimed at enhancing maritime and port security have been introduced, with a special emphasis on protecting the vulnerability of containerized seatrade operations. Among these measures, the International Ship and Port Facility Security (ISPS) Code and, more recently, World Customs Organization's "Framework of Standards to Secure and Facilitate Global Trade" are the most widely cited due to their global nature. However, other non-global measures may be equally, if not even more, significant given the scope and scale of their costs and impacts. Among these, those worth mentioning include the US-led initiatives mainly the Container Security Initiative (CSI), the Customs-Trade Partnership against Terrorism (C-TPAT), the 24-hour advance vessel manifest rule (the 24-hour rule), and Operation Safe Commerce (OSC). Statutory instruments implemented outside the USA include Canada's own 24-hour rule version, the EC Regulation No. 725/2004, the Asia-Pacific Secure Trade (STAR) programme, and a number of other national and regional initiatives. Finally, industry-driven schemes implemented outside government control include the Smart and Secure Tradelanes (SST) programme and a series of recent ISO initiatives. For a detailed review of both compulsory and voluntary maritime security programmes, the reader is referred to recent CBP and OECD publications on the subject (see for instance CBP, 2006; OECD, 2004).

With respect to ship-cargo security, the 24-hour rule is probably the major non-ISPS regulatory instrument specifically targeting ocean carriers and their agents. Under this rule, detailed information on container-cargo on board vessels calling at, or transiting via, US ports must be submitted electronically to the US Customs authorities at least 24 hours prior to departing from a foreign port, except for empty containers whereby notification prior to arrival at a US port can be extended up to 48 hours. In total, 14 data elements must be specified on the electronic manifest with detailed information about the ship and its cargo, as well as its previous and next ports of call.

Since its introduction, the 24-hour rule has provoked mixed reactions from the various parties concerned. For the opponents, the measure acts against logistical optimization and operational flexibility since shippers and receivers alike have to adjust their production and inventory management processes to be in line with the new requirement. Ocean carriers and freight forwarders (including NVOCCs) will also have to decline any late shipment bookings and bear the cost of at least one extra day of container idle time at ports. The latter may be extended to three days or more for carriers and forwarders that are not electronically hooked into the US Customs' Automated Manifest System (AMS). Ports will equally bear commercial and cost impacts of the 24-hour rule, including potential congestion problems. An additional cost may stem from the extra time spent on compiling and recording detailed information, given that vague descriptions such as "freight all kinds" (FAK), "said-to-contain" (STC) and "foodstuffs" are no longer acceptable. Finally, in the event of a cargo delay or a ship detention, the resultant operational redundancies and unreliable demand/supply scenarios would inevitably lead to increased logistics costs and generalized disruption across the supply chain.

1.	Foreign port of departure
2.	Standard carrier alpha code (SCAC)
3.	Voyage number
4.	Date of scheduled arrival in the first US port
5.	Number and quantity of packages (based on bill of lading descriptions)
6.	First port of receipt by the carrier
7.	Detailed cargo description: either shipper's description or the six-digit harmonized tariff schedule number; plus the cargo's weight
8.	Shipper(s) name(s) and address(es). Alternatively ID numbers as assigned by US customs

9.	Consignee(s) names(s) and address(es). Alternatively ID numbers as assigned by US customs
10.	Vessel flag, name and number
11.	Names of foreign ports visited beyond the port named in point 6
12.	International hazardous goods code if applicable to cargo
13.	Container number
14.	Numbers on all seals affixed to the container

Table 1: The 14 Data Information Points Required for Electronic Reporting under the US 24-hour Rule (*Source*: US Customs and Border Protection—CBP)

On the other hand, proponents of the 24-hour rule consider the introduction of the measure as not only necessary in view of the new security threats but also commercially "rewarding" for both liner shipping companies (LSCs) and their supply-chain members. The main argument put forward is that the 24-hour rule fundamentally shifts the focus from inspection to prevention, the benefit of which offsets and ultimately surpasses the initial cost of implementation. Electronic submission of detailed information would allow for prescreening and deliberate targeting of "suspected" containers, which is proven to be more cost-effective and less time-consuming than the traditional approach of random physical inspections. Similarly, ocean carriers and their suppliers/customers would equally benefit from the introduction of the rule, provided that they redesign their logistics and supply-chain processes accordingly. The benefits of reduced lead times and inventory levels have been quantitatively assessed by Lee and Whang (2005) in the context of SST. Other studies have shown that additional security measures would ultimately reduce the distribution and logistics costs (Bowersox and Closs, 2002). The benefits of reduced inspection and cumbersome customs procedures to trade facilitation is also evidenced through applied research (Raven, 2001); although the question of whether the 24-hour rule and other security measures act as a barrier or an incentive to trade and time efficiency has remained unsolved (Hummels, 2001).

3 TOWARDS A QUALITY MANAGEMENT FRAMEWORK FOR THE 24-HOUR RULE

Quality means different things to different people, but is primarily linked to the achievement of specified requirements or standards. In their review of the literature on the subject, Evans *et al.* (2000) and Mehra *et al.* (2001) identified as many approaches to quality management as the number of businesses applying them, but most of the approaches associate the quality movement with at least five core values, namely customer focus, planning and leadership, continuous improvement, empowerment and teamwork, and performance benchmarking.

Quality management has been widely recognized as a potent means for achieving a competitive edge from differentiation across a broad spectrum of business sectors (Lai *et al.*, 2003). Improving service quality as an effective strategy for gaining sustainable competitive advantages has been evidenced both analytically (Morgan and Piercy, 1996) and empirically (Hendricks and Singhal, 1997) in the literature. Quality management is a holistic management approach that can be employed by LSCs to create customer value at lower cost. Recognizing the potential benefits that improved quality is likely to bring, many LSCs have started to implement quality management systems. The objective is to improve process performance continuously by placing shippers' interests at the forefront of customers' satisfaction, while still operating cost effectively.

In the maritime industry, companies have embraced the quality movement mainly through importing external schemes rather than developing firm-specific quality management models. Nevertheless, the industry is left with a wide range of quality standards against which maritime firms and organizations can be assessed and benchmarked. These may range from mandatory regulations (e.g. ISM code, STCW 95, ISPS code, 24-hour rule), to voluntary programmes (e.g. the ISO 90000, ISO 28000 PAS). Table 2 portrays some of these programmes by purpose and relationship.

	ISM code	*ISO 9002 series*	*ISPS codes*	*24-hour rule*
Aim	Safety of ships and pollution prevention	Quality assurance of products and services	Security of maritime network, and prevention of terrorism threats	Security of containerships and their cargo through advanced information sharing
Target	Marine mgt. and shipboard operation	Contractual relationship between customer/ supplier (ocean carriers and ship management companies, freight forwarders, trade houses, cargo insurers, ports, etc.)	Ship, port and mobile offshore facilities, ship/port operations and management	Ocean carriers or their agents. Licensed or registered NVOCCs
Completion	Capacity to meet safety and pollution prevention	Demonstrate ability of marine management and shipboard operation to meet customer requirements	Ability of participants to meet security requirements, and react to changing security levels	Ability to electronically report and manage all the required data elements in advance
Means	Implementation of the safe operation of ships and pollution prevention	Implementation of a quality assurance system	Implementation of part A of the code and chapter X1-2 of SOLAS. Regional implementation of part B	Electronic reporting, via AMS to a central interface (CBP) of advance manifest
Scheme of certification	Company assessment: doc. of compliance. Ship assessment: safety management certificate	Company and ships assessment: quality system certificate	ISSC, SSA and SSP for ships and companies. Local accreditation of PFSA and PFSP for ports	CBP identification/ clearance of transmitted information for each voyage
Maintenance of certification	Follow up assessment each year, re-assessment after three years	Surveillance on company every six months, all ships during three years. Re-assessment after three years	Up to five years for ISSC and intermediate verifications. Period of validity for the statement of compliance of PFSP to be decided by contracting government	N/A

Table 2: Purposes and Relations between the 24-hour Rule and other Maritime Regulatory and Voluntary Programmes (*Source*: adapted from Bichou, 2004)

In implementing the 24-hour rule and other security programmes, quality management can help shipping lines achieve dual cost and service objectives across many functional areas, including ship operations (ship planning, cargo inspection, etc.), marketing (slot booking, issuance of shipping confirmation, etc.) and administration (documentation, data handling and transmission, etc.). Furthermore, an application of the quality management approach helps prevent lines from making defects in conforming to the 24-hour rule and other maritime security requirements. A sample of potential errors that might occur in the work processes while satisfying maritime security is provided in Table 3.

Functional department	*Potential errors*
Marketing	Flagging the CSI cargo in business information system Booking data quality Booking confirmation to shipper CSI cut-off time
Administration (documentation and ICT)	Manifest data quality Transmission of manifest data to AMS timely Handling amendment Bill of lading issuance to shipper Rating the shipment Billing the CSI fee and amendment fee
Operations	Release of empty container Coordination with container terminals and local customers for cargo inspection Ship planning

Table 3: Potential Errors from Implementing the 24-hour Rule

To reach a common maritime security goal, a concerted effort to ensure both regulatory compliance and quality assurance is essential so that the requirements of all the concerned parties are fully met (Lun *et al*., 2006). On the other hand, quality comes at a cost and thus quality improvement might prove meaningless without proper understanding of cost and competitive implications of quality assurance. A balanced approach between the efficiency benefits from a deregulated competitive environment and the cost implications from a regulated quality environment is therefore essential. Hence, there is a a need for a mechanism that incorporates all such objectives while supporting the shipping lines' efforts for security compliance and quality improvement. In the next sections, we examine the maritime security practices in a shipping line to implement the 24-hour rule security programme. Based on the case, we introduce a generic framework for shipping lines to implement the 24-hour rule in response to the above challenges.

4 A CASE STUDY RESEARCH FOR IMPLEMENTING THE 24-HOUR RULE

As a guide for the maritime industry to embark on any maritime security implementation initiative, we propose a general quality management framework, which was validated for implementing and managing the 24-hour rule in a LSC. At the time where no appropriate quality management framework of security implementation and management exists, a structured approach on how to incorporate the 24-hour security requirements into LSCs' operational and strategic management is strongly required.

4.1 Introduction of the Case Shipping Line

Our case is a liner shipping company (LSC) the core business of which lies in the carriage of containerized goods by sea. The LSC under study has a strong worldwide network and operates on major shipping routes with an existing fleet of around 300 ships on more than 80 shipping routes. It has 75 new vessels on order for delivery by 2009. The company has become a global carrier and operates on all the world's oceans. The company's mission is to become one of the worldwide leading container shipping groups offering its customers top quality, door-to-door solutions and increasingly comprehensive global coverage. The company also prepared for the future by constantly expanding its portfolio of services. The need to meet both regulatory requirements and shippers' expectations has prompted the case LSC to become one of the ocean carriers that have conformed to the 24-hour rule. One of the key benefits of using a quality approach to implement the 24-hour rule is the accreditation for best-practice compliance and best-class benchmark, leading to stronger competitive advantage and strategic market repositioning in the industry. Operationally, it allows the organization concerned to develop business processes that best support the implementation of the programme or the regulation. Figure 1 provides an outline of the case LSC working processes in support of the 24-hour rule.

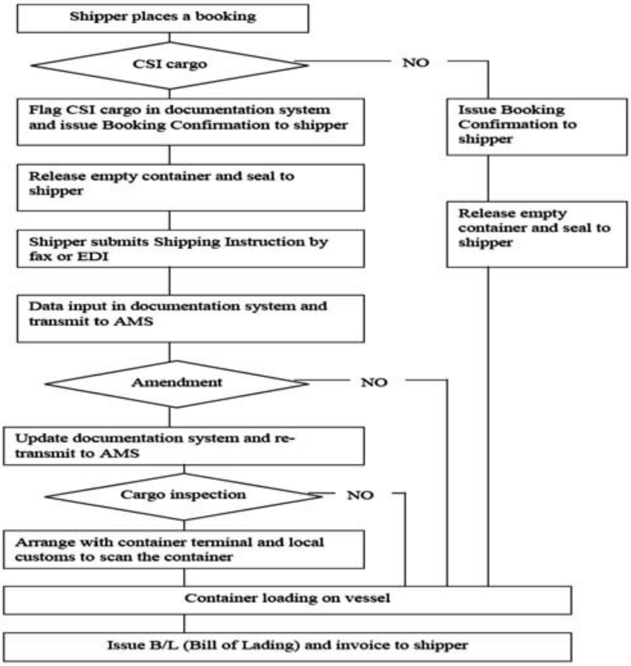

Shipper places a booking
CSI cargo
NO
Flag CSI cargo in documentation system and issue Booking Confirmation to shipper
Issue Booking Confirmation to shipper
Release empty container and seal to shipper
Release empty container and seal to shipper
Shipper submits Shipping Instruction by fax or EDI
Data input in documentation system and transmit to AMS
Amendment
NO
Update documentation system and re-transmit to AMS
Cargo inspection
NO
Arrange with container terminal and local customs to scan the container
Container loading on vessel
Issue B/L (Bill of Lading) and invoice to shipper

Figure 1: A Case Decision Support System to Implement the 24-hour Rule in the Case LSC

Across much of the quality management theory and practice, there exist three interrelated elements that are typically identified as the building blocks for any quality programme (Westphal *et al.*, 1997):

- the generating of objective data for the systematic improvement of work processes as a prerequisite for taking action;
- the focus on key problem areas and customer satisfaction; and
- the involvement and empowerment of employees.

For the 24-hour rule to be perceived and operated as a quality programme, these three elements must be embedded in the different aspects of quality assurance and management. The next sections describe in detail how the quality management framework portrayed below in Figure 2 was applied in our case study to accommodate the various stages of the 24-hour rule implementation and management.

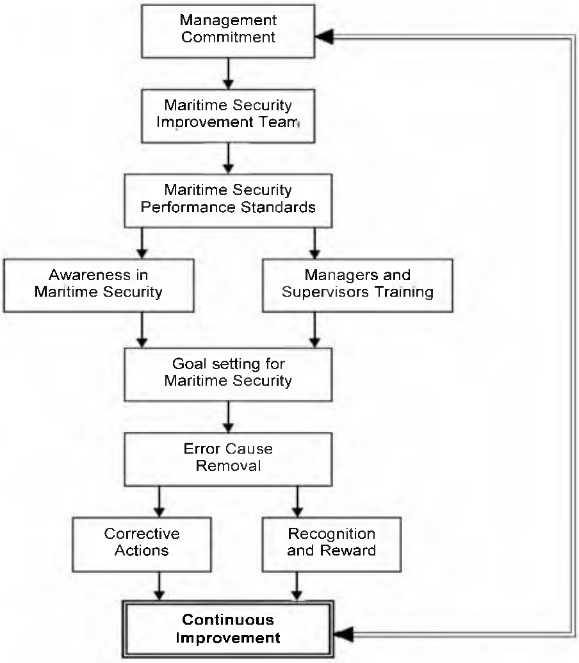

Management Commitment
Maritime Security Improvement Team
Maritime Security Performance Standards
Awareness in Maritime Security
Managers and Supervisors Training
Goal setting for Maritime Security
Error Cause Removal
Corrective Actions
Recognition and Reward
Continuous Improvement

Figure 2: A Generic Quality Management Framework for Implementing a Regulatory Maritime Security Programme

4.2 Procedural Mechanisms for Implementation

Step One—management commitment

The first step in implementing the 24-hour rule was to obtain the support of top management in order to make the shipping service sustainable. A clear and strong message that compliance with the 24-hour rule is compulsory must be articulated and diffused at all levels of the LSC. A mission of implementing maritime security through the 24-hour rule was defined as "to provide quality shipping services with maximum efficiency through the continuous improvement of every aspect of the work processes". The purpose of this step was to diffuse the message that the top management is strongly involved in the security assurance process, and the message was recited regularly throughout the firm.

Step Two—maritime security improvement team

The second step of the process included setting up a quality improvement team (QIT) whose mission was to define a set of measurable maritime security performance objectives and formulate the corresponding strategies to guide the LSC towards achieving these objectives. The team was composed of managers who could steer their departmental activities towards actions for improvement. The QIT was responsible for designing the maritime security implementation exercise, developing operations standards and assessment methods, and estimating and gathering the resources required for a successful implementation. To this end, the LSC checked with its shippers and business partners on a regular basis in order to understand their security requirements and identify the pertinent maritime security performance objectives. The information obtained from shippers covered various aspects of the workflows in the LSC's shipping services including the booking process, release of booking confirmation, release of empty containers and seals, receipt of shipping instructions from shippers, handling of documentation amendments, issuance of bills of lading and invoices, and the overall perception of its staff. The findings provided directions for the LSC to set performance objectives and strive for continuous performance improvement.

Step Three—maritime security performance standards

In view of shippers' feedback in step two, the QIT needed to develop a maritime security improvement model that accommodates appropriate measures to gauge outcomes and performance in line with the overall maritime safety and security policy of the LSC under study. The purpose of setting standards was to identify problems and obstacles so that evaluative and corrective action could be taken. This has been done through undertaking a review in each functional department so as to spot when and where corrections were necessary, and record actual improvements for assessment in subsequent stages.

LSC's maritime safety and security policy	*Developed standard elements and objectives for the implementation of the 24-hour rule*
Priority in safety, health and environment.	100% accuracy in data input in both the booking module and the documentation module.
	Booking confirmation is sent to customers within two working hours of a shipper placing a booking.
Reliable inventory records, i.e. empty containers.	Shipping instruction submission cut-off schedules are clearly communicated to shippers.
	All CSI cargoes are flagged in the business information system.
Zero-defect in data input.	All 14 essential data elements are input before data transmission to the AMS (Automated Manifest System).
	No delay in any cargo declaration to the AMS.

LSC's maritime safety and security policy	*Developed standard elements and objectives for the implementation of the 24-hour rule*
Zero-defect in arranging for cargo inspections.	Bills of lading are ready within one working day of containers being loaded on vessels.
	99% accuracy in freight rating.
Services that satisfy both customers' requirements and related regulatory and legal requirements.	99% accuracy in the billing of maritime security fee and amendment fee.
	Zero defect in coordination with container terminals and local customs authority for cargo inspections.
	All containers loaded on vessels are declared to customs where applicable.
Continuous improvements in its services.	A 10% decrease in the number of incidents regarding incorrect inventory records.
	Zero customers' loss due to sub-standard service quality.

Table 4: Developing Implementation Standards in Line with a LSC's Safety and Security Policy

After the review, the QIT established written standards and procedures to govern the various aspects of the work processes at the level of each department. The standards and procedures provided clear guidelines and instructions to staff members on the requirements of each work process and on their roles and responsibilities in meeting these requirements.

Step Four—awareness of maritime security

The basis of this step is to create awareness and communicate top management's vision about maritime security to all the employees of the LSC. Managers and supervisors were equipped with the basic concepts of maritime security for diffusion to their subordinates. This awareness involved a clear explanation of the objectives of implementing security regulations and introduced all staff members of the LSC to the backgrounds and concepts of maritime security in view of a collaborative contribution and greater commitment towards the implementation exercise.

Step Five—managers' and supervisors' training

Managers' and supervisors' training continues directly from step five and aims at providing management staff with the necessary support to carry out their functions. It is essential that all the managers and supervisors in the LSC have an in-depth understanding of the concepts and objectives of the security and quality assurance process so that they can communicate and explain them to their subordinates in a clear and effective manner. To this end, a series of training seminars and module courses on maritime security were conducted for all management staff in the LSC.

Step Six—goal setting for maritime security

The purpose of this step was to turn commitment into action by encouraging individual departments to set by and for themselves appropriate improvement plans and goals towards achieving "zero defects" with minimum disruptions. The objective is to help employees to think in terms of meeting goals and operate in a teamwork spirit to accomplish the task of security assurance. All the concerned departments incorporated shipper satisfaction and compliance with the 24-hour rule as key criteria in their work procedures, and established department-specific goals capable of being assessed and measured. Examples of such goals include reducing the lead time for sending booking confirmation, speeding up the bills of lading's processing time, improving accuracy in the billing of the CSI and amendment fees, and reducing the number of incidents stemming from incorrect inventory records.

Step Seven—error cause removal

The purpose of this step is to establish channels whereby staff members effectively communicate to management the difficulties and impediments they encounter throughout the implementation process. As a simple yet effective procedure, all employees were invited to record and report in a standard form any problems that hindered their efforts to carry out error-free work. Examples of the feedback from the employees included the followings:

- customers submit too many amendments;
- information on shipping instructions is not clear;
- customers always ask for exemption from the amendment fees; and
- the stock of empty containers is inadequate.

Step Eight—corrective actions

Error-free shipping service under the implementation of the 24-hour rule requires periodic preventive maintenance of the work processes. Simply setting goals and identifying root causes would not automatically lead to continuous improvement of the services. There is a need to frequently assess the required level of performance from the work processes and to improve them when necessary to remain competitive. This step was to provide a systematic method for resolving once and for all the problems that were identified in the previous steps. To this end, task forces were formed in order to solve the reported problems at the level of each department. In addition, the QIT organized successive meetings across departments to proactively identify maritime security problems so far uncovered and come up with applicable solutions.

Step Nine—recognition and reward

Employee empowerment and staff satisfaction based on motivation are crucial to achieving the LSC's goal of security assurance. To this end, regular programmes were established to reward employees who performed outstanding acts and recognize their achievements and continuous commitment to providing quality and secure shipping services. These programmes are in fact still running and have been generalized across different regulatory aspects of maritime security. Compound with mutually supportive relations and teamwork, such programmes have fostered a company's culture towards quality assurance, and have served as a constructive background to satisfy and manage other security schemes and shippers' requirements.

Step Ten—continuous improvement

The last action was to repeat the nine-step cycle described above in view of critical reflection and continuous improvement. The emphasis on continuous improvement is essential because a typical maritime security implementation process spans 12 to 18 months during which employee turnover and market changes might adversely affect the LSC's efforts to comply and improve. To sustain the momentum for continuous improvement, the QIT met periodically to review the design of the work processes and make adjustments to satisfy evolving regulatory requirements. The renewal effort also helped propel the maritime security movement and provided a background for incorporating and managing other security schemes within an established QM programme.

5 CONCLUSION

With the adoption of quality management tools to implement and manage maritime security, shipping companies can expect to meet regulatory requirements while achieving dual cost and service objectives. As an illustration of the influences and benefits of quality management on security assurance in shipping, a case study on the planning, implementation and management of the 24-hour rule in a liner shipping company was presented and discussed throughout this chapter.

With an ever rising regulatory and customer pressure on shipping firms to properly conform to the new security agenda, the quality management framework and procedural mechanisms presented in this case study could serve as a roadmap for other shipping companies to formulate quality standards in line with the new security requirements. Equally, further research can build on this to investigate the link between quality and security in other maritime contexts including port and terminal operations.

Acknowledgement

The authors would like to thank Mr Lee Kwong Kit from CMA-CGM Hong Kong for valuable information and his help and assistance throughout this study.

REFERENCES

Babione, R., Kim, C.K., Rhone, E. and Sanjaya, E., 2003, *Post 9/11 Security Cost Impact on Port of Seattle Import/Export Container Traffic*, GTTL 502 spring session: University of Washington.

Beamon, B.M. and Ware, T.M., 1998, "A process quality model for the analysis, improvement and control of supply chain systems", *International Journal of Physical Distribution and Logistics Management*, 28, 704–715.

Bichou, K., 2004, "The ISPS code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management", *Maritime Economics and Logistics*, 6(4), 322–348.

Bichou, K., 2005, "Maritime security: framework, methods and applications", *Report to UNCTAD*, UNCTAD: Geneva.

Bichou, K., 2006, "Modelling the impacts of security on port operational efficiency and benchmarking", *Proceedings of the International Workshop on Port Operations, Logistics and Supply Chain Security*, 29 September 2006, Imperial College London: UK.

Bowersox, D.J. and Closs, D.J., 2002, "Supply chain sustainability and cost in the new war economy", *Traffic World*: 1 April 2002.

Evans, J.R. and Dean, J.W., 2000, *Total Quality: Management, Organisation and Strategy* (2nd edn), South-Western College Publishing: Cincinnati/Ohio.

Harrald, J.R., Stephens, H.W. and Van-Drop J.R., 2004, "A framework for sustainable port security", *Journal of Homeland Security and Emergency Management*, 1(2), 1–13.

Harrington, L., 2002, "Sourcing globally now that the rules have changed", *Inbound Logistics*, October 2002, 62–69.

Hendricks, K.B. and Singhal, V.R., 1997, "Does implementing an effective TQM program actually improve operating performance: Empirical evidence from firms that have won quality awards?", *Management Science*, 43(9), 1258–1274.

Hummels, J., 2001, *Time as a Trade Barrier*, Mimeo: Purdue University, 1–40.

King, J., 2005, "The security of merchant shipping", *Marine Policy*, 29, 35–245.

Kumar, S.H. and Vellenga, D., 2004, "Port security costs in the US: a public policy dilemma", *Proceedings of the 2004 Conference of International Association of Maritime Economists*, Turkey: Izmir.

Lai, K.H. and Cheng, T.C.E. 2003, "Initiatives and outcomes of quality management implementation across industries", *Omega—The International Journal of Management Science*, 31(2), 141–154.

Lai, K.H., Cheng, T.C.E. and Yeung, A.C.L., 2005, "Relationship stability and supplier commitment to quality", *International Journal of Production Economics*, 96(3), 397–410.

Lee, H.L. and Whang, S., 2005, "Higher supply chain security with lower cost: lessons from total quality management", *International Journal of Production Economics*, 96(3), 289–300.

Lun, Y.H.V., Lai, K.H. and Cheng T.C.E., 2006, *Shipping and Transport Logistics*, McGraw Hill: Singapore.

Morgan, N.A. and Piercy, N.F., 1996, "Competitive advantages, quality strategy and the role of marketing", *British Journal of Management*, 7(3), 231–246.

OECD, 2003, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, OECD: Paris.

Prokop, D., 2004, "Smart and safe borders: the logistics of inbound cargo security", *International Journal of Logistics Management*, 15(2), 65–75.

Raven, J., 2001, *Trade and Transport Facilitation: A Toolkit for Audit, Analysis and Remedial Action*, The World Bank (WDP 427): Washington DC.

Robinson, C.J. and Malhotra, M.K., 2005, "Defining the concept of supply chain quality management and its relevance to academic and industrial practice", *International Journal of Production Economics*, 96(3), 315–337.

Russell, D.M. and Saldana J.P., 2003, "Five tenets of security-aware logistics and supply chain operation", *Transportation Journal*, 42(4), 44–54.

Sletner, T.C., 2000, "Quality system for the implementation of STCW-95 in higher maritime education in Norway", *Maritime Policy and Management*, 27(1), 89–100.

Tzannatos, E.S. 2003, "A decision support system for the promotion of security in shipping", *Disaster Prevention and Management*, 12(3), 222–229.

Van De Voort, M. (2003), *Seacurity: Improving the security of the global sea container shipping system*, MR–1695-JRC, RAND Europe: Brussels.

Westphal, J., Gulati, R. and Shortell, S., 19, "Customization or conformity: An institutional and network perspective on the context and consequences of TQM adoption", *Administrative Science Quarterly*: 42(2), 366–394.

Willis, H.H. and Ortiz, D., 2004, *Evaluating the Security of the Global Containerised Supply Chain*, RAND technical report series, RAND Europe: Brussels.

This page intentionally left blank

CHAPTER 15

MANAGING SUPPLY-CHAIN SECURITY THROUGH QUALITY STANDARDS: A CASE STUDY TO IMPLEMENT ISO 28000 IN A GLOBAL COFFEE HOUSE

Francis D'Addario

Starbucks Coffee

Abstract

Global security professionals responsible for the safe conduct of world trade are reckoning with enterprise threats that have taken on new dimensions since 9/11. Although governments and heads of state remain the arguable targets for regime change by terror organizations, supply-chain economics of entire regions if not the world are at risk. Transnational security conventions that mitigate this risk will require a joint effort by nation states and commerce. Importantly, supply-chain security goes far beyond the needs of any country or commercial interest. It enables people, producers and consumers, the potential hope for developing economies, jobs and standards of living. All remain compelling alternatives to terror for real social change. This chapter outlines the needs and benefits of an integrated supply-chain security system through describing how the adoption of ISO 28000 standards has enabled a global coffee house to continuously improve its supply-chain security. The Guatemala case presented here and its extensions to other supply-chain security processes good serve as a road-map for other supply-chain stakeholders and interests for similar undertakings.

1 INTRODUCTION

The potential risk for containers and other conveyances of trade to be used as an intercontinental delivery system for weapons of mass destruction is real. Analysts persuasively argue that trade may not be merely a means to this end but the primary target. Resulting disruptions would impair commerce as we know it. Democratic societies voting with their pocket book interests demand protections. Thus, we witness a certain preoccupation by politicians with numerous self-centred legislative efforts to protect their constituencies.

It is reasonable to assume that weapons of mass destruction do not have to travel beyond port facilities. Any detonation of a container in a port facility is likely to shut down operations and cause widespread panic in adjacent population centres. Government agencies will likely shut down commerce to assess the situational risk. Commerce was the target objective of 9/11 and 7/7 and many other plots presumably foiled. Shutting commerce down to protect it would achieve the terror agenda.

Supply chains like their relatives, computerized networks are not just vulnerable at the hubs but on the perimeter at all points of entry. Security systems that are sustainable will adopt auditable conventions that protect from the "inside out" to all points of remote consolidation. Processes must be pragmatic and scaleable. They must assure security integrity of trusted agents and goods whether at rest or in transit. Access control must consider due diligence and identity verification processes for all persons, conveyances, pre-loading, loading, and in-transit inspections. Proactive prevention at loading and conveyance points, together with exception reporting will likely deny opportunity for both terrorists and organized crime.

Securing trade hubs is only one part of the equation. Hubs are the spider webs that connect world trade. Our attention must encompass all nations and all means of transit. Integrity assurance will extend to goods, conveyances, facilities, people and systems. ISO 28001 was developed by an international body of stakeholders to enable a constructive methodology for this task. From World Customs Organization guidelines, it is a risk-based formula that encompasses the simultaneous requirements of many nation states and the private sector to move proactively to secure supply chains.

Starbucks hopes to incrementally and continuously improve its ability to deter, detect and mitigate potential attacks on its supply chain. ISO 28001 allows us to build on a path begun with C-TPAT compliance that will be locally relevant around the world. Starbucks Coffee is adopting ISO 28001 as the means to continuously improve its supply-chain security. Starbucks recognized ISO adoption as a strategic opportunity; not only to mitigate risk but to potentially qualify for preferential trade lane consideration. This requires more than sourcing the highest quality coffee, tea and cocoa. It relates directly to the firm's ability to transport, roast, blend and distribute with integrity worldwide. That assurance makes possible the economic efficiencies necessary for premium prices to the company's farmers and suppliers, benefits for its supply-chain partners, and a world class consumer confidence.

2 STATEMENT OF COVERAGE, RISK ASSESSMENTS AND THE SECURITY PLAN: THE GUATEMALA CASE

ISO 28001 is a publicly available specification (PAS) that enables organizations to voluntarily establish, document and validate reasonable levels of security for their supply chains. Perhaps most importantly it enables organizations to define boundaries covered by a security plan based on risk assessment. Thus, finite resources may be efficiently directed at the highest risk portions of a supply chain for prioritized mitigation. Security assessments should reasonably consider threat scenarios. Resultant security plans detail the boundaries, relative threat assessments and security mitigation measures.

Source: Air Security International

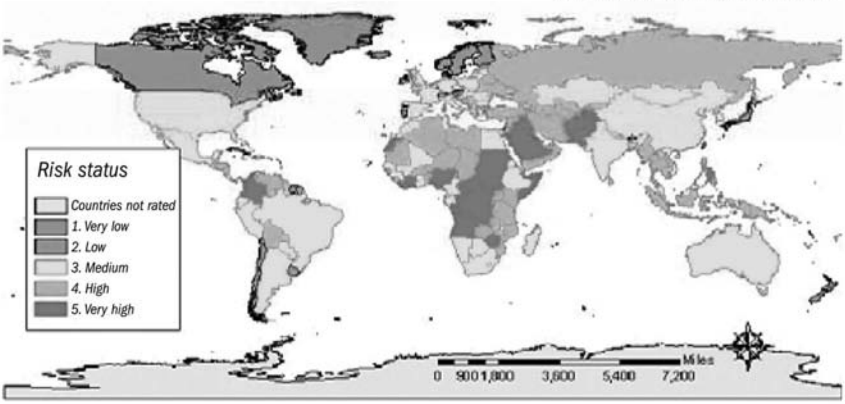


Figure 1: Country risk status.

Country risk maps like the one above are available from a number of sources including Air Security International. Let's consider Starbucks Guatemala supply chain as an example for ISO compliance adoption. Starbuck's Partner and Asset Protection team regularly calculates risks to coffee from origin to domestic roasting and distribution facilities. On a relative scale of country risk, Guatemala appears to be high risk prior to any mitigation. High crime rates and instability in the region following 30 years of civil war are two factors in the analysis. Others include quantity of coffee from the region.

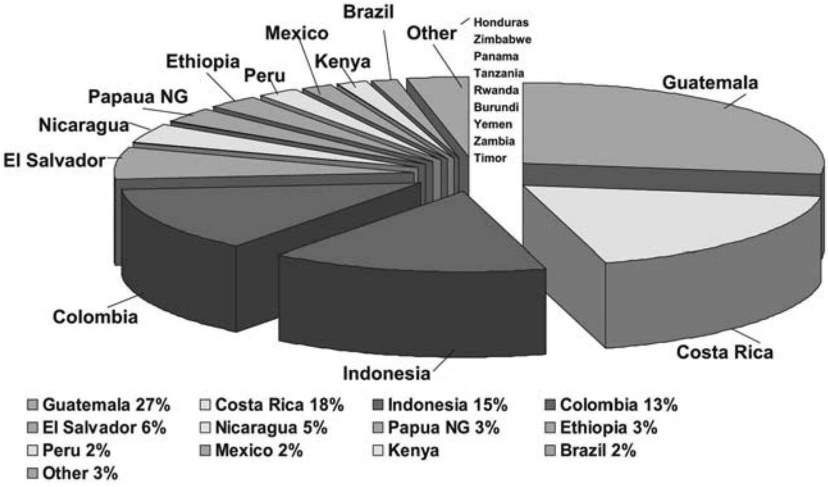


Figure 2: The risk to coffee from the countries of origin to roasting and distribution facilities.

Using an "off the shelf" country risk tool, a baseline may be established for individual segments or an entire supply chain. Similarly our evolving security plan details measures in place to mitigate identified risks. Hence a matrix view may develop detailing the risk, the countermeasure and any relevant metrics. Objectives should always map back to the security mission. A number of risks, mitigations and measures may overlap supply chains to form the security plan.

In our case, the security mission is to protect people, secure assets and contribute margin. People include our customers, partners and fellow citizens. Assets include goods in transit or at rest from coffee to protected information. Margin contributions may include items ranging from cost avoidance through efficiencies and prevention to asset recoveries. Measuring countermeasures also enables both process improvement and authentication of compliance by auditors. A simple matrix of mission objectives, risk or threat assessments follow. Contextually, these are the security plan elements.

Objective	*Risk threat*	*Mitigation, policies and procedures*	*Measures, benchmarks and gaps*
People safety: Partners, customers, and service providers	• Consumer safety • Partner safety • Violent crime • Health hazards • Safety hazards • Travel hazards • Terrorism	• Access control • Preventive patrol • Supply chain security • Health compliance • Safety compliance • Threat/risk/ reporting • Travel compliance	• Due diligence • PACOM/ESP • CTPAT/ISO • Tracking • Exceptions • Audit scores • Partner view
Asset protection: Facilities, goods, products, and information	• Unauthorized access • Property destruction • Tampering • Theft • Extortion	• Access control • Intrusion detection • Surveillance detection • Quality assurance • Inventory control • Exception reporting • Conduct reporting	• Due diligence • Incidents • PACOM/ESP • Security patrol • OS&D • Inventory • Audit scores

Objective	*Risk threat*	*Mitigation, policies and procedures*	*Measures, benchmarks and gaps*
Profitability: Cash, E-commerce, and royalties	● Theft ● Fraud ● Diversion ● Counterfeiting ● Inadequate security	● Access control ● Exception detection ● Code of conduct ● Compliance audits ● Conduct reporting	● Due diligence ● Profit/loss ● Programme analysis

Table 1: Security Plan Elements

Common themes develop that suggest a number of threat scenarios to test any plan. Previous historical data and anecdotal information on attacks of peer enterprises will instruct the process. An attack on any food processor should be routinely brought to the attention of our threat analysts. Similarly mitigation measures may be leveraged to address multiple threats. Interactive access control systems (video and audio enabled) with exception reporting can arguably deter, detect, expedite response and mitigate threats ranging from unauthorized intrusion to violent crimes including contamination. Ancillary threats are also detectable and may be mitigated including fraud and theft. The same processes that will keep supply chains safe and profitable will arguably deny unauthorized access or use of a supply chain for more sinister purposes including the delivery of a weapon of mass destruction. Either assessment model illustrated in the PAS 28001 informative annexes will be helpful in evaluating your security process. A classification of consequences may prove helpful in prioritizing mitigation opportunities in the plan. Both tools follow below.

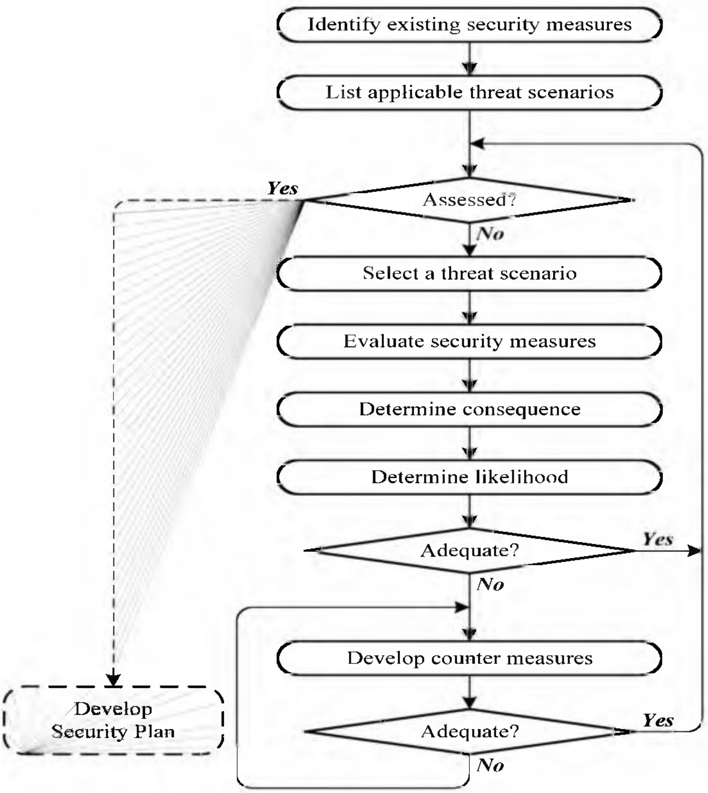


Figure 3: A Decision Support and Process System for Developing Security Plans

In the case of Guatemala the risk posed by criminal enterprise is nominally measurable. Mitigations were adopted by both Starbucks Coffee and our suppliers prior to 2001 including robust physical security measures for access control ranging from fenced perimeters and video equipped security patrols to armed transport of containers. Adoption of C-TPAT in 2002 and participation in Operation Safe Commerce through 2003 detailed gaps and opportunity for improvement in container documentation including demonstrated efficacy of affordable smart container security devices by 2006.

The potential consequences of a given threat scenario particularly influenced mitigation and countermeasure thinking. ISO 28001 similarly informs the process.

Threat scenarios	*Application*
1 Intrude and/or take control of an asset (including conveyances) within the supply chain	Damage/destroy an asset (including conveyances) Damage/destroy outside target using the asset or goods Cause civil or economic disturbance Take hostages/kill people
2 Use the supply chain as a means of smuggling	Illegal weapons into or out of the country/economy Terrorist into or out of the country/economy
3 Information tampering	Locally or remotely gaining access to the supply chain's information/documentation systems for the purpose of disrupting operations or facilitating illegal activities
4 Cargo integrity	Tampering, sabotage and/or theft for the purpose of terrorism
5 Unauthorized use	Conducting operations in the international supply chain to facilitate a terrorist incident including using the mode of transportation as a weapon
6 Other	N/A

Table 2: Threat Scenarios and their Corresponding Applications

In Guatemala, crime is a tangible threat even though approximately 80% of crimes may go unreported due to a lack of public confidence in the judicial system and the police. Major legislative reforms are underway, however, to potentially improve risk. Great strides have been made in only 10 years since the country emerged from civil war according to Bustamante (2006). He goes on to stress that private sector security proliferation including armed escorts of containers has improved some conditions. Even so, an estimated eight to 12 transports per day are stolen or diverted. Starbucks-bound coffee containers travel in armed convoys from coffee mills to the ports of Quetzal and Santo Tomas to mitigate this risk. Additionally a combination of trusted trained agents, security protocol, container security devices and digital television documentation will ensure that untampered, properly inspected, sealed and secure containers in the very near future.

Optimism prevails for improvement in general security conditions as both political parties in Guatemala show interest in a creation of a national security system that will incrementally professionalize public and private sector security capabilities. Starbucks intends to advise and support to the extent possible its partners and government security professionals in this effort. In addition to ISO 28001 and container security device adoptions Starbucks is working diligently with port authorities, ANACAFE and providers including CAFCOM and VOLCAFE to perfect security and quality assurance processes. The pictographic process below depicts digital video documentation of container inspection and device tracking from Guatemala to Seattle and all relevant points of distribution.

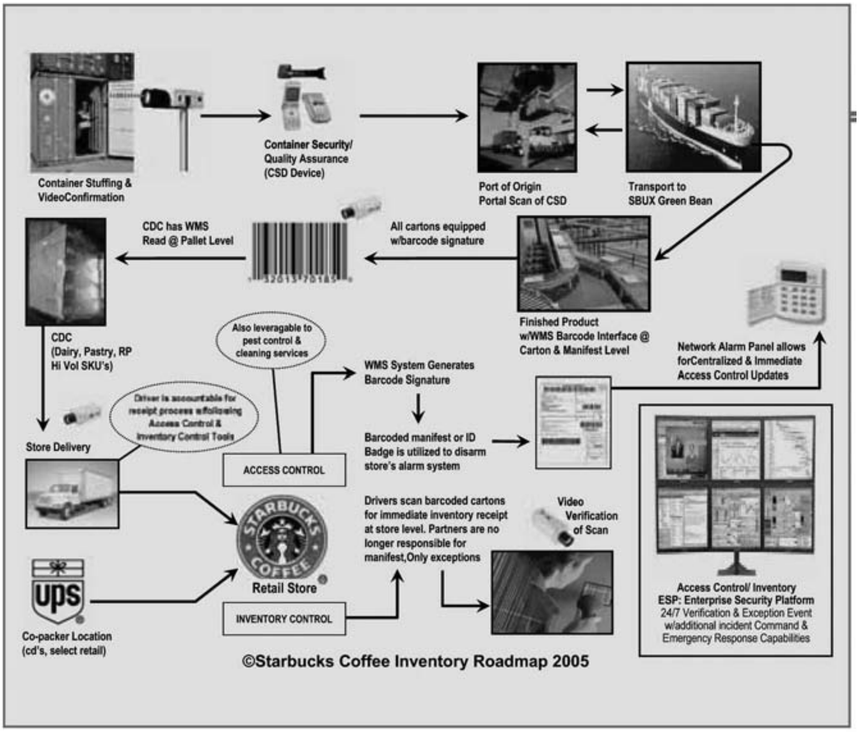


Figure 4: Origin to Store Floor Inventory Control Strategy Map

Starting at the top left, the trusted agent inspects the container prior to loading the finest Arabica coffee beans available in the region. Moving to the right the GE security device is added to the container to report security conditions on key movements. "Hand held" devices and fixed devices at the mill, ports and roasting plants enable "need to know" government and private sector "trusted agents" to be assured that the container has not experienced any unauthorized openings. Additionally exceptional conditions will be detected, reported, recorded and mitigated well before a container arrives at destination. Starbucks is building a 24/7 networked interactive enterprise security platform that will serve as a exception based command centre 2 for shipping exceptions, partner travel emergencies (depicted in the lower right).

Starting at the top left the trusted agent inspects the container prior to loading the finest Arabica coffee bean available in the region. Moving to the right the GE security device is added to the container to report security conditions on key movements. "Hand held" devices and fixed devices at the mill, ports and roasting plants enable "need to know" government and private sector "trusted agents" to assure that the container has not been opened.

These and additional exceptional conditions including heat and humidity (that may effect quality assurance) will be detected, reported, recorded and mitigated well before a container arrives at destination. If a container is deemed "exceptional" when arriving at the plant it may be inspected by trained partners who are capable of detecting Hazmat conditions in protective gear without risking the operational viability of a facility.

Once the coffee is roasted and other inventory is picked it may be tracked to store destinations. Bar code licences affixed to cartons and manifests or credentials will enable peripherals to track both authenticated inventory and trusted agent delivery personnel. A 24/7 enterprise security platform is currently being built to potentially monitor exceptional conditions for supply chain partner movements, and inventory credentials; in addition to tracking the security status of critical facilities and security services personnel.

3 CONCLUSION

Sustainable supply chain is not just about technology, it is also about repeating scaleable processes with dedicated partners in a transparent environment. That requires engagement of all stakeholders not only to assess and reassess their portion of the supply chain but train and re-train the desired objectives. At the end of the day we have to speak the same language for expectations. That will allow us to communicate exceptions and mitigate both security and quality assurance risks with "need to know" individuals. It will also make possible our collective reliance on healthy supply-chain benefits going forward.

The case of Guatemala described in this chapter serves as a prototype of Starbucks supply-chain security processes. It was initially repeated for all high risk supply chains and has evolved as a standard for sustainable procurement.

In this chapter, we do not endeavour to detail our security plans; our intent is merely to validate the tools and information set forth in ISO 28001. The objective to provide international supply-chain owners and governments a pragmatic security reference has been well met by ISO 28001 in the author's opinion. This is a pragmatic and auditable effort to reflect the requirements of global trade well within the World Customs Organization and ISO standards.

Most importantly, its legacy will be a calculable benefit to all who rely on safe and secure supply chains for years to come.

REFERENCES

Bustamante, E.R., 2006, “Where are We Going with Security?”, *Primera Convencion Regional de Seguridad Corporativa*, Guatemala, 26 May 2006.

International Standardization Organization, 2006, *ISO/TC 8/SC 11, Best Practices for Implementing Supply Chain Security, assessments and plans*, PAS 28001, Draft International Standard (4/4/2006), ISO: Geneva.

World Customs Organization, 2006, Framework of Standards to Secure and Facilitate Global Trade: SAFE, WCO: Brussels.

PART IV

MODELS FOR ANALYSING SECURITY RISKS AND POLICY IMPLICATIONS

CHAPTER 16

MARITIME SECURITY AND REGULATORY RISK-BASED MODELS: REVIEW AND CRITICAL ANALYSIS

Khalid Bichou

Port Operations, Research and Technology Centre (PORTeC), Centre for Transport Studies, Imperial College London

Andrew Evans

Imperial College London and the Lloyd's Register Centre for Transport Risk Management, London, UK

Abstract
The primary aim of maritime security assessment models is to assess the level of security within and across the maritime network. When managing risk through legislation, regulatory assessment models are used to assess risk levels and examine the impact of policy options, usually in terms of the costs and benefits of a regulatory proposal. This chapter reviews the development, application and adequacy of existing risk assessment and management models to maritime and port security. In particular, we examine the problematical issues of security perception, value and impact, and discuss the limitations of the current regulatory framework in providing an integrated and effective approach to risk assessment and management including for supply-chain security.

1 INTRODUCTION AND BACKGROUND INFORMATION

Since the 9/11 terrorist attacks in the US in 2001 and with the growing concern about the security of the international movement of goods and passengers, several frameworks have been introduced either on a compulsory or voluntary basis with a view to enhancing maritime and port security. Regulatory measures that have been multilaterally endorsed and implemented include the International Ship and Port Facility Security (ISPS) code, the IMO/ILO code of practice on security in ports, and more recently the "Framework of Standards to Secure and Facilitate Global Trade" commonly referred to as the "WCO Framework". Other statutory instruments with less global coverage, yet greater scope and implications, have been introduced on a local or regional scale. Among these, the US-led initiatives are probably the most significant and consist of a multi-layer regulatory regime involving measures such as the Container Security Initiative (CSI), the Customs-Trade Partnership against Terrorism (C-TPAT), the 24-hour advance vessel manifest rule (the 24-hour rule), the Public Health Security and Bioterrorism Preparedness and Response Act (Bioterrorism Act) and the Operation Safe Commerce (OSC). A third set of initiatives consists of primarily industry-led schemes such as the Smart and Secure Tradelanes (SST), the Star-Best programme and a series of ISO initiatives (ISO 28000, 28001, 28004 and 20858 series). Although many of these programmes have not yet been finalized, it is believed they will build up a more formal and effective framework and ensure a higher level of security assurance within and beyond the maritime network. For a detailed review of both mandatory and voluntary security programmes in ports and shipping, the reader is referred to Bichou, 2004, UNCTAD, 2004 and OECD, 2003/4.

With such complexities in the current maritime security framework, much of the literature on the subject has focused on prescriptive details of the measures being put in place as well as on their compliance costs and economic impacts. However, there has been little work on security-risk assessment and management models, be it at the physical or the supply-chain level.

The primary aim of maritime security assessment models is to assess the level of security within and across the maritime network. When introducing the risk factor, the concept and measure of uncertainty must be considered. The conventional approach to risk defines it as being the chance, in quantifiable terms, of an adverse occurrence. It therefore combines a probabilistic measure of the occurrence of an event with a measure of the consequence, or impact, of that event. The process of risk assessment and management is generally based on three sets of sequenced and interrelated activities:

- the assessment of risk in terms of what can go wrong, the probability of it going wrong, and the possible consequences;
- the management of risk in terms of what can be done, the options and trade-offs available between the costs, the benefits and the risks; and
- the impacts of the risk management decisions and policies on future options and undertakings.

Performing each set of activity requires multi-perspective analysis and modelling of all conceivable sources and impacts of risks as well as viable options for decision making and management. In engineering, traditional tools for risk assessment use the fault tree analysis (FTA) and the event tree analysis (ETA). Both are logical processes with the difference that the first examines all potential incidents leading up to a critical event while the second works the opposite way by focusing on events that could occur after a critical incident. In both models, risks are identified, estimated, assessed and prioritized through a combination of probability and impact. A simplified application of risk assessment models to the ISPS code would be to categorize and grade scenario-risks according to their overall threat potentials using a rating scale system from (1) for minor to (3) for severe to fit into the ISPS provisions of maritime security (MARSEC) levels.

Most of the general tools described above have been successfully applied across many areas of transport safety, and there seems to be a general consensus among researchers on standardized processes of assessment and management. Methodological questions, such as in terms of selecting or adjusting the appropriate tool, may not constitute a problem as much as data availability and accuracy may do. Nonetheless, these tools may not be relevant to assessing and managing transport security, including for the port and maritime network.

The essence of safety risk models is a probabilistic approach based on the assumption of unintentional human and system behaviour to cause harm. This is not the case for security incidents stemming from terrorism and we are not aware of the existence of any risk models being applied to malicious acts. Another major problem with assessing security threats is that much of the assessment process is intelligence-based, which does not always follow the scrutiny of statistical reasoning. Even with a sound intelligence risk approach, there are many uncertainties involved such as in terms of higher levels of noise in background data. An additional instance of inadequacy of conventional risk models to maritime security is the lack of historical data given the rarity of occurrence of large-scale terrorist incidents. Another important issue stems from the supply-chain dimension of the international shipping network, and as such data on the scope and levels of externalities are extremely difficult to extract and analyse. In either case, the security of the maritime network must be considered in both its physical and supply-chain dimension, the latter evolving around disruptions and risk-driven uncertainties in the supply chain.

In view of the above, this chapter reviews the development, application and adequacy of existing risk assessment and management models to maritime and port security. It introduces the reader to recent approaches to risk assessment and management and examines the link between physical and supply-chain security. However, not all aspects relevant to security-risk assessment and management in shipping and ports are discussed in this chapter, which limits the analysis to precursor and risk assessment, supply-chain security models and economic evaluation of regulatory measures.

2 PRECURSOR AND RISK ANALYSIS FOR MARITIME SECURITY INCIDENTS

Accident precursors, also referred to as accident sequence precursors, can be defined in different ways depending on the approach used such as in terms of causation or correlation. A broad definition of precursors may involve any internal or external condition, event, sequence, or any combination of these that precedes and ultimately leads to adverse events. More focused definitions reduce the range of precursors to specific conditions or limit their scope to a specified level of accident's outcome. For instance, the US nuclear regulatory commission (NRC) defines a precursor as any event that exceeds a specified level of severity (NRC, 1978), while other organizations incorporate a wider range of severities. In either case, a quantitative threshold may be established for the conditional probability of an incident given a certain precursor, with events of lesser severity being considered either as non-precursors with no further analysis or as non-precursors that need categorization and further investigation.

Several formalized programmes are available for observing, analysing and managing accident precursors including comparison charts and reporting systems. The latter have taken the lead in recent years as many organizations have designed and implemented them for taking advantage of precursor information, with the most recognizable reporting system being the colour alert system used by the US Department of Homeland Security (DHS). Relevant examples in ports and shipping include voluntary reporting initiatives for maritime safety (BTS, 2002), the IMB reports of piracy incidents and the IMO reporting system for ISPS compliance.

A major drawback resulting from the combination of warning thresholds and event reporting is that the system may depict several flaws and errors. If precursors are defined too precisely or the threshold is set too high, several risk-significant events may not be reported. On the other hand, setting the threshold for reporting too low may overwhelm the system by depicting many false alarms, and ultimately a loss of trust in the system. Table 1 shows the types of errors that may occur given these conflicting approaches. Type I error refers to a false negative and occurs in situations of missed signals when an incident (e.g. terrorist attack) occurs with no warning being issued. Type II error refers to false positive whereby a false alert is issued leading, for instance, to mass evacuation or a general disturbance of the system.

	Significant	*Not significant*
Event reported	True positive (Significant event)	False positive (Type II error)
Event not reported	False negative (Type I error)	True negative (Non-significant event)

Table 1: Errors Resulting from the Interplay between Threshold Settings and Event Reporting (from Phimister *et al.*, 2004, p. 7)

Another issue arises when reporting precursor events under regulatory constraints. The fact that much of reported data remains in the hands of the regulator raises questions about (a) the reliability and validity of information since fears of regulatory actions may discourage organizations from reporting precursor events and (b) the dissemination of reported information given that the regulator may restrict access to data which is considered too sensitive to be shared. The argument here is that the purpose of reporting must emphasize organizational learning along with a guarantee of privacy and immunity from penalties for those reporting the information.

A particularly useful concept developed from precursor analysis is the so-called "near miss" also referred to as the near hit or the close call. A near miss is a particular kind of precursor with elements that can be observed in isolation without the occurrence of an accident. The advantage of the concept is that organizations with little or no history of major incidents can establish systems for reporting and analysing near misses. This is because it has been found that near misses occur with greater frequency than the actual event (Bird and Germain, 1996). This argument is even made stronger with much of the literature on reported transport accidents confirming that near misses have usually preceded the actual incidents (Cullen, 2000; BEA, 2002).

In ports and shipping, implementing programmes of security assessment based on precursor analysis would have a number of benefits including for such aspects as identifying unknown failure modes and analysing the effectiveness of actions taken to reduce risk. Another opportunity from precursor analysis is the development of trends in reported data, which may be used for the purpose of risk management and mitigation. Even so, we are not aware of any formal precursor programme being implemented in the context of port and maritime security, except for on-going research into potential security hazards for liquid-bulk and specialized ships such as LNG and LPG vessels. On the one hand, inherently secure designs against the threats of terrorism and other similar acts are yet to be developed, although improvements have been made in ship design for safer and sustainable transportation. On the other hand, existing reporting schemes of security incidents in shipping and ports depict noticeable gaps in both content and methodology. This is the case for instance for piracy and armed robbery incidents whereby available reports show general information with no sufficiently detailed data to display and analyse incident precursors.

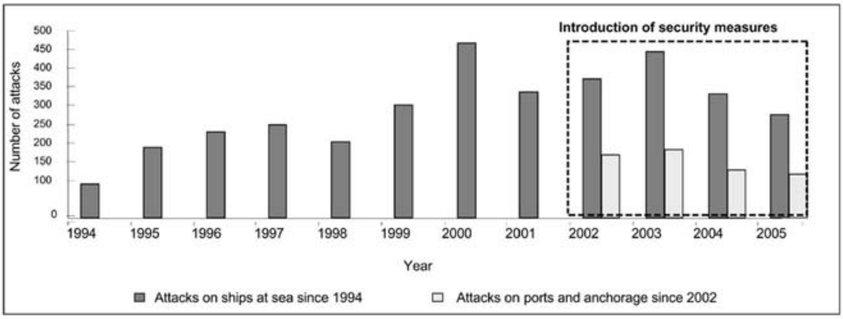


Table 2: Reported Actual and Attempted Piracy Incidents on Ships and Ports (compiled by us from IMB & IMO piracy reports)

Analysis of accident precursors can also be useful in conjunction with probabilistic risk analysis (PRA). PRA is a quantitative risk assessment method for estimating risk failure based on system's process mapping and decomposition into components (Bier, 1993; Bedford and Cook, 2001). PRA has been used in a variety of applications including risk analysis in transportation systems. PRA can be combined with precursor analysis to quantify the probability of accidents given a certain precursor, thus helping in prioritizing precursors for further analysis or corrective actions. The method can also be improved based on precursor data analysis, for instance, by checking on the validity of PRA model assumptions.

Hence, against conventional approaches of risk assessment based on probabilistic measurements of observed accident frequencies, precursor analysis ideally combined with other techniques such as near-misses and PRA methods provides an effective framework for risk assessment and management in the context of maritime security. Security assessment and management in shipping and ports may also be analysed by examining the reliability and robustness of the maritime network. This could be one way from which an analytical approach may be developed, for instance, towards the complex network theory (Bichou, 2005; Angeloudis *et al.*, 2006; Bell, 2006).

3 THE SUPPLY-CHAIN RISK DIMENSION OF MARITIME SECURITY

Since the introduction of the new security regime in shipping and ports, researchers and practitioners alike have questioned the wisdom of such a plethora of regulations. Others have justified the overlap of these programmes by the need to establish a multi-layer regulatory system in an effort to fill potential security gaps (Flynn, 2004; Willis and Ortiz, 2004). The concept of layered security is not entirely new to transport systems and dates back to the 1970s. Prior to the introduction of new maritime security measures, the concept has also been cited in 1997 in the context of aviation security (Gore Commission, 1997).

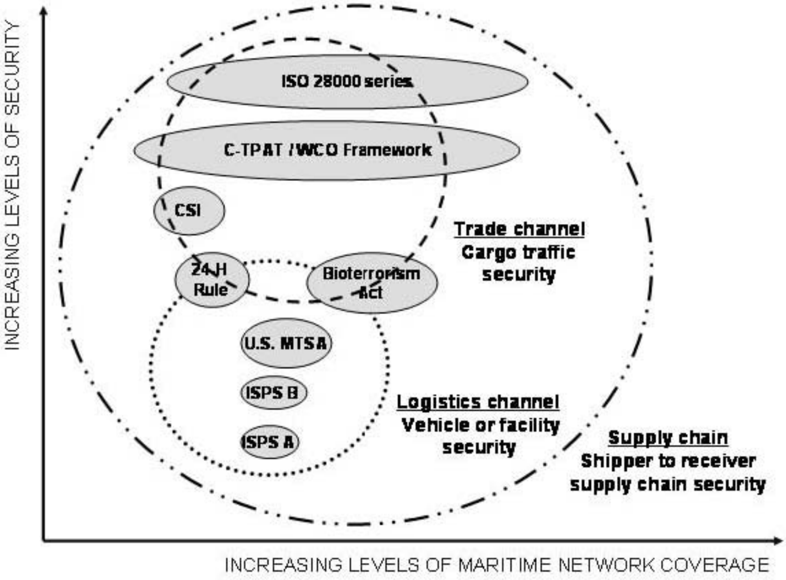


Figure 1: Hierarchy of Security Measures by Level of Security and Maritime Network Coverage

In our model, the supply chain (or supply channel) encompasses both the logistics and trade channels, but rarely oversees the different arrangements within each of them. The logistics channel consists primarily of specialists (carriers, freight forwarders, 3PLs, etc.) that facilitate the efficient progress of cargo through, for example, warehousing and transportation. Both the trade channel and supply channel are associated with the ownership of goods moving through the system, with the difference that the trade channel is normally perceived to be at the level of the sector, the industry or the nation (e.g. the oil trade, the containerized trade, the US–Canada trade) and the supply channel at the level of the firm (Toyota or Wall-Mart respective supply chains). For each channel, one or a combination of physical, information and/ or payment flows is taking place. Figure 2 depicts the interactions between channels and flows in a maritime network system. For simplification, channel and flow configurations are depicted in linear path combinations, although a better illustration would be in terms of web-type networked relationships.

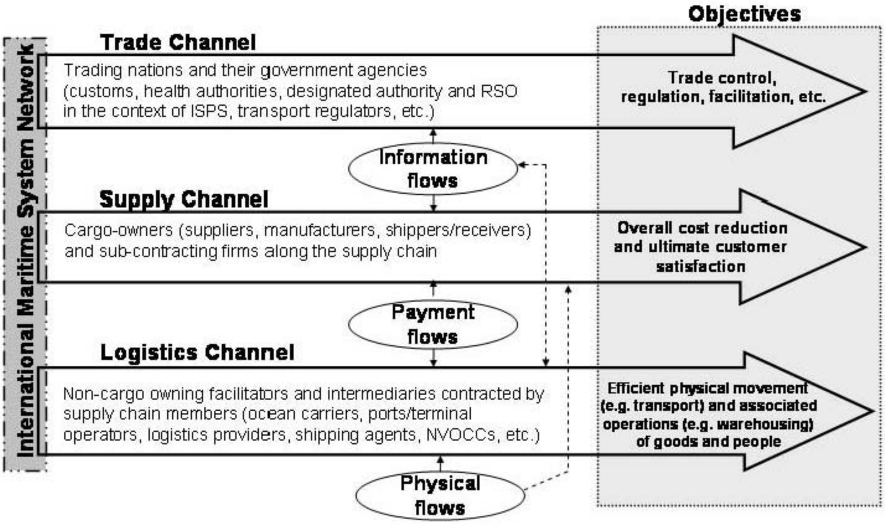

Objectives
International Maritime System Network
Trade Channel
Trading nations and their government agencies (customs, health authorities, designated authority and RSO in the context of ISPS, transport regulators, etc.)
Trade control, regulation, facilitation, etc.
Information flows
Supply Channel
Cargo-owners (suppliers, manufacturers, shippers/receivers) and sub-contracting firms along the supply chain
Overall cost reduction and ultimate customer satisfaction
Payment flows
Logistics Channel
Non-cargo owning facilitators and intermediaries contracted by supply chain members (ocean carriers, ports/terminal operators, logistics providers, shipping agents, NVOCCs, etc.)
Efficient physical movement (e.g. transport) and associated operations (e.g. warehousing) of goods and people
Physical flows

Figure 2: Channel Typologies and Components of the Maritime Network System

To illustrate the need for a layered framework to maritime security, consider a typical global movement of a containerized cargo, which is estimated to involve as many as 25 parties and a compound number of flow-configurations within and across the maritime network (Russell and Saldana, 2003). The role and scope of control exercised by members of the supply channel (mainly manufacturers, shippers and receivers) would only oversee the management of direct interactions between them rather than the details of logistical arrangements. Arrangements such as cargo consolidation and break bulk, multi-modal combinations, transhipment and reverse logistics are typically performed by third parties including carriers, ports and other intermediaries. In a similar vein, the trade channel stakeholders (customs, health authorities, regulators, etc.) may be able to scrutinize and monitor the logistical segment within their own national territory, but would have little or no control over arrangements taking place in a foreign country including at transit and transhipment locations. Thus, the combination of intersecting functional and institutional arrangements across the supply chain makes it almost impossible for a single actor within a single channel to effectively trace and monitor operations across different channels.

One can argue, however, that the layered approach, as being currently implemented, has not yet materialized into an integrated and comprehensive system capable of overcoming existing and potential security gaps. For instance, the emphasis on goods and passenger movements has diverted the attention away from non-physical movements such as financial and information flows. Similar observations can be made for outbound cargo and the associated flows and processes. Other gaps include the exclusion from the current regulatory regime of fishing vessels, pleasure crafts and yachts, and other commercial ships of less than 500 GT. There is also a lack of harmonization between the new security regime and other maritime environmental and safety programmes such as the STCW Convention and the ISM and IMDG codes. No wonder why the emphasis has been shifting to more comprehensive tools such as C-TPAT and ISO programmes.

Another aspect of interest when examining maritime network security is the interplay between supply-chain security and supply-chain risk, the latter being closely related to uncertainties stemming from specific supply-chain configurations. Juttiner *et al.* (2003) review the literature on supply-chain risk management and categorize sources of supply chain-risk into three major groups:

- environmental risk sources corresponding to uncertainties associated with external sources such as terrorism or environmental risks;
- organizational risk sources relating to internal uncertainties within the supply chain, for instance strikes or production failures; and
- network-related risk sources referring to uncertainties arising from the interactions between organizations in the supply chain.

The current maritime security framework strongly emphasizes environmental and organizational risk sources, but there is less focus on network-related vulnerabilities. However, excluding or minimizing network-related risk sources may overlook the capacity of the system to either absorb or amplify the impact of events arising from environmental or organizational sources. Examples of network-related risk drivers in maritime security include uncertainties caused by contracting with non-compliant (non-certified) supply-chain partners. A recent study involving 20 top US firms has shown that there is a tendency among American shippers towards trading off lowest bidders with known suppliers (MIT/CTS interim report, 2003). In the context of C-TPAT, this could imply trading-off foreign manufacturers with national suppliers; and for a US firm with a global sale outreach, this could even imply trading-off producing in the USA against transferring operations abroad. There have been similar examples across the shipping and port industry, for instance, shipping lines changing their ports of call because of the existence or absence of a regulatory programme.

4 ECONOMIC EVALUATION AND APPRAISAL OF MARITIME SECURITY MEASURES

Several attempts have been made to assess the cost impacts of new security regulations, mainly the ISPS code. Table 3 summarizes aggregate estimates

			Costs in $ million		
Source of estimates	*Cost items*	*Scope*	*Initial costs*	*Annual costs*	*Overall cost over 10 years (2003–2013) @ 7% discount rate*
USCG	Total ISPS US ports	226 port authorities, of which 5000 facilities are computed (from Fairplay) (ISPS Parts A & B MARSEC Level 1)	1125	656	5399
	Total ISPS US-SOLAS and non-SOLAS vessels subject to the regulation	3500 US-flag vessels, as well as domestic and foreign non-SOLAS vessels (i.e. operating in US water) (ISPS parts A & B MARSEC level 1)	218	176	1368
	Automated identification system		30	1	50
	Marititime area (contracting government)	47 COTP US zones	120 (+ 106 for 2004)	46	477
	OSC facility (offshore installations)	40 US OCS facilities under US jurisdiction	3	5	37
	US cost for ISPS implementation	(ISPS parts A and B)	115	884	7331
	Aggregate cost of elevating MARSEC level from 1 to 2	Based on twice MARSEC level 2 per annum, each for 21 days	16 per day		
UK	Total ISPS UK port facilities	430 facilities (ISPS parts A MARSEC level 1)	26	2.5	
	Total ISPS UK-flagged ships and company related costs	620 UK-flag vessels (ISPS parts A, MARSEC level 1) (calculations based on an exchange rate of US$ = UK £1.6	7.4	5.2	
OECD	AIS	Based on 43 291 international commercial fleet of more than 1000 GT (passenger and cruise vessels not included), MARESC level 1, ISPS part A only	649.3	Undetermined	
	Other vessel measures		115.11	14.6	
	Ship operating companies		1163.89	715.4	
	Total ships and shipping companies		1279	730	
	PFSA, PFSA, PFSO	2180 port authorities worldwide, of which 6500 facilities are computed (from Fairplay) (ISPS part A only MARSEC level 1)	390.8	336.6	
	Total ISPS ports		Undetermined	Undetermined	
	Global cost for ISPS implementation	(MARESC level 1, ISPS part A only)	Undetermined	Undetermined	
Australian Government	Total costs for Australia	70 ports, of which 300 port facilities. 70 Australian flag ships	240	74	

Table 3: Summary of Isps Cost Estimates as Calculated by Various Regulatory Risk Assessment Tools (compiled from various sources)

for the ISPS cost-compliance. Note that all such estimates were based on national risk assessment models such as the US national risk assessment tool and the UK risk assessment exercise (US N-RAT, 2003; UK RAE, 2004), and thus they were calculated for the purpose of cost assessment of what was at the time "the ISPS proposal", and in any case before its adoption and implementation.

In evaluating the costs and benefits for optimal regulatory decisions, cost-benefit analysis (CBA) is regarded as a fairly objective method of making assessments. Cost-efficiency analysis (CEA) is an alternative method to CBA usually applied when the output is fixed and the economic benefits cannot be expressed in monetary terms. CBA and CEA are widely used to assess the efficiency of various measures and alternatives such as in terms of a new regulatory regime or a new investment (e.g. in infrastructure or technology). In the context of maritime regulation, CBA was first introduced by the Formal Safety Assessment (FSA) guidelines as approved by the IMO in 2001, and later adopted in most subsequent regulatory programmes including for regulatory assessment of the ISPS code and other related measures.

However, in a typical CBA or CEA model the results of implementing a regulation can be entirely different from one stakeholder (firm, nation-state, etc.) to another. The concept of externality is very difficult to apprehend in the context of malicious incidents. According to the definition of externality, costs arising from accidents are external when one person or entity causes harm to another person involved in the accident, or a third party, without providing appropriate compensation. Risk decisions regarding the introduction of regulatory measures involve multiple stakeholders who influence decisions through a complex set of legal and deliberative processes. Whether this is beneficial to the whole community or not is very debatable given the differences between stakeholders' values and perspectives. In a typically fragmented maritime industry, this focus raises the important question: costs or benefits to whom? In other words, who will bear the cost of or gain the benefits from the compliance with statutory measures.

To correct CBA/CEA deficiencies particularly with regard to cost sharing and distribution, stakeholder analysis (SHA) was introduced in the early 1980s. SHA is designed to identify the key players (stakeholders) of a project or a regulation, and assess their interests and power differentials for the purpose of project formulation and impact analysis. Several procedures have been proposed for SHA implementation, with the World Bank four-step formula (stakeholders identification, stakeholders interests, power and influence inter-relationships and strategy formulation) being the most recognized and widely used. It must be noted, however, that there is no clear-cut predominance of one method over another, and quite often not all the conditions for the implementation of a complete regulatory assessment exercise are met.

An important element in any valuation method of new regulatory decisions is the cost of preventing principal losses in security incidents, a key component of which stems from human casualties, that is, fatalities and injuries. However, since the value of these losses is not observable in market transactions, most economists believe that these valuations should be based on the preferences of those who benefit from security measures and who also pay for them, either directly or through taxation. In the context of casualty prevention, these preferences are often measured using the "willingness to pay" (WTP) approach, that is, the amount people or society is willing to pay to reduce the risk of death or injury before the events. There are two major empirical approaches to estimating WTP values for risk reductions, namely the revealed preference method (RPM) and the stated preference method (SPM). RPM involves identifying situations where people (or society) do actually trade off money against risk, such as when they may buy safety (or security) measures or when they may take more or less risky jobs for more or less wages. SPM, on the other hand, involves asking people more or less directly about their hypothetical willingness to pay for safety/security measures that give them specified reductions in risk in specified contexts. The WTP approach has been extensively used in the context of road safety, but little literature exists on the use of the methodology in the context of shipping safety, let alone in the context of maritime and port security. The problem with the WTP approach in the latter context is that it is difficult to assume that people or society are capable of estimating the risks they face from terrorism (RPM) or that they are willing to answer questions about trading-off their security, or safety, against a given amount of money (SPM).

In addition to compliance cost, other costs arise from implementing the new regulatory requirement. These mainly refer to commercial and operational costs stemming from potential inefficiencies brought about by the new measures. For instance, one study has estimated that the security measures introduced in the awake of the 9/11 terrorist attacks, including transport-related initiatives, would cost the US economy as much as $151 billion annually, of which $65 billion is just for logistical changes to supply chains (Damas, 2001). Against this, a simulation game exercise of a terrorist attack on a major US port has found that it could cost as much as $50 billion with a backlog of up to 60 days (Grenscer *et al.*, 2003).

Another way to analyse the cost-benefit of a regulatory change is to contrast transfer costs against efficiency costs. The first refer to the costs incurred and recovered by market players through transferring them to final customers (e.g. from ports to carriers to shippers), while the second represent net losses in consumer/producer surpluses. Note that such analysis is not without bias, including the common practice of cost spin-off and exponential computations of security expenses. Table 4 provides a sample list of terminal security fees as charged by major ports and terminal operators.

Example of average terminal security fees			*$/TEU*
Australian ports (those operated by P&O Ports)			3.8
Europe	Belgian ports		10.98
	Denmark		61
	Dutch ports		10.37
	French ports		10.98
	Italian ports		9.76
	Latvian ports		7.32
	Norwegian ports		2.44
	Spanish ports		6.1
	Irish ports		8.54
	Swedish ports (Gothenburg)		2.6
	UK ports	Felixstowe (HPH)	19 for import and 10 for export
		Harwich	19 for import and 10 for export
		Thames port	19 for import and 10 for export
		Tilbury	12.7
Canada	Vancouver		2.7% increase in harbour dues
	TSI terminal handling charges		1.5
USA	Charleston, Houston, Miami		5
	Gulf seaports marine terminal conference		2
Others	Shenzhen		6.25
	HK		6.41
	Mexico		10

Table 4: Summary of Press Reports on Port's Container Security Charges

(*Source*: various news articles from *Lloyd's List*, *Fairplay* and *Containerisation International*)

5 CONCLUSION

This chapter is intended to serve as a conceptual piece that draws from the interplay between engineering and supply-chain approaches to risk in the context of recent maritime security regulations. It is hoped that cross-disciplinary analysis of the perception and impact of the security risk will stimulate thinking on appropriate tools and analytical frameworks for enhancing port and maritime security. In so doing, it may be possible to develop new approaches to security assessment and management, including such aspects as supply-chain security.

The framework and methods reviewed in this chapter could serve as a roadmap for academics, practitioners and other maritime interests to formulate risk assessment and management standards and procedures in line with the new security threats. Equally, further research can build on this to investigate the mechanisms and implications of security measures on port and shipping operations, including such aspects as the cost and economic impacts on operational and supply chain efficiency.

REFERENCES

Accorsi, R., Apostolakis, G. and Zio, E., 1999, "Prioritising stakeholder concerns in environmental risk management", *Journal of Risk Research*, 2(1), 11–29.

Angeloudis, P., Bichou, K., Bell, M.G.H. and Fisk, D., "Security and reliability of the liner container-shipping network: analysis of robustness using a complex network framework", forthcoming.

Babione, R., Kim, C.K., Rhone, E. and Sanjaya, E., 2003, *Post 9/11 Security Cost Impact on Port of Seattle Import/Export Container Traffic*, University of Washington: GTTL 502 Spring Session 2003.

Bedford, T. and Cooke, R., 2001, *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press: Cambridge.

Bell, M.G.H., 2006, "Mixed route strategies for the risk-averse shipment of hazardous materials", *Networks and Spatial Economics*, forthcoming.

Bichou, K., 2004, "The ISPS code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management", *Maritime Economics and Logistics*, 6(4), 322–348.

Bichou, K., 2005, *Maritime Security: Framework, Methods and Applications.* Report to UNCTAD, Geneva: UNCTAD, June 2005.

Bichou, K. and Gray, R., 2005, "A critical review of conventional terminology for classifying seaports", *Transportation Research A*, 39, 75–92.

Bier, V.M., 1993, "Statistical methods for the use of accident precursor data in estimating the frequency of rare events", *Reliability Engineering and System Safety*, 42, 267–280.

Bird, F.E. and Germain, G.L., 1996, *Practical Loss Control Leadership*, Det Norske Veritas: Alberta.

Bureau d'Enquêtes et d'Analyse pour la Sécurité de l'Aviation Civile (BEA), 2002, *Rapport sur l'Accident de Air France Concorde F-BTSC ayant lieu le 25*

Juillet 2000 à la Platte d'Oie, Paris: Ministère de l'Equipement, du Transport et du Logement.

Bureau of Transportation Statistics (BTS), 2002, Project 6 Overview: Develop Better Data on Accident Precursors or Leading Indicators, In: *Safety Numbers Conference Compendium*, Washington DC: BTS.

Cullen, W.D., 2000, *The Ladbroke Grove Rail Inquiry*, Norwich: Her Majesty's Stationary Office.

Damas, P., "Supply chains at war", *American Shipper*, November 2001, 17–18.

Darren, P., 2004, "Smart and safe borders: the logistics of inbound cargo security", *The International Journal of Logistics Management*, (15)2, 65–75.

De Kay *et al.*, 2002, "Risk-based decision analysis in support of precautionary policies", *Journal of Risk Research*, 5 (4), 391–417.

Erkut, E. and Ingolfsson, A., 2000, "Catastrophe avoidance models for hazardous materials route planning", *Transportation Science*, 43(2), 165–179.

Flynn, S., 2004, *America the Vulnerable: How our Government is Failing to Protect Us from Terrorism*, Harper-Collins Publishing: New York.

Grencser, M., Weinberg, J. and Vincent D., 2003, *Port Security War Game: Implications for US Supply Chains*, Booz Allen, Hamilton.

Guasch, J.L., 2000, *New Port Policies in Latin America and Caribbean*, New Press: Cambridge, MA.

Helferich, O.K. and Cook, R.L., 2002, *Location and Networks: Theory and Algorithms*, MIT Press: Cambridge, MA.

International Maritime Bureau On-line *http://www.icc-ccs.org*.

Joseph, G.W. and Courtier, G.W., 1993, "Essential management to support effective disaster planning", *International Journal of Information Management*, 13(5), 315–325.

Juttner, U., Peck, U.H. and Christopher, M., 2003, "Supply Chain Risk Management: Outlining an Agenda for Future Research", *International Journal of Logistics: Research and Applications*, 6(4), 197–210.

Lake, E.J., Robinson, W.L. and Seghetti, L.M., 2004, *Border and Transportation Security: The Complexity of the Challenge*, Washington DC: CRS Report RL23839.

MIT/CTS Interim Report, 2003, *Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains*. Also available on-line at: *http://web.mit.edu/scresponse/repository/SC_Resp_Report_Interim_Final_8803.pdf*.

OECD, 2003, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee Report, Paris: OECD.

OECD, 2004, *Report on Container Transport Security across Modes*, Report by the OECD Transport Section, Paris: OECD.

Phimister, J.A., Bier, V.M. and Kunreuther, H.C. (eds) 2004, *Accident Precursor Analysis and Management: Reducing Technological Risk through Diligence*, National Academy of Engineering, Washington DC: The National Academies Press.

Russell, D.M. and Saldana J.P., 2003, “Five tenets of security-aware logistics and supply chain operation”, *Transportation Journal*, 42, 4, 44–54.

Stavins, R.N. (ed.), *Economics of the Environment*, 4th edn, Norton & Co.: New York NY, pp. 378–393.

The Gore Commission, 1997, *Report to the White House on Aviation Safety and Security*, also available on-line *http://www.fas.org/irp/threat/212fin~1.html.*

The US Federal Register, 2003, *N-RAT Assessment Exercise*, 204(68), 60464–6046.

The US Nuclear Regulatory Commission (US NRC), 1978, Risk *Assessment Review Group Report*, NUREG/CR-400, NRC: Washington DC.

The World Bank Group, 2001, *Stakeholder Analysis*, also available on-line under social development/social assessment: *http://www.worldbank.org/social.*

UNCTAD, 2004, *Container Security: Major Initiatives and Related International Developments*, Report by the UNCTAD Secretariat, Geneva: UNCTAD.

Willis, H.H. and Ortiz, D., 2004, *Evaluating the Security of the Global Containerised Supply Chain*, RAND technical report series.

CHAPTER 17

ISPS CODE IMPLEMENTATION IN PORTS: COSTS AND RELATED FINANCING

Hassiba Benamara and Regina Asariotis

Trade Logistics Branch, UNCTAD, Geneva, Switzerland

Abstract

On 1 July 2004, amendments to the 1974 Convention for the Safety of Life at Sea (SOLAS), including the new International Ship and Port Facility Security Code (ISPS Code), entered into force and became mandatory for all SOLAS Member States. The new international maritime security regime imposes wide-ranging obligations on governments, shipping companies and port facilities. Implementing these obligations entails costs and may have economic implications. In order to obtain a better understanding of these potential economic implications, the UNCTAD Secretariat conducted a global study based on a set of questionnaires designed to obtain first-hand information from all parties affected by the ISPS Code. In this chapter, the results based on data received from the port sector regarding ISPS Code-related costs and financing are presented. The main findings are: (a) an assessment of unit costs and averages revealed important cost differentials between smaller and larger respondents, suggesting that economies of scale, type and structure of cargo traffic handled and the state of security prior to the ISPS Code may play a role; (b) based on the data provided, global port-related costs were estimated to range between ~US$1.1 billion and ~US$2.3 billion initially and ~US$0.4 billion and ~US$0.9 billion annually thereafter. These costs are equivalent to increases in international maritime freight payments of about 1% with respect to the initial expenditure and 0.5% with respect to the annual expenditure; (c) as to the cost factor distribution, the data suggests that, on average, expenditures on equipment absorb the largest share of the initial costs, whereas personnel and staff time represent the largest share of ISPS Code related annual costs; and (d) cost-recovery schemes are reasonably widespread and tend to target several port users, in particular cargo and containerized trade. In general less than full recovery of costs is expected. Ports that reported/receive funding are mainly located in developed regions, whereas ports in developing regions appear to receive mainly technical assistance and capacity building.

1 INTRODUCTION

An important development in the field of transport security was the entry into force, on 1 July 2004, of amendments to the International Convention for the Safety of Life at Sea (SOLAS) 1974 and the International Ship and Port Facility Security Code (ISPS Code) (see SOLAS/CONF.5/34, Annex I). The ISPS Code had been adopted in 2002 under the auspices of the International Maritime Organization (IMO), as part of a new Chapter XI-2 to SOLAS on "Special measures to enhance maritime security". The new international maritime security regime introduces wide-ranging obligations on SOLAS Contracting Governments, shipowning and/or operating companies and port facilities (for a better overview of these obligations, see UNCTAD, 2004: 30). Part (A) of the Code establishes a list of mandatory requirements, and Part (B) provides recommendations on how to fulfil each of the requirements set out in Part (A).

As concerns ports, it should be noted that the ISPS Code applies to port facilities serving ships engaged on international voyages. Therefore, any individual port may encompass more than one port facility to which the ISPS Code applies. Contracting Governments decide the extent to which the Code may be applied to port facilities within their territory, which are required, occasionally, to serve ships involved in international traffic. It should be noted that under the Code port facilities are defined as the ship/port interface. The wider issue of port security was dealt with as part of the further joint work between the IMO and the International Labour Organization (ILO) which resulted in the adoption of the IMO/ILO Code of Practice on Security in Ports.

Under the ISPS code, the main obligations in respect of port facilities include, among others, undertaking Port Facility Security Assessments (PFSA), developing Port Facility Security Plans (PFSP), designating Port Facility Security Officers (PFSO) and ensuring that training and drills take place regularly. The designated PFSO is responsible for developing, implementing and maintaining the PFSP. Other responsibilities and requirements include regular security inspections of the port facility, adequate training of port facility security personnel, reporting to the relevant authorities and ensuring that security equipment is properly operated, tested and maintained.

Clearly, implementing these obligations entails costs and may have economic implications. Although preliminary cost estimates were made prior to the coming into effect of the ISPS Code, these were based on broad modelling assumptions rather than on empirical data regarding actual costs incurred or expected (for an overview of other early estimates, see Asariotis, 2005). Given its entry into force on 1 July 2004 the ISPS Code lends itself to a cost assessment exercise, since affected parties must have taken necessary action to ensure compliance and may be expected to have gained clearer insight into the actual costs associated with the ISPS Code implementation. Although equally important, other transport security-related initiatives, including supply-chain security currently being developed or already adopted at the national and international levels, fall outside the scope of the present study.

Against this background, the UNCTAD secretariat conducted a global study based on a set of questionnaires, designed to obtain first-hand information from all parties affected by the ISPS Code, namely Contracting Governments, shipowning and/or operating companies and port facilities. The main objective was to establish the range and order of magnitude of the ISPS Code-related expenditures made from 2003 to 2005 and to provide insights into the financing mechanisms adopted or envisaged. In addition, the questionnaires sought to obtain information on views and experiences related to the implementation of the ISPS Code and any relevant supplementary measures, as well as other ISPS-related impacts.

A report entitled “Maritime Security: ISPS Code Implementation, Costs and Related Financing” and presenting the results of the survey in full, has been published by the UNCTAD Secretariat and is available electronically on its website at www.unctad.org (UNCTAD, 2007). This chapter is based on the report, but presents only the results relevant to ISPS Code-related costs and financing for the port sector.

Unless otherwise specified, percentages are expressed as a proportion of responses received to a given question. When questions can accommodate more than one response, percentages do not add up to 100%. Reference to averages means “unweighted” averages while “tonne” means a “metric ton” and includes all cargo. The expressions “costs” and ‘expenditures’ are used interchangeably. “Initial” or “one-off” costs refer to expenditures required to set up and implement the ISPS Code regime, while “annual”, “recurring” or “running” costs mean expenditures required to operate the security regime and to maintain compliance.

UNCTAD’s port questionnaire was widely distributed through port industry organizations. A total of 55 completed questionnaires were received from respondents (ports and organizations managing ports, hereinafter respondent ports) located in 28 countries. Almost all respondent ports (92%) are multipurpose facilities which handle various types of traffic including bulk, break-bulk, containers and passengers. The overwhelming majority of all respondent ports (91%) are publicly owned, but, irrespective of the ownership structure, the majority (55%) are operated by private entities.

A significant majority of all respondent ports (86%) provided information on their respective cargo throughput handled and number of ISPS port facilities. To categorize respondent ports by size, an existing tentative benchmark has been used (see Fourgeaud, 2000). Based on information obtained with respect to cargo throughput (measured in tonnes), there is an almost equal split between large (46%) and small respondent ports (43%), while average sized ones represent a smaller share (11%). According to this benchmark, a small port authority handles few million tonnes, an averaged sized authority handles between 10 and 20 million tonnes and larger ports handle over 20 million tonnes.

Respondent ports that provided information on their cargo throughput and number of ISPS port facilities cover about 800 ISPS port facilities or approximately 7% of the total number of the declared ISPS port facilities. Together these respondent ports handle about 16% of the global port cargo throughput (tonnes), based on 2004 world seaborne trade data, and approximately 24% of the global container port throughput (TEUs). (See UNCTAD’s Review of Maritime Transport, 2006.) However, input on costs and financing was not obtained from all respondent ports that provided information on cargo throughput. Relevant data on costs and financing, in a format suitable for analysis, and as reported here, was obtained from respondent ports which together handle about 13% of global port cargo throughput (tonne), estimated on the basis of world seaborne trade data for 2004.

2 SURVEY RESULTS REGARDING THE COST OF COMPLIANCE WITH THE ISPS CODE

The port industry was asked to estimate the direct initial "one-off" and the annual "recurring" expenditures required to comply with the requirements of the ISPS Code. The questionnaire also asked about the cost distribution among a list of cost items or factors.

2.1 Initial and Annual Costs

Expressed in absolute terms, the reported initial cost figures for respondent ports range between a low of US$3,000 and a high of US$35,500,000. As to the annual costs, reported figures vary between US$1,000 and US$19,000,000. The lower end of the cost range was reported by a small Asian port whereas the higher was reported by a large European port featuring among the top 15 global container ports.

In order to allow for some comparisons to be made and to put reported cost figures in perspective, unit costs and averages have been assessed on the basis of a number of reference points, after filtering out for extreme values. Reference points used include respondent ports' annual revenues, cargo throughput (tonnes and TEUs), ship calls and number of ISPS port facilities. The size of the respective samples used to estimate unit costs and averages varies, depending on the data provided in respect of each parameter. Size of respective samples is indicated, as appropriate, in relation to the relevant figures, as a percentage of global cargo port throughput (tonnes), based on world seaborne trade data for 2004 (UNCTAD, 2006).

Respondent ports in these samples have been divided into larger (upper half or top 50%) and smaller ports (bottom half). The dividing figure between larger and smaller respondent ports in the case of all cargo throughput is 15 million tonnes. With respect to respondent ports' container throughput, ship calls, annual revenues and number of ISPS port facilities, the cut-off points are, in the same order, 500,000 TEUs, 3,000 ship calls, US$45 million and 10 ISPS port facilities. It should be noted that, for the purposes of the average unit cost calculations, the breakdown between larger and smaller respondent ports is not comparable with that referred to in the introduction above.

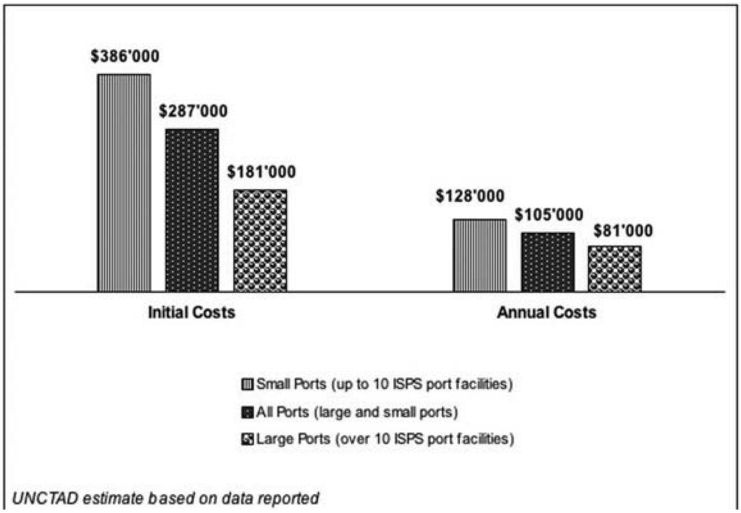
In those cases where initial costs are expressed in relation to annual performance data, reported initial costs have been annualized using the straight-line depreciation method. This method assumes that the value of an asset or capital investment drops in equal, constant yearly increments over the depreciation period. As responses received with respect to the structure of the initial costs suggest that, on average, over one-third of the initial costs are attributed to expenditures on equipment (see Figure 10), the average useful economic life of the ISPS Code-related initial investments or the average depreciation period is set to five years.

Expressing reported costs as a proportion of respondent ports' annual performance measures aims to provide an order of magnitude of the ISPS Code-related costs and to ascertain whether there are differences between "larger" and "smaller" respondent ports. Thus, the main objective is not to compare initial and annual costs or establish the exact depreciation period. Therefore, the selected depreciation period and resulting annualized initial costs are indicative only.

2.1.1 Average Costs per ISPS Port Facility

Figure 1 below highlights the unit cost differentials that prevail between respondent ports depending on the number of ISPS port facilities (with no further information available on the type of traffic handled). The relevant sample represents respondent ports handling about 7% of the global port cargo throughput (tonnes).

The average initial cost per ISPS port facility for smaller respondent ports amounts to US$386,000 which is more than double the cost for larger respondent ports (US$181,000). The average initial cost per facility for all respondent ports, irrespective of the number of the ISPS port facilities, amounts to US$287,000. As to the annual costs, the average cost per facility for smaller respondent ports continues to be higher (US$128,000) as compared with the cost of larger ones (US$81,000). The average annual cost per ISPS port facility for all respondent ports, irrespective of size, amounts to US$105,000.

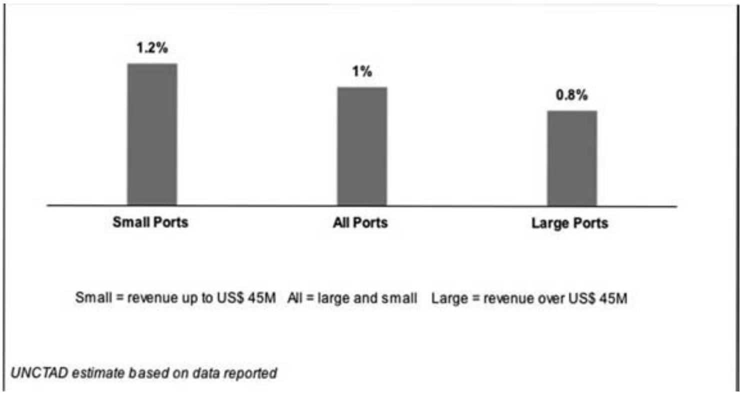


UNCTAD estimate based on data reported

Figure 1: ISPS Code-related Average Unit Costs (US$ per ISPS port facility)

2.1.2 Average Costs as a Percentage of Operating Revenues

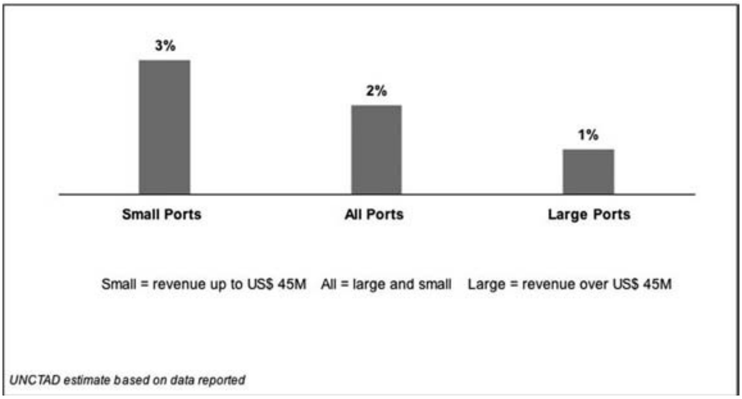
On average, the ISPS Code-related initial costs account for about 1% of respondent ports' annual revenues (Figure 2). A breakdown of respondent ports by size indicates that smaller respondent ports allocate a larger share of their operating revenues to financing the ISPS Code (1.2%) as compared with larger ones (0.8%). The relevant sample represents respondent ports handling about 8% of the global port cargo throughput (tonnes).



UNCTAD estimate based on data reported

Figure 2: ISPS Code-related Average Initial Unit Costs Over Five Years (% of ports' annual revenue)

On average, respondent ports allocate about 2% of their revenue to financing the ISPS Code-related annual expenditures (Figure 3). Smaller respondent ports allocate a larger share of their revenue (3%) to financing such costs as compared with larger ones (1%). The relevant sample represents respondent ports handling about 7% of the global port cargo throughput (tonnes).



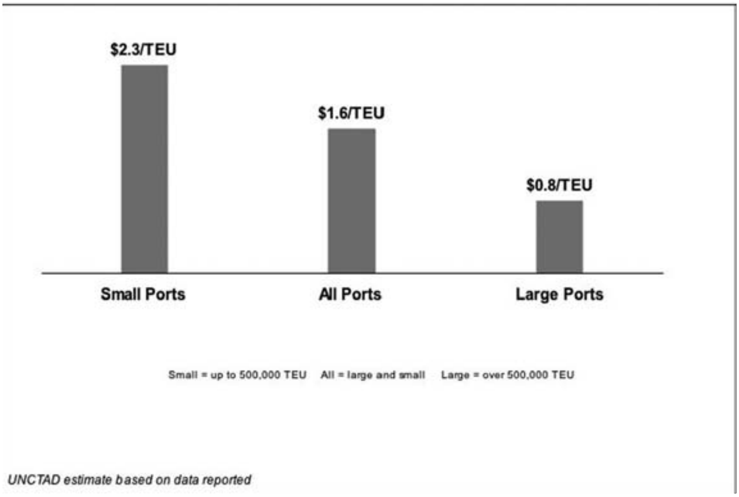
UNCTAD estimate based on data reported

Figure 3: ISPS Code-related Average Annual Unit Costs (% of ports' annual revenue)

The above results suggest that the financial impact of the ISPS Code is more pronounced in the case of smaller ports. Taking the analysis one stage further and accounting for other relevant parameters such as cargo throughput and ship calls, the following sections confirm the above findings and support the argument that costs seem to vary according to size.

2.1.3 Average Costs per TEU Handled

Taking into account the volume of container traffic handled and, with no assumptions made with respect to the distribution of such traffic between respondent ports, the average costs per TEU for respondent ports have been assessed (Figure 4). The average initial cost per TEU amounts to about US$1.6. The average cost for smaller respondent ports amounts to US$2.3 per TEU—about three times (US$0.8) the cost for larger ones. The relevant sample represents respondent ports handling about 10% of the global port cargo throughput (tonnes).



UNCTAD estimate based on data reported

Figure 4: ISPS Code-related Average Initial Unit Costs Over Five Years (US$ per TEU throughput)

A similar picture emerges when considering reported annual costs (Figure 5). The average annual cost per TEU handled amounts to US$2.5 for smaller respondent ports, while the cost for larger respondent ports amounts to US$1.6. On average, the annual cost per TEU for respondent ports, irrespective of size, amounts to US$2. The relevant sample represents respondent ports handling about 8% of the global port cargo throughput (tonnes).

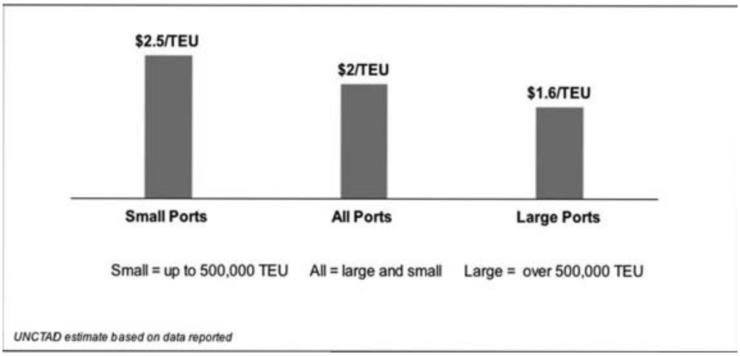


Figure 5: ISPS Code-related Average Annual Unit Costs (US$ per TEU throughput)

2.1.4 Average Costs per Tonne of all Cargo Handled

Using a different reference point—tonnes of cargo throughput—the average initial and annual unit costs have been assessed (Figure 6). The average initial cost per tonne for larger respondent ports amounts to approximately US$0.01, while that of smaller respondent ports is about US$0.05 or five times the average unit cost of larger respondent ports. The average initial cost for respondent ports, irrespective of size, amounts to US$0.03 per tonne. The relevant sample represents respondent ports handling about 9% of the global port cargo throughput (tonnes).

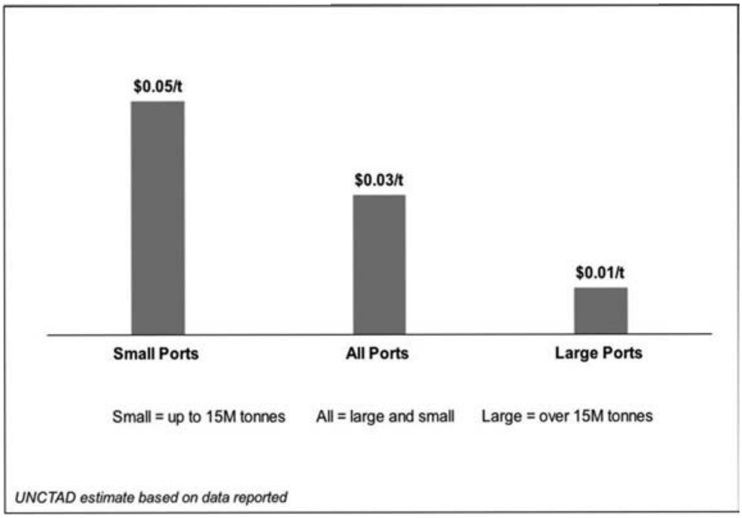
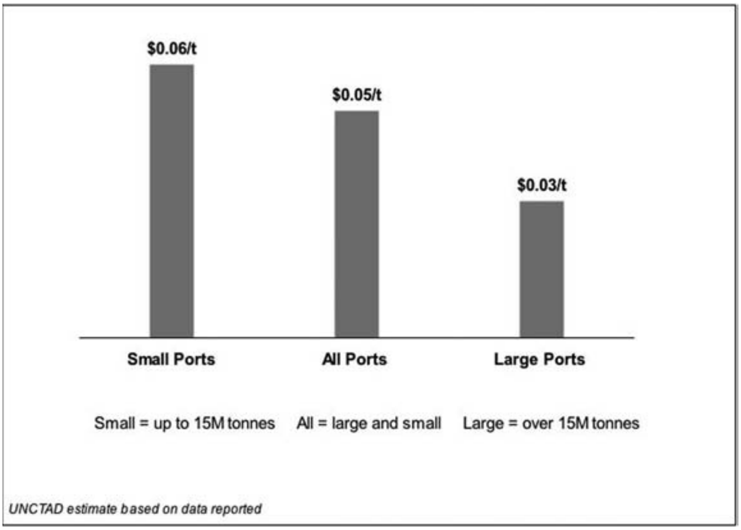


Figure 6: ISPS Code-related Average Initial Unit Costs Over Five Years (US$ per tonne of all cargo throughput)

This result is replicated when considering annual costs (Figure 7). The average cost per tonne for smaller respondent ports amounts to US$0.06 or double the average unit cost of larger respondent ports (US$0.03). The average annual cost per tonne of cargo handled amounts to US$0.05 for all respondent ports irrespective of size. The relevant sample represents respondent ports handling about 9% of the global port cargo throughput measured in tonnes.



UNCTAD estimate based on data reported

Figure 7: ISPS Code-related Average Annual Unit Costs (US$ per tonne of all cargo throughput)

2.1.5 Average Costs per Ship Call

Figure 8 presents the result of an assessment of average unit costs based on the reported number of annual ship calls with no further information available with respect to ship size, type or berthing time. The results indicate that smaller respondent ports have an initial cost per ship that is higher (US$113 per ship call) than the cost of larger respondent ports (US$72 per ship call). The average cost for respondent ports, irrespective of the number of ship calls per year, amounts to US$93 per ship call. The relevant sample represents respondent ports handling about 13% of the global port cargo throughput (tonnes).

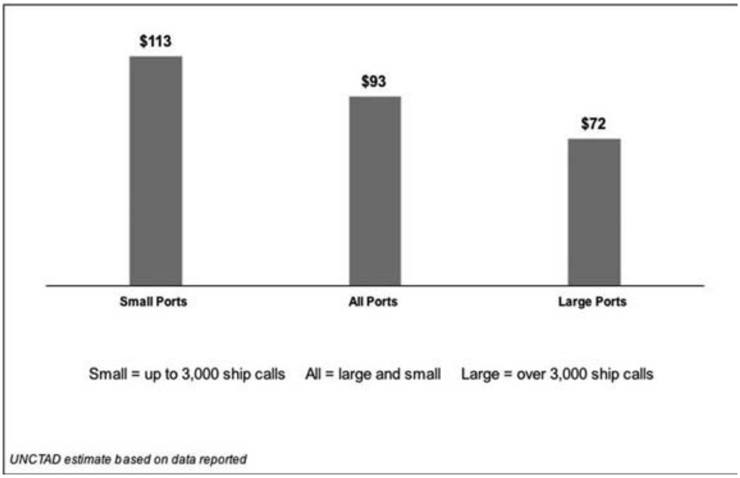


Figure 8: ISPS Code-related Average Initial Unit Costs Over Five Years (US$ per ship call)

The average annual unit cost continues to be larger for smaller respondent ports (Figure 9) and amounts to US$244 per ship. The average cost per ship call for larger respondent ports and for all respondent ports, irrespective of size, amounts to US$132 and US$190, respectively. The relevant sample represents respondent ports handling about 9% of the global port cargo throughput (tonnes).

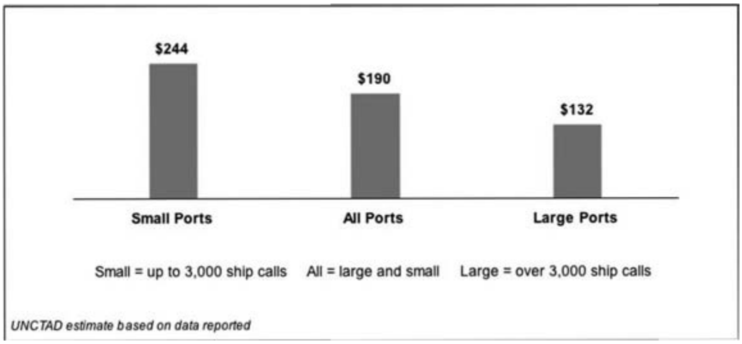


Figure 9: ISPS Code-related Average Annual Unit Costs (US$ per ship call)

2.1.6 Summary and Discussion

Table 1 below summarizes the estimated average costs and highlights the cost differentials between larger and smaller respondent ports. Smaller ports represent the bottom 50% of respondent ports, while larger ports represent the top 50%. Except for the average costs per ISPS port facility, average initial costs are annualized throughout a five-year depreciation period.

Clearly, smaller respondent ports have higher average costs as compared with larger respondent ports. Economies of scale, the type and structure of cargo traffic handled and prevailing security environment prior to the implementation of the ISPS Code may play an important role in this respect.

	As % of annual revenue		*Per tonne of cargo throughput*		*Per TEU throughput*		*Per ISPS port facility*		*Per ship call*	
	Larger >$45 million	Smaller	Larger >15 million	Smaller	Larger >500,000	Smaller	Larger >10 facilities	Smaller	Larger >3,000 calls	Smaller
Initial	0.8%	1.2%	$0.01	$0.05	$0.8	$2.3	$181,000	$386,000	$72	$113
Annual	1%	3%	$0.03	$0.06	$1.6	$2.5	$81,000	$128,000	$132	$244

Table 1: ISPS Code-related Average Costs of Relevant Respondent Ports

Economies of Scale and Structure of Traffic

The fixed costs element, together with an insufficient level of throughput necessary to spread the costs, may explain the higher costs of smaller respondent ports. The effect of economies of scale is illustrated in Table 2 below, which presents annual cost figures reported by two European respondent ports. Clearly, higher cargo volumes result in lower unit costs despite larger total reported annual costs. In addition, the type of cargo handled may have a bearing on costs since bulk trades, for example, may require fewer security-related investments and hence result in lower costs.

	Annual costs	*Annual cargo throughput (tonnes)*	*Unit cost (US $)*
Port 1	296,000	1,400,000	$0.21
Port 2	19,000,000	152,000,000	$0.13

Table 2: Effect of Economies of Scale (example)

Security Environment Pre-ISPS Code

The state of the security set-up prior to the application of the ISPS Code could also help explain the divide between larger and smaller respondent ports. The latter may have a wider gap to bridge in terms of security in contrast to larger respondent ports that have probably in the past invested more in securing the premises and access to the relevant facilities. Depending on their specific activities and type of traffic handled, some types of facilities such as major transit areas have probably already acquired equipment and implemented measures which can be used for security purposes, although initially intended to respond to existing safety requirements or to counter theft.

2.2 Cost Factor Distribution

As to the manner in which costs are distributed among various cost headings (Figure 10), responses received suggest that, on average, expenditures on equipment absorb the largest share of the *initial* costs (35%) followed by expenditures on infrastructure (26%). Other cost factors include expenditures related to personnel and staff time requirements (14%), training, drills and exercises (8%), ICT use (7%), administrative (6%), operations and procedures (2%) and upgrades of security to levels 2 and 3 (2%).

With respect to security upgrades, it should be noted that under the ISPS Code, Contracting Governments are responsible for setting the security levels. Security level 2 refers to the level at which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of security incident. Security level 3 means the level at which further specific protective measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

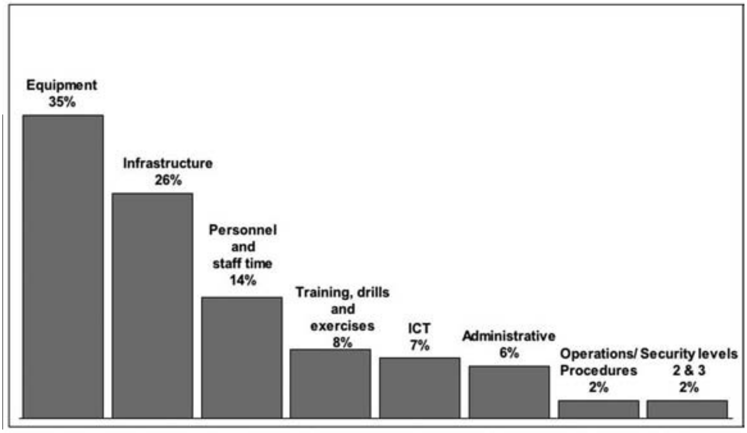


Figure 10: ISPS Code-related Initial Costs of Respondent Ports: Cost Factor Distribution

As concerns *annual* ISPS Code-related costs (Figure 11), responses received suggest that, on average, expenditures on personnel and staff time (47%) represent by far the largest share of the ISPS Code-related costs followed by expenditures on training, drills and exercises (13%) and equipment (11%). Expenditures associated with administrative functions and ICT-related requirements amount respectively to about 10% and 8% of these costs. Infrastructure-related expenses absorb a smaller portion of the costs (6%)

followed by expenditures associated with operational requirements (3%) and security upgrades to levels 2 and 3 (2%).

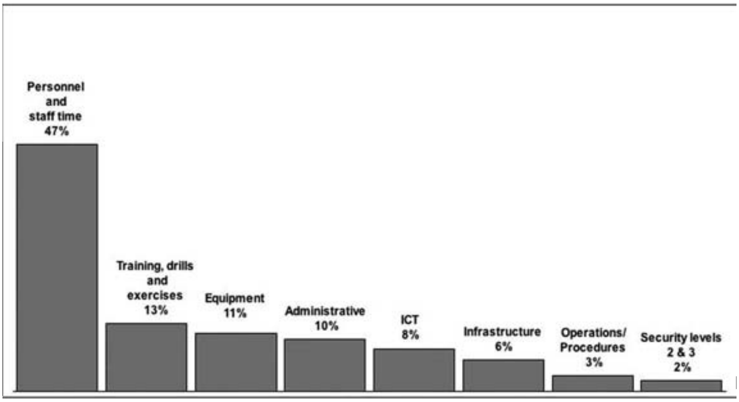


Figure 11: ISPS Code-related Annual Costs of Respondent Ports: Cost Factor Distribution

2.3 Estimated Global Costs

In order to obtain a better understanding of overall cost implications of the ISPS Code, global initial and annual costs have also been estimated using cost data reported and three reference points, namely respondent ports' share of (a) world seaborne trade measured in tonnes, (b) global container port throughput and (c) total number of declared ISPS port facilities. The share of respondent ports of world seaborne trade (tonnes) is estimated to ~13%, while their share of global container port throughput and total number of declared ISPS port facilities is estimated to ~16% and ~6%, respectively. These shares are established based on 2004 data on global container port throughput and seaborne trade reported in UNCTAD's *Review of Maritime Transport*, 2006, as well as the total number of 10,652 declared ISPS port facilities reported by the IMO Secretariat as of October 2006.

Table 3 below summarizes the estimated port-related global costs of ISPS Code implementation. Bearing in mind the limitations that may characterize such calculations, the estimated global ISPS Code-related costs range between approximately US$1.1 billion and US$2.3 billion initially and between US$0.4 billion and US$0.9 billion annually thereafter.

	Initial (billion US$)	*Annual (billion US$)*
ISPS port facilities	2.3	0.9
Tonnes	1.3	0.4
TEU	1.1	0.4

Table 3: Estimated Global Initial and Annual Costs (billion US$)

To put these results in perspective, the above estimates are assessed against the 2004 global estimated international maritime freight costs (UNCTAD 2006: 73). The estimated global initial costs range from about 0.6% to 1.3% of the global international maritime freight costs, while the estimated global annual costs range between 0.2% and 0.5%. Thus, the estimated global port-related costs associated with the ISPS Code are equivalent to increases in international maritime freight payments of about 1% with respect to the initial expenditure and 0.5% with respect to the annual expenditure.

It should be borne in mind that these estimated global costs are based on reported data relating to the implementation of the ISPS Code only and do not reflect (a) the costs associated with other security measures and initiatives which may require additional investments and expenditures, or (b) indirect costs which may arise, for instance, in the context of security-related delay or congestion.

3 SURVEY RESULTS RELATING TO THE FINANCING OF ISPS CODE-RELATED COSTS

3.1 Market-driven Solutions: Cost Recovery by Charging Port Users

The questionnaire asked about the sources used by ports to finance their initial and annual recurring expenditures and whether they had introduced or envisaged implementing any cost-recovery schemes. In addition, respondent ports were asked to identify the party responsible for implementing the resulting pricing strategy and to clarify the basis for the levies or the charges applied or planned. Finally, the questionnaire inquired about the proportion of the total initial and annual expenditures expected to be recovered by way of the cost-recovery schemes.

The majority of respondent ports have no cost-recovery schemes in place. Only 37%—mainly from developed regions—have indicated the presence of or the intention to introduce cost-recovery schemes. Others (6%) indicated that they had introduced or planned to introduce cost-recovery schemes in addition to receiving public funding. The limited use of cost-recovery schemes by respondent ports located in developing regions suggests that charging port users might be more difficult for ports in some regions. It might also be the case that some port and terminal operators are bound by the terms of the leasing contract or concession agreement.

As Figure 12 shows, recovery schemes adopted or envisaged by respondent ports include fees or charges applied to cargo (48%) and passengers (17%). Others involve imposing security charges on the basis of ship calls, tariffs or dues (35%) or increasing facility rent (9%). Clearly, respondent ports appear to favour an approach that targets several users, with a preference for cargo, especially containerized trade. Approaches to cargo-based recovery schemes vary with relevant respondent ports indicating that charges were levied on a variety of cargo movements. Based on information provided by respondent ports, charges appear to be levied on either: (1) imported, exported and transhipped full and empty containers as well as imported, exported and transhipped tonnes of cargo; (2) imported, exported and transhipped full containers; (3) imported and exported full containers; (4) imported and exported tonnes of cargo; (5) imported full containers; or (6) imported and exported empty containers as well as imported and exported tonnes of cargo. There are no reports about cost-recovery schemes that apply to transhipments only.

It is interesting to note that cargo throughput measured in tonnes and TEUs is positively correlated with the reported costs. The estimated coefficients of correlation between reported annual costs on the one hand, and tonnes and TEU throughput on the other, amount to 0.59 and 0.53, respectively. This might partly explain the reasoning behind cargo-based recovery schemes, especially in containerized trade. The corresponding coefficients correlating annual costs with ship calls, annual revenues and ISPS port facilities amount to 0.26, 0.54 and 0.81, respectively. Statistical analysis of the relationship between costs and various measures of port sizes including tonnes, TEU, ship calls, passengers and ISPS port facilities could contribute to informing the debate on the criteria to be used when designing ports' cost-recovery schemes with a view to internalizing costs.

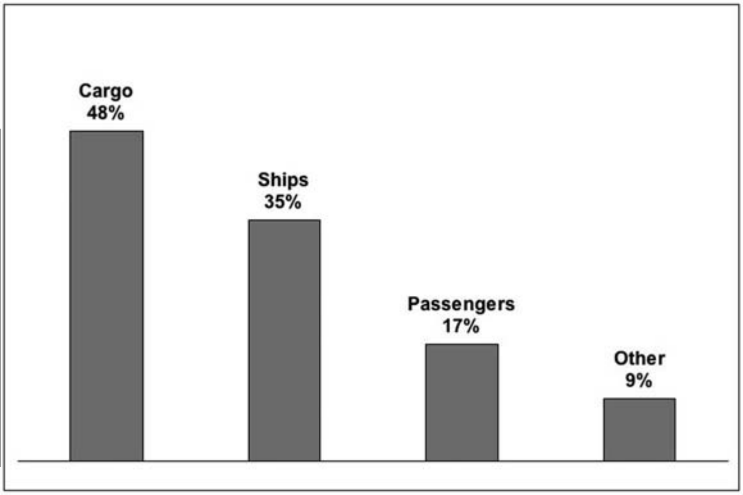


Figure 12: ISPS Code-related Cost-Recovery Schemes as Reported by Respondent Ports

The majority of respondent ports (61%) indicated that they did not expect to recover directly from users more than half of their ISPS Code-related initial costs. The remaining respondent ports (31%) expect to recover over 50% and up to 80% of their costs and only few (8%) anticipate full or almost full recovery. As to the annual costs, the majority (54%) expect to recover more than half of their costs, but not necessarily the full amount. An important minority (46%), however, does not expect to recover more than 50% of their annual costs.

These results suggest that, although higher with respect to annual costs, the expected recovery rate is, in most cases, no more than 50%. It is not clear, however, irrespective of the expected recovery levels, how recovered amounts will be distributed among the various port stakeholders.

A fundamental issue arising in relation to cost-recovery schemes is whether levies charged in ports are proportionate to the cost of security and are based on clear objective grounds. According to press reports, the maritime industry and its users, whether shipping lines or shippers, argue that the manner in which security charges are being set requires further transparency; also that, substantiation is required that these charges are commensurate to services rendered and expenditures incurred as a result of the enhanced maritime security (for an overview, see Asariotis, 2005). One respondent port commented that " . . . Ship and cargo owners believe costs should be absorbed by ports and have put up a strong resistance to contributing".

Only a few respondent ports indicated the amounts of security charges applied; these are consistent with the level of security fees published in some industry reports and compilations. Selected security surcharges as published elsewhere (for example, by Hapag-Lloyd (www.hapag-lloyd.com) and the American Association of Port Authorities (AAPA at www.aapa.ports.org)) are presented in Table 4 below, together with the estimated average costs per cargo throughput derived on the basis of responses received to UNCTAD's questionnaire. The examples below of security fees per tonne relate to the Florida Ports Conference and the Gulf Seaports Marine Terminal Conference. These rates are minimum fees which member ports may increase if justifiable. The average container security fees are calculated on the basis of the compilation of container terminal security charges published by Hapag-Lloyd.

A comparison between the estimated unit costs and the security surcharges levied by ports should, however, be handled with care since the criteria used to set the level of security fees remains unclear and levied amounts might aim to recover expenditures resulting from security measures other than the ISPS Code.

Unit costs	*Respondent ports*			*Published security charges*	
	All	Larger	Smaller	Levy per tonne	
Initial cost per tonne	US$0.03	US$0.01	US$0.05	Liquid bulk	US$0.02
				Dry bulk	US$0.02
Annual cost per tonne	US$0.05	US$0.03	US$0.06	Breakbulk	US$0.10
Initial cost per TEU	US$1.6	US$0.8	US$2.3	Average container security fee/ container:	
Annual cost per TEU	US$2.0	US$1.6	US$2.5	Australia (5 ports)	~US$4
				Brazil (3 ports)	~US$9
				Canada (2 ports)	~US$2.8
				China (2 ports)	~US$2.6
				Europe (42 ports)	~US$9
				Hong Kong	~US$2.6
				New Zealand	~US$13.5
				USA (14 ports)	~US$3.8

Table 4: ISPS Code-related Unit Costs and Selected Security Charges

3.2 Public Intervention: Funding and Assistance

To gain further insight into the manner in which the port industry managed to finance ISPS Code-related expenditures, the questionnaire asked whether public funding had been received or was expected. Additional questions sought to clarify the sources, the types and the amount of these funds.

A minority of respondent ports (26%), mainly from developed countries and none from Africa and Oceania, indicated that they had received or expected to receive public funding. Another share of respondent ports (6%) indicated that they had not only received or expected to receive public funding, but had also implemented or envisaged introducing cost-recovery schemes.

All respondent ports that have received or expect to receive financial assistance appear to be publicly owned. Grants constitute the main form of assistance, followed by governmental cost-sharing agreements, interest free loans, subsidies and tax credits. In terms of sources of funding, for a significant majority of relevant respondent ports (82%), the local or national government remains the main source of funding. Other sources include inter-country funding and regional organizations. Other types of assistance received or expected include technical assistance and capacity building provided by international organizations, such as the IMO, to some respondent ports located in developing regions.

3.3 Summary

The overall picture that emerges is one whereby not all respondent ports have financing schemes (i.e. cost recovery and/or public funding and assistance) to offset the ISPS-Code related costs (Figure 13). Those that do, have either implemented cost-recovery schemes by charging port users (37%), benefited from public funding and assistance (26%), or relied on both (6%). An important minority (31%) have no existing or planned financing schemes. Clearly, the port industry appears to rely on various approaches to financing its ISPS Code-related costs. These range from cases where costs are financed in full by ports with no cost-recovery schemes and funding in place, to instances where ports, governments and port users together share the costs of the new port security regime.

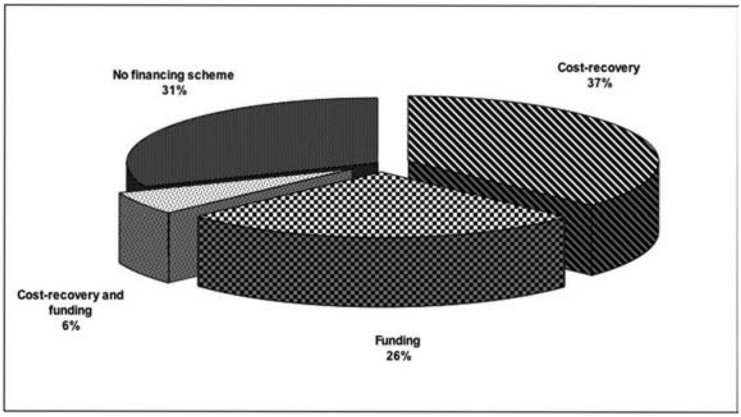


Figure 13: ISPS Code-related Financing Schemes as Indicated by Respondent Ports

4 SUMMARY OF KEY FINDINGS REGARDING COSTS AND FINANCING

An overall satisfactory representation of ports' perspective is achieved given the good response rate and the sizeable share of the global port cargo throughput handled by respondent ports. It should be noted that respondent ports from developed regions constitute the majority in terms of number of responses received and share of the overall cargo throughput (tonnes) reported. That being said, the views and experiences of respondent ports from developing countries are also reflected. The limited number of responses from ports that handle one single type of traffic did not allow for any conclusions to be drawn with respect to potential differences to the position of multipurpose ports.

The figures reported in absolute numerical terms and the estimated average costs highlight important cost differentials between respondent ports. Costs differ from port to port and from facility to facility depending on a variety of factors, in particular size. The ratio of costs to annual revenue, cargo throughput, ISPS port facilities and ship calls is significantly lower for larger respondent ports as compared with smaller ones.

Responses received, depending on the reference point adopted, suggest an annualized average initial cost burden for relevant respondent ports equal to around: 1% of the annual revenue; US$0.03 per tonne of cargo; US$1.6 per TEU and US$93 per ship call. Initial average costs per ISPS port facility amount to US$287,000. The average annual cost burden for relevant respondent ports amounts to approximately 2% of the annual revenue; US$0.05 per tonne of cargo; US$2 per TEU; US$190 per ship call and US$105,000 per ISPS port facility.

Estimated global port-related costs range between approximately US$1.1 billion and US$2.3 billion for the initial implementation and between US$0.4 billion and US$0.9 billion for the annual maintenance and operation of the security regime. Expressed as a proportion of international maritime freight costs, estimated global port-related costs of the ISPS Code are equivalent to increases in international maritime freight payments of about 1% with respect to the initial expenditure and 0.5% with respect to the annual expenditure.

Responses received suggest that the initial implementation of the ISPS Code requires more investments in equipment and infrastructure to put in place the conditions necessary to comply with the new security obligations. Personnel and staff time requirements generate most of the costs associated with the annual maintenance of compliance with the ISPS Code. Maintaining and operating the new security regime would normally require hiring more personnel or extended working hours for existing staff. Other important cost factors, yet of lesser magnitude than personnel and staff time, are training, drills and exercises, equipment, administrative and ICT-related expenses. The ISPS Code requires that regular training and drills be conducted and hence, the importance of the associated costs is not surprising. Costs driven by operational and procedural requirements or by security upgrades appear to continue to be negligible in proportion to the remaining cost items.

To finance these costs, a significant proportion of respondent ports resort to market-driven solutions whereby security surcharges, are levied directly on port users. Such cost-recovery schemes are reasonably widespread. Cargo, especially containerized traffic and including various movements (imports, exports, transhipments as well as empties) seems to be the most common basis for the application of security surcharges, although other users (ships, port operators, passengers) are, to some extent, also affected. These cost-recovery schemes, however, do not necessarily result in full recovery since the majority of respondent ports expect to recover no more than half of their respective initial costs. As to their annual costs, a majority expect to recover more than half of their costs, with only a minority expecting to achieve full recovery.

The results of the survey did not provide much insight with respect to the basis upon which applicable cost-recovery schemes are devised, including the relevant levels of surcharges. It also remains unclear how revenues generated are being allocated. Thus, achieving greater transparency with respect to criteria used to set security charges remains a challenge.

A minority of respondent ports have received or expect to receive public funding and assistance. These are mainly located in developed regions and assistance received or expected includes governmental grants and cost-sharing agreements as well as technical assistance and capacity-building. Technical assistance and capacity-building initiatives are mainly deployed by international organizations such as the IMO and directed to respondent ports located in developing countries. Few respondent ports have implemented or envisage introducing cost-recovery schemes as well as benefiting from public funding.

An important minority financed the ISPS Code-related costs entirely from their general revenue funds since no cost-recovery schemes and no public funding were in place or expected.

The cost levels and associated implications of the ISPS Code and the call, by some respondent ports, for assistance highlight the need to address the challenges posed by the ISPS Code implementation and to capitalize on the potential associated benefits. In this respect, responses received reiterate the message that emerged from a recent survey of the port industry by the International Association of Ports and Harbours (IAPH). A number of IAPH members called for technical and financial assistance or support including for personnel training and installation of advanced security equipment and drew special attention to the particular needs of ports in developing countries (IAPH, 2006).

It should be stressed that the above results, while insightful, reflect the experiences of ports in relation to the implementation of the ISPS Code only, and thus provide a limited basis for any assessment of the wider potential economic implications of transport security measures. The potential impact of other far-reaching unilateral and multilateral security initiatives and programmes was beyond the scope of the study, as was the assessment of potential indirect security-related costs such as those arising from delays and congestion. It is hoped that the results of UNCTAD's global survey will help further the debate on maritime transport security and its potential economic implications, especially for developing countries. However, further research in this field may be required.

REFERENCES

Asariotis, R., 2005, "Implementation of the ISPS Code: an overview of recent developments", *Journal of International Maritime Law*, July–August 2005, 266–287.

Fourgeaud, P., 2000, *Measuring Port Performance*, World Bank.

International Association of Ports and Harbours (IAPH), 2006, *IAPH surveys on ISPS Code Implementation*, IAPH Report of 10 October 2006, IAPH: Japan.

UNCTAD, 2004, *Container Security: Major Initiatives and Related International Developments*, Geneva: UNCTAD (UNCTAD/SDTE/TLB/2004/1).

UNCTAD, 2006, *Review of Maritime Transport*, Geneva: UNCTAD.

UNCTAD, 2007, *Maritime Security: ISPS Code Implementation, Costs and Related Financing*, Geneva: UNCTAD (UNCTAD/SDTE/TLB2007/1).

This page intentionally left blank

CHAPTER 18

ENHANCING PORT SECURITY VIA THE ENACTMENT OF EU POLICIES

Athanasios A. Pallis and George K. Vaggelas

Department of Shipping, Trade and Transport, University of the Aegean, Greece

Abstract

International regulatory initiatives aiming to minimize risk and increase the security and operational reliability of the port sector are increasingly complementing policies promoting the competitiveness of ports and their integration in supply chains. Part of this global trend is the European Union (EU) move to bring into force a number of laws, regulations and administrative provisions for enhancing port security. A long-term EU strategy with a reference to all parts of the supply chain and a specific policy on maritime infrastructure protection is under preparation. Whilst the aim of these EU policies is to introduce security standards for (trans)port service providers and the "secure operator" concept, they also affect Europe's ports in several economic and operational ways. This chapter analyses the implications of the enactment of these policy measures for European ports. The following are some of the issues discussed in order to enhance security by the enactment of these policies by the EU while maintaining a balanced level playing field: (a) the resulting task division among port authorities, other relevant authorities and stakeholders; (b) the cost implications of these measures for the various actors; (c) the search for a balance between risk and regulatory policies; and (d) the emerging financial issues. Finally, this chapter discusses the major controversies between policymakers and stakeholders as regards the introduction of further supranational security related policies.

1 INTRODUCTION

Throughout the last two decades, the focus of port policies in Europe has been on restructuring the port industry and reinforcing the quality of provided services (i.e. by integrating ports in supply chains). Since 2001 these efforts have been accompanied by the search for a collective public policy regime that would ensure secure port operations for all international European ports.

Transport security has become a vital issue worldwide and a new scene has revealed: security, not only of ports but of the whole supply chain, has been transformed into a key theme of public port policies. Security-related regulations have been introduced at three levels: national level, for example, the USA; peripheral/supranational, for example, the EU; and international level, for example, the International Maritime Organization (IMO). The majority of them mostly pay attention to container trade and include measures for protecting containers, ships and ports. The ultimate purpose of these policies is to minimize the security risk thus preventing unlawful acts that may occur throughout the transportation chain.

Maritime security is defined as the resistance to an intentional, unauthorized act designed to cause harm or damage to ships and ports. This definition can also be extended and applied to the entire supply chain. A broad, yet major, distinction between safety and security is that security has a reference to the protection from intentional acts, while safety has a reference to the protection from accidental events.

Security risk in transport equates to the combination of two factors. The first factor is the vulnerability of the system, which reflects the possibility of a successfully undertaken unlawful act against the transport network compared to the possibility of protecting it through inherent or managed safeguards. The second factor is the consequences of such a successfully undertaken unlawful act. These consequences are related to two measurable magnitudes: the possible number of fatalities and the economic impact of these acts, respectively. The latter is calculated in relation to three variables: the reconstruction costs; the disruption time of the transport flow; and the volume of transport flow.

The introduction of security measures in the international transportation process has greatly influenced the competitiveness of modes and supply chains. In combination with factors such as cost, time, safety and risk, security has become a factor affecting the competitive position of all the supply-chain related stakeholders. Therefore, questions regarding which market actors should act in order to enhance the security of the system and how should they do so, as well as who should bear the cost of security implication, are vital.

At European level, following the events of 9/11, the European Union (EU) policy-making institutions advocated a port security "policy gap" and moved decisively towards developing regulatory and non-regulatory initiatives aimed at minimizing risk and increasing the security and operational reliability of the sector.

Some EU policy initiatives have already been transformed into EU laws, obliging Member States to bring into force national laws, regulations and administrative provisions. Other proposals, like the draft regulation on supply-chain security, are still under discussion. A long-term strategy with a reference to all parts of the supply chain was put forward by the European Commission in the form of a Green Paper on a European programme for critical infrastructure protection (CEU, 2005a) and is currently under consideration by policymakers and stakeholders. A specific policy on maritime infrastructure protection is under preparation. Whilst the aim of all these policies is to introduce security standards for (trans)port service providers and the secure operator concept, they also affect Europe's ports in several economic and operational ways.

This chapter presents the EU security-related initiatives affecting European ports and analyses the implications of their enactment. It also discusses the major controversies as regards the introduction of further supranational policies. Some of the other issues examined in an effort to enhance security while maintaining a balanced level playing field for all EU ports include: (a) the resulting task division among port authorities, other relevant authorities and stakeholders; (b) the cost implications of these measures for the various actors; (c) the search for a balance between risk and regulatory policies; and (d) the emerging financial issues. Section 2 investigates the rationale behind the recent transformation of security into a primary issue in transport-related public policies, while section 3 focuses on the main international and national mandatory or voluntary security regulations and initiatives that are closely related with the content of the relevant EU policy initiatives. The relevant EU policies are analysed in section 4, which concludes with the presentation of the perspective of the various stakeholders on the implications of the existing and under-discussion relevant policies. Section 5 closely looks at the costs and the benefits of the security-related EU rules. The concluding section has a reference to the potential future policy directions.

2 (TRANS)PORT SECURITY AS A MAJOR PUBLIC POLICY ISSUE

A few years ago the enhancement of port and supply-chain security was not a major policy issue. Nor was it treated as a necessary factor to be tackled by the companies involved in trade and transport. Security-related disruptions in maritime transport were rare and security focus, if any, was restricted to piracy and armed robbery. Nowadays, security is a global issue affecting the entire transport sector. Acting internationally, public agencies introduced a number of regulatory and non-regulatory measures in order to enhance it.

Three are the driving forces inducing the reversal of the trend towards international decision-making and the way in which security is treated. The first one is the increased frequency of unlawful acts that took place at economic centres and/or transport nodes, disrupting transport processes, and foremost, threatening the lives of those involved in transportation. The second driving force is the spatial dimension of security-related regulations. The limited spatial jurisdiction of national policies hampered their potential to turn to a holistic approach of tackling security issues in transport and global trade systems. The third driving force concerns the structural changes of the world economy and the implementation of advanced technologies, which altered the way transport systems in general, and ports in particular, operate. Focusing on the EU this list of parameters should also include the economic importance of the port sector for the European economy.

The 9/11 World Trade Centre, New York attacks in 2001, accelerated work on coherent security measures in maritime transport at international level. Before that, the common practice had been for each country (EU Member State, or not) to develop its own rules aiming to discourage such attacks.

International organizations occasionally adopted security guidelines. This pattern had developed despite the fact that national security regulations, whenever existing, encountered several implementation difficulties due to their spatial dimension; by concerning only specific transport processes, or even some specific infrastructures, their implementation did not cover all the potential targets of unlawful acts.

Notably, the European Commission addressed the issue of security in the White Paper drawing the themes of the EU Transport Policy up to 2010 (CEU, 2001), which was published just one day after the 9/11 attacks. However, this was a reference only to security of passengers on board cruise vessels and ferries, as well as security during the transportation of nuclear goods. The purpose of this reference was to cover only a limited part of maritime transport.

After the 9/11 attacks, security moved up on the political agenda. Fearing that ships could carry weapons of mass destruction or be used as weapons themselves, member governments of the International Maritime Organization (IMO) met in December 2002 to establish mandatory security standards for ships and ports. The increased frequency of maritime-related unlawful acts provided the incentive for national administrations and supranational organizations to pay more attention to security issues. Unlawful acts disrupting maritime transport activities and endangering lives onboard are not a new phenomenon. The taking hostage of passengers onboard the cruise ship *Aquile Lauro* (October 1985) is just an example. Unfortunately, however, since 2000 the frequency of such actions has increased. Maritime-related incidents, like the attacks on the battle cruiser USS *Cole* (October 2000) outside the harbour of Aden, and the oil tanker MV *Limburg* (October 2002), were not the only ones. Other transport modes were also affected, including the Madrid commuter trains (March 2004) and the London public transport system (July 2005), with these unlawful acts taking place in the aftermath of the September 2001 events.

All the above indicated the vulnerability of the different transport modes to unlawful acts. National governments and international organizations responded by a fast-track endorsement of policy initiatives, reflecting a changing geopolitical climate. As the Commissioner at the time responsible for transport (Loyola De Palacio) pointed out (CEU, 2003):

> “The current geopolitical climate requires an urgent and effective implementation in Europe of what has been agreed at world level to ensure highest possible levels of security for seamen, ships, ports and the whole intermodal transport chain.”

Progressively, the maritime security agenda expanded to include measures that minimize a number of security risk factors that are associated with cargoes (for example, the potential to be used as weapons), vessels (the potential to be used to disrupt infrastructure and/or as weapons), and people (the potential transportation of people attacking ships or infrastructure), and limit the potential of transport means and nodes from becoming potential targets (Johnston, 2004).

Meanwhile, ports were affected by major economic (i.e. globalization and liberalization of world markets), technological (i.e. containerization) and organizational (i.e. implementation of just-in-time and door-to-door processes) changes. Following the rapid and pervasive restructuring of supply chains and logistics pathways, modern ports are not simply places that facilitate the interface of sea and inland transport modes. Ports are areas of commercial, industrial and distribution activities (Barton and Turnbull, 2002), which are embedded in value-driven chain systems (Robinson, 2002). The expanding use of combined transport (*cf.* Slack, 1998) advanced this trend to an extent that was acknowledged by policy makers: EU institutions indicated the beginning of a new intermodal era for ports in the early search for a long-term EU port policy (see: CEU, 1997). At a latter stage, they endorsed public policies aiming to integrate ports in the multimodal transport chain (for details: Chlomoudis and Pallis, 2002).

These developments produced the expansion of port hinterlands and port "regionalization" (Notteboom and Rodrigue 2005): there is a geographical and functional integration of ports in wider regions in order to serve a specialized transportation context by using the comparative advantage of spatially effective fragmented locations (i.e. better access to space, markets, labour, parts and resources). The concept of within port localization, either for operational and/or cost minimization justifications, is downgraded. Complex transport flows and spatially fragmented operational networks operate as integrated systems, with a number of actors involved within the wider supply chain, operating on a wider geographical scale.

This integration of ports in supply chains has certain security implications. By expanding the spatial area within which transport operations take place and due to the fact that intermediate goods are processed at various stage of the transport chain (*cf.* Juhel, 1998), one needs to secure the entire "process" which begins at the manufacturing site, rather than the parts of the supply chain. In the case of Europe it involves more than 4 million operators and is generally marked by low levels of security awareness. The fact that these complex networks are mostly situated near urban areas, adds to the necessity of approaching security issues through holistic frameworks (i.e. addressing the security of the entire chain), rather than piecemeal ones (i.e. addressing security in a specific transport mode or location). At the same time, the implementation of security measures at ports is a difficult task given the different priorities of the various stakeholders and the emerging multiplicity of port organization and ownership statuses.

The economic importance of the port sector for the EU stands as an additional driving force for developing European-level policies aiming to address security concerns. A total of 3.5 billion tons of cargo (90% of the external EU trade and the 40% of the intra-EU trade) and 350 million passengers are annually transported via European ports. Ports are also significant as places of employment and as added-value generators. The EU has approximately 1,200 sea ports and 3,700 port facilities and including the services related to them, they produce an annual added-value of €20 billion and employ approximately 350,000 citizens.

3 DEVELOPMENTS INDUCED BY NON-EU SECURITY INITIATIVES

Given the geopolitical developments and the events that took place in 2001, the US has been the leading force in the introduction of a new maritime security regime. The latter has an international dimension that contributes to the presence of relevant policies outside the US. Although developed in a non-EU context, these port security initiatives have had a considerable impact on the observed upgrade of the EU interest in developing its own policies.

3.1 Developments in the US

Two of the major maritime transport-related security regulations with a global impact developed in the US and deal with container transportation. Their purpose is to enhance the effectiveness of inspections on cargoes transferred by containers in order to avoid imports of undesirable and dangerous for the national security, goods.

The Container Security Initiative (CSI), which has been in force since February 2003, is the first of these regulations. This initiative has established relevant inspections of containers at the foreign ports where imports are loaded for the US, rather then at the US port of discharge. The essence of this initiative broadens the US borders away from the actual ones, as well as the jurisdiction of the US security-related public policies. Today US customs officials are located in a number of these ports around the world from which the vast majority of containerized US imports is transported.[1] These officials work in cooperation with the local customs authorities during the inspection of containers at the non-US foreign port and before their loading on vessels destined for US ports. To succeed in this task, the CSI uses four different processes:

- the identification of high risk containers;
- the pre-screen and the evaluation of the containers before their loading;

[1] The list of ports participating in the CSI scheme includes: Gothenburg, Klang and Tanjung Pelepas, Algeciras, Antwerp, Bremerhaven, Bussan, Felixstowe, Genoa, Hamburg, Hong Kong, Kobe, La Spezia, Le Havre, Nagoya, Rotterdam, Shangai, Shenzhen, Singapore, Tokyo, Yokohama. The total number of the ports is 50 and cover almost 90% of all transpacific and transatlantic imports. There are nine ports in Americas and the Caribbean, 23 in Europe, 17 in Asia and the East and one in Africa (data as at October 2006).

- the use of state of the art technology—to ensure high definition screening and minimize security related transportation delays; and
- the ongoing use of smart and more secure containers.

CSI is implemented on a reciprocal basis, allowing participating countries to send their customs officers to major US ports in order to inspect containerized cargo being exported to their countries (CBP, 2006a).[2]

This rule has certain implications beyond the US, especially as, since January 2003, its implementation goes hand-in-hand with the application of the "24-hour rule". According to the latter, the US Customs and Border Protection Agency must receive cargo manifest information and bills of lading information from carriers 24 hours before cargoes bound for the US are loaded onboard ships departing from a foreign port. The 24-hour rule has generated concerns due to its potential to distort port competition worldwide (*cf.* UNCTAD, 2004) since some ports that implement the rule might gain the status of more favourable origins for seaborne trade towards the US than others. CSI also contains measures for the elimination of crew list visas, trying to discourage foreign seamen from embarking on ships from US ports, as a means to minimize potential security threats.

This process shifts costs to foreign shippers and ports (CBP, 2006b) and generates policy developments outside the US. To secure container trade according to an "acceptable" CSI regime, a bilateral US–EU agreement provides for joint customs cooperation (CEU, 2004a). This agreement indicates that at least some of the US security measures have a cost and operational impact on European supply chains (see: CEU, 2006a).

The Customs-Trade Partnership Against Terrorism (C-TPAT) is the second major US security-related initiative. According to this voluntary programme, the participating US importers impose security requirements on themselves and their partners in the supply chain with the ultimate goal being to secure the entire chain. This is an initiative operating on a voluntary basis with participants enjoying specific benefits as a motive for joining it. The most important one is the Green Lane award, according to which, Green Lane awarded operators are exposed to less customs inspections and consequently, decreased clearing time for cargo and customs procedures in US ports.

3.2 International Regulations

As in the case of maritime safety, some of the most important regulations regarding security in trade and transport have been undertaken by IMO. The maritime security-related emphasis of the IMO work became evident early in 2002. By the end of the same year, IMO had adopted a major security-related amendment to the Convention of Safety of Life at Sea (SOLAS). This is the new Chapter XI-2 that contains the International Ship and Port Facility

[2] Two examples of countries that have sent customs officers to US ports are those of Canada and Japan.

Security (ISPS) Code, a policy that was to change the way ship and port security is considered.

The ISPS Code has two parts. Part A is mandatory for all the contracted countries, while Part B contains recommended actions. Some countries, including the US, have adopted the optional provisions of the second part as mandatory. The ISPS Code established three security levels denoting the need for normal (level 1), heightened (level 2), and exceptional (level 3), security measures, respectively. The implementation of the Code's requirements and the respective certification of vessels and shipping companies is the responsibility of the flag state, while ports' national authorities are responsible for inspecting and certifying proper implementation. These provisions cover all types of ships that are bigger than 500 grt, mobile offshore drilling units and port facilities serving ships, which are engaged in international voyages.[3]

As regards ports, the ISPS Code concentrates on the locations of ship/port interface. Ports have to develop a port facility security plan (PFSP), detailing the actions that must be taken to prevent, or to correspond to, a security incident at this interface. They also have to designate a port facility security officer responsible for regularly carrying out drills, exercises and seminars in relation to port facility security. In addition, mandatory Part A makes an explicit reference to the "identification and estimation of important assets and infrastructures that are important to protect". This reference provides the background for the ongoing European search for a long-term programme that will effectively protect the critical maritime infrastructures in the EU.

Finally, the amended SOLAS Chapter XI-2 introduced a new technological security measure for ships. This is the automatic identification system (AIS), which enables ships to transmit a unique identification signal in order for the shore operational centres to observe the ship's route. Ships are also required to have on board a security alert system transmitting a security alert to a designated competent authority when activated in emergency situations, and the continuous synopsis record (CSR) that contains details of the ship (including: name, flag, port of registry, IMO number, and owner information).

The Code of Practice on Security in Ports is another security-related initiative that has been undertaken by IMO jointly with ILO. This Code of Practice provides a guidance framework for the development of a strategy appropriate to identifying threats to security in ports (IMO and ILO, 2003). The main provisions are:

- the development of a port's security policy statement by the signatory states;
- the establishment of a port security assessment;

[3] The EU and South Africa are among those that have expressed the intention to extend the ISPS Code to special ships bigger than 500 gt, such as research, expedition and survey vessels, training vessels and fish factory ships.

- the identification and evaluation of the critical assets and infrastructures that are important to protect;
- the development of a port security plan, compatible with the ISPS Code for a port facility security plan; and
- the increased security awareness of personnel training.

Various other organizations strived to create security rules and related documentation. An example, the International Organization of Standardization and its ISO series, ISO 20858, provides guidelines on maritime port facility security assessment, demanding that the relevant port authority develops a port facility security plan and ensures its application in the case of the critical port facility assets (ISO, 2004). ISO 28000 gives guidelines on security management of supply chains (ISO, 2005), and ISO 28001 gives specifications on best practices for implementing supply-chain security (ISO, 2006).

A second example is the adopted in 2003 ILO "Revised Seafarer's Identity Documents Convention" (No. 185) that establishes a "positive" and "verifiable" uniform global identity document for seafarers (ILO, 2003). The World Customs Organization adopted in 2004 a Resolution on Security and Facilitation measures concerning the International Trade Supply Chain (WCO, 2004) The latter requires from customs administrations to develop an action plan for enhancing the security of the trade supply chain. It also demands developed countries to provide assistance to developing and other countries on financing security measures. The resolution also developed guidelines for cooperative arrangements between customs and the industry in order to increase supply-chain security. In particular, the adopted "Integrated Supply Chain Management Guidelines", demand advances in cargo information considering it a living document that should be modified appropriately. These guidelines represent a completely new approach to Customs controls and have a stronger focus on the information requirements for goods.

Overall, security issues today are among the major policymakers' concerns. Previously unwritten customary ethical codes and normative shipping practices (company specific rules, standing orders and practices), take an explicit form of mandatory codified written text, legal or other text with general application to wider groups of stockholders. The transboundary character of maritime laws leads, almost mechanistically, to a growing number of global policy responses that respect this international character. Along with these regulatory developments, a restructuring of international organization is underway in order to prepare for further work on maritime-related security issues: IMO has already set up a new security sub-division within its Secretariat's Maritime Safety Division; a move demonstrating the priority given by the organization to security matters.[4]

[4] The World Customs Organization (WCO) has made a similar move by establishing a "Task Force on Security and Facilitation of the International Supply Chain" in 2002.

4 EU POLICY INITIATIVES

The aforementioned international policy developments took place in a period that the EU was reviewing its Common Transport Policy (CTP) strategy. In line with this, the relative White Paper identified the security of (maritime) transport systems and passengers onboard cruise ships and ferries, as major issues that EU policies should address (CEU, 2001). In the same period, the Commission considered the bilateral agreements on CSI signed by EU Member States (Italy, France, Netherlands, Belgium, Germany) powerless to reverse the situation and limit security-related worries. Since then, the EU has been a leading policymaker in the field. In its Declaration, the European Council of March 2004 called for the strengthening of the security of all forms of transport through the enhancement of the legal framework and the improvement of prevention mechanisms. The reaction of the Commission was to decisively coordinate European reactions, initially by producing proposals based on the IMO agreements, and then focusing on related issues of competence (customs), competition (between ports), external relations and integrated security measures.

Reversing a long period of inertia (*cf.* Power, 1992; Pallis, 2002) the EU developed a rather comprehensive regional regulatory framework in order to secure trade and transport systems. It did so via an evolutionary process, which reflects the endorsement of the concept that the realities of the market make a "big bang" approach unrealistic.

4.1 Regulation on Enhancing Ship and Port Facility Security

Aiming to reinforce a comprehensive and uniform implementation of the mandatory requirements of the ISPS Code throughout the Union, the EU adopted a Regulation mainly aiming at transposing the provisions of the ISPS Code and the rest of the SOLAS amendments into binding EU law.[5]

Regulation 725/2004 (and the ISPS Code) requires that ship and port facility security plans (SSPs and PFSPs) specify a range of security measures to be maintained by ships and port facilities. Ports have to identify restricted areas and monitor them in order to prevent unauthorized access, and implement measures to prevent weapons, dangerous substances and devices being taken onto ships or into port facilities.

The EU has also introduced new additional security measures, extending the application of security provisions to cover international extra-EU but also intra-EU (between EU Member States) trade and transport. While the ISPS covers ships engaged in international voyages and those ports that accommodate them, Regulation 725/2004 includes provisions that extend these measures to the ships engaged in national voyages within the EU, as well as the

[5]. Regulation 725/2004, of 31 March 2004, on enhancing ship and port facility security, O.J. L. 129/6, 29.4.2004.

related port facilities that serve these ships. It also introduces a different agenda by extending the application of the rule to a certain extent to domestic traffic of Member States (i.e. to those ports that might only occasionally serve international transport). The specified port area that is covered by this Regulation is “the location where the ship/port interface takes place”. This includes areas such as anchorages, waiting berths and approaches from seaward as appropriate. This designation of the port area that must be secured is the same as in the ISPS Code.

This rule also requests Member States to identify and evaluate the transport assets and infrastructure that are important to protect. The primary concern of this process is the avoidance of death or injury. The secondary concern is to figure out how the port facility, structure or installation can rapidly re-establish a normal functioning following the threat or occurrence of a security incident. Member States retain the power to determine further measures in order to ensure the appropriate level of security in port facilities that only occasionally serve international voyages, thus not covered by the ISPS Code. Finally, the EU rule created an inspection regime that is managed, and *ex-pos*t monitored, by the Commission.

The ISPS Code has been implemented in European ports with international traffic since 2004. The absence of reports of security incidents of high risk levels in these ports suggests a general good situation of port security. Yet several shortfalls have been recorded in EU ports and include the following:

- cases of ships that insist on a declaration of security even though both the port and the vessel are at low security level, which is causing unnecessary trouble and work;
- cases of vessels’ present tonnage certificates which claim a tonnage of 499 in order to be exempt from the Code; and
- problem of communication/information flows between different parties involved in the implementation of ISPS.

4.2 Revised Customs Code

In the aftermath of the endorsement of the CSI by the US in 2003, and the US–EU customs agreement to reciprocal practices in order to strengthen maritime container security in 2004, the EU adopted Regulation 648/2005, which details a revised EU custom code, in turn setting up common EU secure custom systems.[6] This is because customs administrations are considered to be the ideal authorities to deal with security. They are key players in the supply chain, they have the necessary risk management techniques to target high-risk consignments, they are able to collect and analyse the necessary data for control, and most probably, have the necessary equipment.

[6] Regulation 648/2005, of 13 April 2005, amending Council Regulation 2913/92 establishing the Community Customs Code. O.J. L. 117, 13–19, 4.11.2005.

The revised customs code introduced measures to tighten security for goods entering or leaving the EU. The measures, which will be fully in force in 2009, aim to produce better-targeted customs controls, and be consistent with the analysis and electronic exchange of risk information between customs authorities in a common risk management framework. This policy follows the principles of the US C-TPAT regulation and similarly to the 24-hour rule, it sets up risk-based controls by establishing the requirement of pre-arrival or pre-departure information for all goods brought into or out of the customs located in EU territory.

It also introduces for the first time the status of the authorized economic operator (AEO) as a core element for enhancing supply-chain security. When an operator complies with the administrative rules and supply-chain security requirements, as defined by the code, he is awarded the AEO status and experiences reduced customs inspections; a status similar to the Green Lane award that is established in the US under the C-TPAT regulation. There are four criteria to be fulfilled in order to be granted the AEO status:

- appropriate record of compliance with customs requirements;
- a satisfactory system of managing commercial records;
- proven financial solvency (where appropriate); and
- appropriate security and safety standards (where applicable).

As a consequence of the requirements of the new customs codes on both sides of the Atlantic (i.e. C-TPAT and the EU revised Code), customs now fulfil a new upgraded role when a few years ago their major task was the collection of import duties. Now customs also have a tendency to become security inspectorates of imported and exported cargoes.

4.3 Directive on Enhancing Port Security

Within this context, the EU discussed additional measures aiming explicitly to secure the port industry. As Regulation 725/2004 tackles the issue of security at the ship/port interface, the EU moved in order to secure the rest of the port. This led to the adoption of Directive 65/2005 on enhancing security in the broader port area, giving particular attention to ro-ro vessels carrying passengers and vehicles.[7] The latter depends on the boundaries of the port, and given the absence of a widely accepted definition of the "port area", the Directive leaves the designation of the port boundaries to the member states. In turn, Member States must comply with the Directive requirements no later than June 2007.

Directive 65/2005 applies to every port in which one or more port facilities are situated to which the Regulation 725/2004 applies; thus an approved port facility security plan (PFSP) exists. Measures to enhance port security consist

[7] Directive 2005/65, of 26 October, on enhancing port security, O.J. L. 310/28, 25.11.2005.

of common basic rules, an implementation mechanism and an appropriate compliance monitoring system, with a clear division of tasks between the parties involved. Ports must develop a port security plan (PSP) that contains the necessary procedures and actions to be undertaken in the event of a security incident. It is explicitly mentioned that these actions shall also apply to passengers and vehicles, set for embarkation on seagoing vessels which carry passengers and vehicles. Ro-ro vessels are individuated as particularly vulnerable to security incidents, in particular if they carry passengers or cargo, therefore relevant authorities are asked to proceed to a risk assessment of those vessels trading in domestic and international routes, in a way which impedes the fluidity of the operations as little as possible.

The monitoring of the compliance, including the confidentiality and dissemination of information, has to be implemented by a responsible port security authority established in each Member State. Moreover, every port or, if necessary, a group of ports must have a port security officer (PSO) who acts as the contact person. Finally, the Directive designates three security levels (normal, heightened and exceptional) reflecting differences in the risk profile of different sub-areas in the port, and demands different measures. The whole process must be revised at least once every five years, while member states have to ensure the presence of a focal point for port security assigned the role of contact point with the Commission, in order to ensure the proper implementation of the Directive.

This rule supplements Regulation 725/2004. By implementing security measures to the whole port, it contributes to the creation of a common playing field for the entire port sector. Second, Directive 65/2005 is in line with the view that only a uniform level of security at all ports will reduce the risk of disruption in global supply chains (Banomyong, 2005). To reduce this risk further, the Commission has already proposed an additional regulation on supply-chain security.

4.4 Towards an EU Policy Enhancing Supply-Chain Security

Having addressed different transport modes and nodes with security-related regulations,[8] the EU moved towards developing rules for the protection of the remaining parts of the supply chain. The absence of such rules contradicts the necessity for a holistic approach to security and for the application of security measures to the entire supply chain in which ports are integrated (Bichou, 2004).

Supply-chain management expands the principles of logistics management to customers and suppliers, crossing geographical and organizational boundaries (Henstra and Woxenius, 1999). On these grounds, the Commission

[8]. For instance on 16 December 2002, the EU adopted Regulation 2320/2002 establishing common rules in the field of civil aviation security. O.J. L. 355, 30.12.2002.

proposed a Regulation in 2006 aiming at enhancing supply-chain security (CEU, 2006a). A key theme is the integration of the various piecemeal EU initiatives and in order to do so, the proposal elaborates the concept of "known shipper/operator" to the whole supply chain, making use of already existing concepts like "consigned agent", "known consignor", "known shipper" and "authorized economic operator". If adopted, this measure will affect the port industry as supply-chain corridors commence at the production site and end at the cargo's final point of destination. During the consultation process,[9] however, stakeholders were critical of additional security measures in the field of maritime (and air) transport, arguing that any security rule addressing the supply chain has to include only provisions that complement existing policies.

The philosophy of the EU institutions is that "any chain is only as secure as its weakest link". The Commission has endorsed this concept since the consultation process of Regulation 725/2004. In this vein, its policy initiative recognizes four groups of supply-chain activities:

1. the preparation of goods for shipment and shipment from the production site;
2. the transportation of goods;
3. the forwarding of goods; and
4. warehousing, storage and inland terminal operations.[10]

The security of the entire supply chain is feasible only in situations where each operator assumes responsibility for the security of his/her own activity. The key issue is to motivate operators to participate in relevant schemes. Towards this end the Commission proposes the method of "positive discrimination". According to the proposal in discussion, the various stakeholders will be motivated by the secure operator (SO) status, to be awarded to any supply-chain operator that fulfils minimum security requirements. This status will be designated to an operator by the member state in which it operates and will be recognized by all member states. As in the case of the AEO status, the benefits include facilitations in security controls and a quality status. Due to the latter, security performance might create a commercial and competitive advantage: this operator will provide a more comprehensive interconnectivity with the already secured maritime and air transport and enjoy a Europe-wide recognition. Due to the SO scheme, Member States will be able to allocate resources to the inspection of the "unsecured" operators. The measure will also contribute to the formation of a homogeneous security environment with common requirements, awareness and objectives throughout Europe.

[9] Available at: *http://europa.eu.int/comm/dgs/energy_transport /security /intermodal/consultation _en.htm.*

[10] For a description of the supply-chain security requirements: DNV Consulting (2005).

4.5 Revising the Port State Control Process

Whilst aiming almost exclusively to increase pressure on sub-standard ships and deal with the consequences of accidents, regulatory proposals that are part of EU maritime safety policy are also relevant to security. To achieve these goals in 2005 the Commission proposed the adoption of seven measures, the so-called third EU maritime safety package (CEU, 2005b).[11]

One of these proposals will reform the port state control regime and it is of particular importance for the enhancement of maritime security. During the discussions of the proposed Directive, the Council of Ministers (2005) included in its Annex VII procedures that port state control authorities must follow for inspecting and controlling ships compliance with security related rules. If transposed to an EU rule, these procedures will give the authority exercising port state control, the right of inspection of the security conditions onboard the ship and if required, the detention of the ship at the call-port.

4.6 European Critical Infrastructure Protection

In 2005 the EU embarked on a discussion about a European Programme for Critical Infrastructure Protection (EPCIP), aiming to cover the infrastructures that are vital for the EU (CEU, 2005a).

According to the Commission's Directorate General responsible for Transport and Energy (DG-TREN), European critical infrastructures are those physical resources, services and information technology facilities, networks and infrastructure assets or parts thereof that if disrupted, or destroyed, would have a serious impact on critical social functions (including the supply chain, health, safety, security, economic or social well-being) of two or more Member States, or a single Member State if the critical infrastructure is located in another member state (DG-TREN, 2006a). Such critical infrastructures can be found in 11 sectors, one of them being transport.[12]

The EPCIP considers unlawful acts, as well as disasters due to natural phenomena. The goal is to ensure adequate and equal levels of protective security on critical infrastructures, minimal points of failure and tested recovery arrangements throughout the whole infrastructure which is vital for the EU, while at the same time minimize the negative impacts that increased

[11] The themes of the seven proposed measures are: (a) the improvement of the quality of European flags; (b) the review of the legislation on port state control; (c) the amendment of the Directive on traffic monitoring; (d) the improvement of the rules in force regarding classification societies; (e) a directive on enquiries following accidents; (f) a regulation on responsibility and compensation to passengers in the event of an accident; and (g) a Directive on the civil liability of shipowners. These measures will be monitored by the European Maritime Safety Agency.

[12] The other nine identified sectors are: energy; nuclear industry; information and communication technologies; water; food; health; financial; chemical industry; space and research facilities.

security investments might have on the competitiveness of a particular industry. The three main steps towards this direction are: (a) the identification of the European critical infrastructures; (b) the assessment of their vulnerability and the needs for additional protection; and (c) the introduction, whenever necessary, of additional protection measures.

For each EU Member State, this strategy implies the establishment of a critical infrastructure protection authority responsible for monitoring the process within this state. For the operator of the infrastructure, it implies the development of an operator security plan, which describes the security measures that have been taken, and a security action plan in relation to the protected infrastructure. It also implies the designation of a security liaison officer who is the contact point between the authority responsible for the critical infrastructure and the critical infrastructure protection authority of the member state.

The monitoring measures that are part of this programme include an action plan, a warning information network, the mobilization of expert groups at EU level, information sharing processes, and finally a broader discussion towards the identification and analysis of interdependencies of the various European transport (and other) infrastructures.

European ports with international traffic facilitate the function of the single European market and therefore can be characterized as critical infrastructures. Yet this development is controversial precisely due to the same problem that had dominated discussions regarding the inclusion of ports in the Trans-European Transport Networks (TEN-T): there are no clear-cut criteria to be used in order to include or exclude specific ports from a list of ports characterized as European critical infrastructures (*cf.* Pallis, 2007). Port authorities, for instance, have already expressed concerns that such a list might result in undesirable side effects in terms of port development, planning and competition (ESPO, 2006).

DG-TREN (2006a) proposed the use of three criteria as a means to overcome this difficulty, advocating that the combined presence of these criteria should result in including ports in the list of the European critical infrastructures:

- a threshold of total traffic volumes (with an option to exclude short-sea shipping and passenger volumes);
- the origin or final destination of a fixed percentage of cargo that flows outside the country where the port is located; and
- the location of alternative ports in proximity to the port which will be able to handle equivalent volumes of cargo/passengers in order to substitute the port in the case of a terrorist attack.

However, several Member States support the characterization of all European sea ports as "critical". The Euro-group representing port authorities (ESPO), demands the application of precisely the same criteria that apply for the inclusion of ports in the TEN-T. The reaction of the DG-TREN (2006b) was to format a new proposal that combines the following criteria:

- ports in which the Directive 65/2005 is applicable;
- ports in which the Regulation 725/2004 is applicable;
- ports that are part of the TEN-T, according to Decision 1346/2001;
- the type and volume of the cargoes handled in a port and the presence of alternatives;
- ports that handle vessels from/to EU Member States;
- ports that handle cargo volume above a threshold;
- ports that handle dangerous types of cargo (e.g. LNG);
- ports where no suitable neighbouring alternative port exists.

Using these variables DG-TREN suggests that those ports that fulfil the three first criteria as well as the combination 4.a + 4.b + 4.d, or the combination 4.a + 4.c + 4.d, of the elements of the fourth criterion, should be characterized as European critical infrastructures.

At the beginning of 2007 there are still no horizontal provisions on critical infrastructure protection at EU level. To overcome this situation, the Commission has put forward a proposal for a Directive that establishes a procedure for the identification and designation of European critical infrastructures, and a common approach to the assessment of the need to improve the protection of such infrastructures (CEU, 2006b). Then, a sector-by-sector European project will be deployed for the protection of these infrastructures on the basis of the principles of subsidiarity, complementarity with existing sectoral measures, confidentiality of information, stakeholder cooperation, and proportionality to the level of risk and type of threat involved (CEU, 2006c).

It is not likely that sea ports will be addressed in an early phase of the implementation of the Directive. This is because a number of sectoral measures already exist. In addition, the proposal for the aforementioned Directive as it stands, explicitly exempts sea ports from the requirement to establish such a plan. This is because it is acknowledged that Directive 2005/65 on enhancing port security already satisfies the requirement to establish an operator security plan. The other ECIP obligation is for operators and owners to designate a security liaison officer (SLO). The Commission indicated that, although not entirely identical, the PSO existing under port security Directive 2005/65 serves as a basis for the designation of a SLO. In the same vein, stakeholders and Member States in the field of transport have already agreed on the absence of an immediate need to impose additional security measures on ports, which are nevertheless already covered by the Directive on port security.

4.7 The Contemporary EU Regulatory Scene

As Figure 1 illustrates, the total of the analysed initiatives, along with Regulation 2320/2002 that the EU has adopted in order to address security issues of air transport,[13] mark the presence of a regulatory framework that deals with all the parts of a supply chain, i.e. supply-chain security, port security and ship and port facility security.

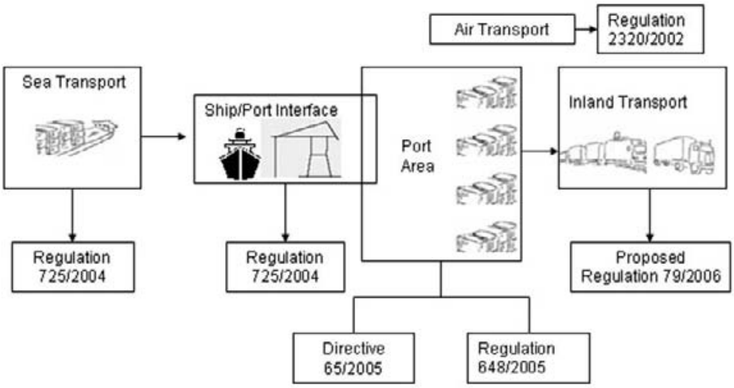


Figure 1: The European Supply Chain and the Applied Security Regulations

Regulations 2320/2002, 725/2004 and 648/2005 are already in force. The same is true as regards Directive 65/2005 and Member States have brought into force national level laws, regulations and administrative provisions that are necessary to comply with it since June 2005. The other two security initiatives are not yet in force. Regarding the European Programme on Critical Infrastructure Protection, the Green Paper, the process of stakeholders' consultation, is in the stage of completion and a Communication on protecting Europe's critical energy and transport infrastructure is expected to be published within 2007. Relevant legislative initiatives remain an option for the future. Finally, the European Commission is also expected to publish a Communication putting forward a proposal for a regulation on enhancing supply-chain security within the first half of 2007.

Geopolitical developments induced a widespread acknowledgement of the need for a major effort to secure port areas and maritime transporting in order to prevent unnecessary security incidents. Yet, port authorities have been sceptical about the aforementioned supranational EU policies. Reactions have focused mainly on the need to avoid a "one size fits all ports" approach and on the transfer of the responsibility for inspections to a supranational level. Via the European Seaports Organisation (ESPO, 2004) port authorities expressed the view that the Commission's role should be limited to verifying the overall

[13] *Op cit.*, footnote 8.

implementation of the general principles of Directive 65/2005 and Regulation 725/2004 by member states.

Moreover, port authorities reacted strongly to a potential EPCIP advocating that there is no need for another security regulation in ports, as it would place an unnecessary burden on commercial activities with adverse effects. Their view is that this programme might result in situations where a carrier may choose a port that has been characterized as critical infrastructure solely because this would suggest that he enjoys increased security.

Port authorities believe that the proposed regulation on enhancing supply-chain security is another unnecessary regulatory burden, as the port sector is already secured by the existing policy regime and asked for an exclusion of ports from any additional measures. ESPO has also stressed the contradiction between the proposed regulation on supply-chain security and the ISPS Code. The latter implies stricter inspection measures at the port points of entrance and exit, while the former requests fewer checks for the “secure operators” at ports. Port authorities are also negative to the introduction of voluntary schemes and favour a mandatory minimum basic security standards regime. This is because in the case of a voluntary scheme, the weaker parts of the supply-chain would face difficulties in participating due to their inability to finance the substantial costs involved (ESPO, 2006).

On the contrary, European freight forwarders are in favour of a voluntary supply-chain security scheme. Yet, via the European Association for Forwarding, Transport, Logistics and Customs Services (CLECAT) they have requested certain actual incentives for companies that will participate and implement the requirements of this scheme (i.e. partial compensation for their expenses) therefore major importance is placed on the re-examination of the liability issue (CLECAT, 2006). Specifically, it is of primary interest to associate the status of the “secure operator” with the opportunity to insure the operation and the eligibility for compensation in the case of a major incident. Freight forwarders advocate the need for an advisory stakeholders’ group, similar to the Stakeholders’ Advisory Group on Aviation Security (SAGAS). Pointing out that all security regulations and statuses have many common requirements or identical criteria and cause confusion to operators; they suggest that this group could contribute to the simplification of the security processes and the related statuses.

5 ASSOCIATED COSTS AND BENEFITS

The profound benefits of the EU rules addressing supply chain, port and ship security are accompanied by substantial implementation costs. The allocation of these costs and the presence of uniform methods of financing this implementation are two controversial issues. In the case of the port sector, a number of policymakers and stakeholders have expressed diverge approaches, mainly because of the presence of organizational, management and port financing dissimilarities.

5.1 Cost and Benefits of Rules Enhancing Ship and Port Security

The costs of the ISPS Code implementation as detailed in Regulation 725/2004 largely depend on the peculiarities of each ship or port, rather than on a standard and uniform approach for every ship or port. The challenge is to address potential ways of financing this implementation. To start with, in the absence of a global financial tool, there is a need to define how to finance the expenditure. Then, there is the question of how to incorporate these costs into pricing and marketing strategies, while at the same time these ports maintain their market shares and achieve reasonable profit margins (*cf.* Bichou, 2004). Today, terminal security fees as charged by operators vary significantly, as do the approaches to financing and recovering schemes.

For a port facility located in the EU the average initial investment cost in order to implement the ISPS in line with Regulation 725/2004 has been estimated at $464,000. The annual running costs are estimated at $234,000 (RMG), undated).[14] Overall, the estimation of the global initial investment stands as a low proportion of the overall investment and operating cost in maritime transport.[15]

There are three distinctive approaches as regards the financing of this implementation (*cf.* UNCTAD, 2006):

- the facility operators might finance the entire cost which is then recharged to customers;
- the port authority might cover the financial burden; and
- the cost might be shared between different parties, for instance, the state, the port authority and the port operator(s), with each one assuming responsibility for recovering its own costs.

Identifying the most suitable scheme remains a more complex issue than in cases like shipping. In the case of a vessel, responsibility lies with its operator. In the case of ports the various ownership and management structures result in the absence of a uniform financial scheme. According to the Rotterdam Maritime Group 19% of port facilities increased port tariffs in order to recover the implied costs and 55% have imposed a separate ISPS tariff (RMG, undated). Another 23% have opted to finance the cost of the ISPS implementation from subsidies. Assuming that these subsidies are provided by public entities, the private sector finances the cost in 74% of the total number of port facilities (CEU, 2006d). Users, port authorities and port operators

[14] The same study estimated that the implementation of the ISPS Code for shipping companies demands an average investment of $98,109 per vessel and an annual running cost of $25,000 per vessel.

[15] *Lloyd's List*, "Caribbean fears US trade link loss", 30.1.2004.

currently cover most of the security-related costs. Most European ports have introduced port container security charges to recover initial expenditures. In 2006 the average terminal security fees were $10.98/TEU in Belgian ports, $10.37/TEU in Dutch ports, $10.98 in French ports, $9.76 in Italian ports, $6.1 in Spanish ports and $8.54 in Irish ports.[16] Yet the presence of public funds in some cases questions the impact on the conditions of competition in the sector.

The lack of a EU rule regarding state aid creates further ambiguities regarding the impact of security measures on port competition. Given the lack of such rules, public finance is in some cases used to secure the transportation process, while in other ports shippers have to pay for security measures. In this case, maritime security measures create competitive advantages that distort competition.

On the one hand, it is argued that the mobilization of public funds for implementing security measures contradicts Article 87(1) of the EU Treaty on state aid, as it distorts market conditions. On the other hand, it is advocated that the EU Treaty acknowledges that public finance which is devoted to the implementation of measures imposed by law and connected with the exercise of powers, typically those of a public authority, does not constitute economic activity. Thus, the public financing of transport security measures does not constitute state aid. The potential to overcome this situation and achieve the smooth implementation of the EU security-related port measures is inextricably linked with the presence of clear guidelines or regulations, creating a homogeneous regime insofar as state aid to European ports and the transparency of their financing are concerned.

Directive 65/2005 results in additional security obligations spreading cost-related concerns. ESPO and the Federation of Private Port Operators (FEPORT) endorse the view that measures taken under the Directive are in the general public interest and should be covered by public funding. The latter should also cover the costs made by the designated authority (the formation of which is required under the Directive) and the recurring overhead costs (audit and control), while the users of the specific port facilities should cover all other costs.

The major benefit of Regulation 725/2004 and Directive 65/2005 is the elimination of the risk of an unlawful act. The higher the risk—which equals the possibility of an action/element occuring, multiplied by its consequences—the higher the adverse effect on the operators' returns (Carter and Simpkins, 2002), and on the operating companies' capacity to remain attractive to capital investors (Homan, 2006). Security policies not only reduce the threat from unlawful acts and the direct costs that the latter might produce,

[16] Summary of various news articles from *Lloyd's List*, *Fairplay* and *Containerisation International*, as quoted in UNCTAD, 2006.

including human casualties, value of the destroyed investments and value of infrastructure reconstruction. They also reduce the systematic risk, which is a primary component of a firm's weighted average cost of capital (Hamada, 1969).

Stricter security measures produce ancillary economic benefits, including invisible collateral benefits, such as the improvements in efficiency and trade facilitation that are difficult to measure where no security incidents occur (Rice and Spayd, 2005). Temporary closures of a sea port result in highly variable product delivery lead times and thus increase supply-chain inventory management costs. Since short port closures typically lead to ships waiting to off-load cargoes, the long-term average cost for a firm operating a supply chain that uses a sea port subject to unexpected closure increases (Lewis *et al.*, 2006). Beyond these benefits, the presence of uniform security requirements for all European ports eliminates potential competition distortions and contributes to a level playing field within the Single European Market.

5.2 Costs and Benefits of the Proposal on Enhancing Supply-Chain Security

The proposed Regulation on enhancing supply-chain security has an effect on all the elements integrated in this chain. The number of enterprises in the 25 EU Member States to be affected stands at approximately 4.75 million (DNV Consulting, 2005). In the case of the port sector, economic effects (costs) have a reference to the integration of inland transport modes (road, train, inland shipping) and the providers of value-added services and value-added logistics within the port area. There are also additional requirements for port operators, such as the fast track treatment of the "secure operators". The development of maritime supply chain underlines the interaction between security issues and management strategies of ports around the world (Flemming, 1999).

For the moment, there are three potentials as regards supply-chain security. The first one is for the situation to remain as it is. The second is the development of a voluntary scheme which companies participating in the supply chain are free to join. The third option is for a mandatory EU policy according to which all companies in the supply chain are forced to implement common security rules.

The cost for the implementation of either the potential mandatory or voluntary schemes derives from the demands for inspection of security measures, the audit of the implementation status, the enforcement of the requirements, etc. The Commission has put forward a categorization of the affected enterprises (based on the number of employees) in order to estimate the cost for the implementation of a security management system (SMS).

In the case of a mandatory scheme, the costs are estimated to range from €5,000 to €300,000 (Table 1). Based on an estimated number of companies in each category, the cost of implementation will reach a total of €60 billion for all the companies participating in European supply chains. For member states the costs for verifying implementation through audit will be €3.867 billion: €2.7 billion initial verification, plus €1.167 billion for annual verification thereafter (DNV Consulting, 2005). This corresponds to an auditing cost of €0.55 per EU citizen per year (CEU, 2006e). There is an additional cost of enforcement estimated at €450 million for an initial three-year period plus €50 million per annum thereafter. In practice there are further costs because of the required aftermath actions (such as the awareness campaign, the employee vetting system and the EU seal programme) resulting in a higher final total cost.

Company type	*Employees*	*Estimated costs for implementing a SMS(€)*
Micro companies	1–9	5,000
Small companies	10–49	50,000
Medium companies	50–249	135,000
Large companies	>250	300,000

Table 1: Costs for Implementing a Mandatory Security Manage-Ment System

(Data source: DNV Consulting, 2005)

The endorsement of a voluntary scheme in Europe is estimated to attract approximately a maximum of 904,500 companies, or 75% of all freight flows within five years from the introduction of the regulation. In this case, the cost for the supply-chain companies will reach €12.1 billion. The enforcement cost will remain at €450 million for the first three-year period but there will be no annual enforcement cost thereafter. Finally, the auditing cost will be substantially lower and estimated at €514 million for the initial verification and €227 million for the annual auditing cost (DNV Consulting, 2005).

As Table 2 summarizes, a mandatory scheme requires significantly higher funds than the voluntary scheme. There are further questions regarding the potential of a mandatory scheme. Many companies, especially the small ones that are the vast majority of the companies participating in the supply chain, place hardly any importance on security. The successful implementation will be difficult as these companies cannot afford it. Moreover, these are mostly companies of national importance which do not think that security measures will give a competitive advantage to their operations. Taking into account all these, it seems probable that the EU institutions might finally endorse the voluntary scheme advocated by the Commission.

Cost	*Mandatory*	*Voluntary*
Supply chain companies	€60 billion	€12.1 billion
Member states (audit, implementation)	€2.7 billion initial three year period + 1.167 billion p.a.	€514 million initial three year period + €227 million p.a.
Enforcement	€450 million + €50 million p.a.	€450 million
Coverage (freight flows)	100% (4.75 million companies)	75% (904,500 companies)

Table 2: Comparison of the Major Costs of Mandatory and Voluntary Schemes

(Data Source: DNV Consulting, 2005)

The benefits of the endorsement of any of the two schemes extend the societal benefits resulting from trade facilitation, the reduction of the risks of human casualties and economic damage from a security incident, and the increased confidence in the supply chain. For the participating companies there are further benefits resulting mainly from the reduction in cargo theft, the prevention of damage to the brand, and the reputation of a company. A cargo theft reduction of 10% will result in €10 billion savings for the EU economy (DNV Consulting, 2005). The short-term effects might be negative due to the required investments, but the medium- to long-term impacts are likely to be beneficial, at least for the certified and recognized operators (Banomyong, 2005).

An additional issue that remains to be addressed is the fair distribution of the costs of the new rules. In the absence of a common approach in all security-related polices the funding regime might distort competition. The Directive on port security emphasizes that the financing of security measures has to be shared between public authorities, port authorities and operators. On the other hand, the proposed EPCIP recommends that the owner/operator of the European critical infrastructure should finance the preparation of the operator security plan and the work of the SLOs. Taking into account the increased number of stakeholders in ports and their complex relations (Notteboom and Winkelmans, 2002), as well as the multiplicity of ports' ownership, operational and management status (Bichou and Gray, 2005), a means to specify the distribution of optimum security costs (financing of an action) is to identify and quantify the benefits that the security measures result in, and then apply the principle "beneficiary pays" (*cf.* Pallis and Vaggelas, 2005). Nonetheless, the implementation of this efficient (as it includes the distortion of competition) financing of security regulation needs to also take into consideration equity objectives, i.e. the contributive capacity of the different actors involved (*cf.* Dubecco and Laporte, 2004).

5.3 Implementing EU Security Policies

Among the greatest impediments to improving port security is the extent to which this issue has previously been neglected both at micro (firm) and macro (regulatory) level. Although policymakers are no longer neglecting security, numerous factors make port security planning and implementation a continuing challenge. These include:

- *Volume*. An extremely large amount of goods flows through the maritime supply chain.
- *Intermodality*. Goods arrive at and depart from the port not only by ship but by rail and truck.
- *Jurisdictional conflicts*. Supranational institutions, national states and local governments may all have oversight over some port activities. In addition, some ports are managed by local or regional port authorities, whereas others are managed by local or state governments or by private entities.
- *Quantity of stakeholders*. Carriers, shippers, logistics firms, producers, labour unions, and others all work at or use the ports and all must be involved in security efforts for these to be effective.
- *Global nature of industry*. Any serious security effort requires international cooperation from foreign governments, foreign port operators and foreign ship owners.
- *Time sensitivity*. Production has moved to just-in-time processes, with manufacturers relying on steady shipments of inputs.
- *Public and private involvement*. Both sectors are likely to be interested in having the other carry the burden of financing or even planning security efforts.

Despite their contribution to safeguarding world trade and transport modes from unlawful acts, the aforementioned EU security policies have caused an ongoing debate. Without ignoring the apparent social and economic benefits, stakeholders have advocated that the four EU regulatory initiatives on port-related security will lead to an overregulated scheme and contribute to the creation of a confusing policy framework. To a certain extent these complaints are valid as the partial examination of the port complex during the policy formation has resulted in some contradictory practical requests. Regulation 725/2004 applies only in the area in which ship and port interface takes place, Directive 65/2005 aims at securing the rest of the port area. At the same time a Regulation concerning the security of port interface with inland transport modes is under discussion. Within this scheme, some port areas are affected by the requirements of more than one policy initiative. For example, the port road network falls within the scope of two policies: the proposed Regulation on enhancing supply-chain security applies at those port areas which interact with inland transport modes; Directive 65/2005 applies in the rest of the port area. Implementation and planning difficulties increase as it is complicated to identify and clearly define at port level those port areas and activities in which each of these security policies should apply. A smoother implementation of security policies demands a holistic EU approach, with the latter contributing to avoid misunderstandings and the development of an unnecessarily complex security regulatory framework.

Another major implementation concern relates to the implications of the developed regime on port productivity due to an increasing number of checks, inspections and accreditations. The proper implementation of the secure operator status, as well as the use of high-technology equipment stand as two developments that would allow for cargo inspections while minimizing the relevant interruption of the transport process. Regarding the former development, providing incentives that would convince firms to seek this status stands as a vital issue for successful implementation of the discussed security regime. Neither the EU institutions nor the national governments of its Member States would benefit by demanding that companies directly participate in security costs, as this would increase transportation costs to/from Europe. Thus it is worth finding innovative ways to convince the involved (trans)port users and service providers to jockey for the effective implementation as a "win-win" situation.

6 CONCLUSIONS

The frequency of the recent major transport-related incidents has demonstrated how vulnerable (trans)port infrastructures may be to unlawful acts. As a result, the level of transport security awareness has increased while in the field of maritime transport, security has moved up on the political agenda worldwide.

In this context, the EU has been active in legislating in order to improve security at ports and at sea. The spatial dimension of the problems contributed to the evolution of EU-level decisions, at the expense of national policy initiatives. Considering Europe as a single transport market where there should not be a multitude of national security rules, has provided further impetus for the intensive EU institutions' intervention and for complementary international efforts in this policy arena.

Yet, as in other fields of maritime transport (i.e. safety—*cf.* Pallis, 2006), the initiative of the EU institutions had to acknowledge that any relevant threat needs a global response, and security measures can be locally defined only in exceptional cases. The first major EU initiative focused on the enhancement of a uniform implementation of the ISPS Code throughout Europe, and expanded its application to vessels engaged in national voyages.

The two policies aiming to bring a coordinated approach to security matters in European ports as a whole and upgrade the role of customs also follow principles that are similar to those schemes adopted either in the US or in the international fora. The first principle is that there should be compatibility of security measures with custom rules, as customs are responsible for security at external borders. The second one is that, secure operators should be rewarded; a strategy that enables the introduction of voluntary rather than mandatory security rules. The third principle is that transport modes and/or nodes, or even competing operators of the same mode and/or node, should be treated according to their peculiarities since the presence of different levels of security demands in different ports results in a variation of the applied security rules.

The functional implementation of transport nodes, like ports, in the wider transport supply chains justified the endorsement of the concept that inner EU supply chains are transnational and interdependent. Hence, EU policy is seeking to secure freight flows and passenger movements throughout relevant policy proposals that complement the rules for maritime security. The Regulation on enhancing supply-chain security, and the European Programme for Critical Infrastructure, which are currently under consideration, are part of the process of incorporating modal rules into an integrated approach of security issues.

The key themes of all these policies are the introduction of port authorities' tasks on security management systems assessing the risk and planning of both proactive and reactive measures (plans, security officers, etc), allocation of responsibilities to operators and the reward of the secure ones, national legislation imposed by cooperating national administrations and the mutual recognition between the national systems and a monitoring system allocating a major role to the European Commission.

All these EU measures transformed within a short time a port market that was previously unregulated as regards security issues. Complaints about an over regulated market and about confusing contradictory requirements by these regulations are not rare. The potential of additional security measures (supply-chain regulation), and measures to be applied in some but not all European ports (i.e. EPCIP) have already been questioned by port authorities and port operators. The benefits of the secure operation are associated with issues of financing and cost-recovery of the expenditures involved in implementing security measures.

Concerns in Europe regarding the regulatory framework have intensified as further security rules are under discussion in the US. The latter include a new bill that, once enacted will prohibit entry into the US of containers that have not been scanned (i.e. for nuclear weapons and explosives) and secured with an approved seal. This rule will require a programme according to which within three years these requirements will be applied to any container loaded on a vessel destined for the US in a country where more than 75,000 TEUs of containers are loaded on vessels for shipping to the US. The requirement will be expanded to all other countries in five years. Some believe the Bill may result in serious disruption of trade in the US, while costs for technology for such levels of rigorous screening might not be affordable by various port facilities worldwide.

Nonetheless, the EU has chosen a different policy path. The Commission's work programme, with support from member states, includes consideration of minimum standards for security measures. The purpose of the used generic title "minimum standards" is not meant to be limited to minimum security standards *per se*, but to include performance specifications, guidelines and/or best practices to implement the security requirements and measures in Regulation 725/2004. The aim is to develop a number of security requirements that Member States will apply once security assessments and plans are reviewed and updated. Depending on the subject, the most adequate instrument for implementing these minimum standards will have to be chosen. Towards this direction the Commission already focuses on the current situation in the EU in order to conclude on the best practices for applying maritime security rules and the most reliable accreditation process for recognized security organizations.

The enactment of the EU rules will soon provide a comprehensive security policy addressing all (trans)port issues in an integrating way. Assuming that the right allocation of economic costs succeeds, the positive effects are apparent. The focus will then be on their proper implementation via the inspection and auditing of the participating member states, port and other relevant authorities, and companies involved in (maritime) transport operations.

This chapter discussed the relevant EU port security policies mainly from a macro scale point of view. When these policies are applied, the implications might be quite different at a micro scale, i.e. intracontinental shipping. Ng, in Chapter 20 of this volume, addresses this issue, by focusing on a more specific case study, that is, the examination of the effects of port security policies on EU short-sea shipping.

REFERENCES

Banomyong, R., (2005), "The impact of port and trade security initiatives on maritime supply-chain management", *Maritime Policy and Management*, 32, 1, 3–13.

Barton, H. and Turnbull, P., (2002), "Labour regulation and competitive performance in the port transport industry: The changing fortunes of three major European seaports". *European Journal of Industrial Relations*, 8, 2, 133–156.

Bichou, K., (2004), "The ISPS Code and the cost of port compliance: An initial logistics and supply chain framework for port security assessment and management", *Policy Perspective, Maritime Economics and Logistics*, 6, 322–348.

Bichou, K. and Gray, R., (2005), "A critical review of conventional terminology for classifying seaports", *Transportation Research*, part A, 39, 75–92.

Carter, D. and Simpkins, B., (2002), *Do markets react rationally? The effects of the September 11th tragedy on airline stock returns*, Stillwater: Oklahoma State University.

CBP (Customs and Border Protection US), (2006a), "Fact sheet". September 2006, Washington DC.

CBP, (2006b), "Container Security Initiative. 2006–2011 strategic plan". *CBP Publication 0000–0703*. August 2006, Washington DC.

CEU (1997), "Green Paper on sea ports and maritime infrastructure", Com (97)678 final, Brussels, 10.12.1997.

CEU (2001), "White Paper-European transport policy for 2010: time to decide", Com (2001)370 final. Brussels, 12.9.2001.

CEU (2003), "Fight against terrorism: Security of European maritime transport to be strengthened", IP/03/651, Brussels, 8.5.2003.

CEU (2004a), "Customs: EU and US adopt measures to strengthen maritime container security", IP/04/1360. Brussels, 15.11.2004.

CEU, (2005a), "Green Paper on a European Programme for Critical Infrastructure Protection", Com (2005)576 final. Brussels, 17.11.2005.

CEU (2005b), "Proposal for a Directive on Port State Control" (Recast), Com (2005)588 final. Brussels, 23.11.2005.

CEU (2006a), "Proposal for a regulation of the European Parliament and of the Council on enhancing supply chain security". Com (2006)79 final. Brussels, 27.2.2006.

CEU (2006b), "Proposal for a Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection", Com (2006)787, final. Brussels, 12.12.2006.

CEU (2006c), "Communication from the Commission on a European Programme for Critical Infrastructure Protection", Com (2006)786, final. Brussels, 12.12.2006.

CEU (2006d), "Report from the Commission to the Council and the European Parliament on transport security and its financing", Com (2006)431 final. Brussels, 1.8.2006.

CEU (2006e), "Annex to the Communication on enhancing supply chain security and Proposal for a Regulation on enhancing supply chain security—Impact Assessment", SEC(2006)251, Commission Staff Working Document. Brussels, 27.2.2006.

Chlomoudis C.I. and Pallis A.A., (2002), *European Port Policy: The movement towards a Long-term Strategy*, Cheltenham: Edward Elgar.

CLECAT, (2006), "Discussion paper", Brussels: CLECAT, 6.8.2006.

Council of Ministers (2005), "Third Maritime Safety Package: Proposal for a Directive on Port State Control", W.Doc 2005/67, Brussels: General Secretariat of the Council, 30 11.2005.

DG-TREN (2006a), "Minutes of the Expert Group meeting on Critical Maritime Infrastructure", 28 March, Brussels: CEU.

DG-TREN (2006b), "Element of background", TREN.J.3/RGG/mcgD (2006)213863. 29 June. Brussels: CEU.

DNV Consulting (2005), "Study on the impacts of possible European legislation to improve transport security", Final report: impact assessment. Report for European Commission, DG TREN. Report No. 4000 8032-6-2. Rev 2: final.

Dubecco, P. and Laporte, B., (2004), "Securing International Trade form Terrorism: The Financing Issue", WIDER Conference on Making Peace Work, June 2004, Helsinki, Finland.

ESPO (2004), "Response of ESPO to the draft report of the directive proposal on enhancing port security—COM (2004)76", Brussels, 22.11.2004.

ESPO (2005), "8 months after ISPS deadline: Success for EU ports", Press release. 15 March, Brussels.

ESPO (2006) Green Paper on Critical Infrastructure: ESPO's initial views. Available at *www.espo.be*, accessed December 2006.

Flemming, D.K., (1999), "A geographical perspective of the transhipment function", Paper presented at the International Association of Maritime Economists (IAME) 1999 Conference, September 1999, Halifax, Canada.

Hamada, R., (1969), "Portfolio analysis, market equilibrium and corporation finance", *Journal of Finance*, 24, 13–31.

Henstra, D. and Woxenius, J., (1999), "Intermodal transport in Europe", TRILOG report for the European Commission, 99NL/379.

Homan, A., (2006), "The impact of 9/11 on financial risk, volatility and returns of marine firms", *Maritime Economics and Logistics*, 8, 4, 387–401.

ILO, (2003), "Seafarer's Identity Documents Convention (Revised)", No. 185. Geneva: ILO.

IMO–ILO, (2003), "Code of practice on security in ports", Tripartite meeting of experts on security, safety and health in ports. Geneva.

ISO, (2004), "Ships and marine technology—maritime port facility security assessments and security plan development", ISO/PAS 20858. First edition, 7.1.2005, Geneva.

ISO, (2005), "ISO/PAS 28000. Specification for security management systems for the supply chain", First edition 15.11.2005. Geneva, Switzerland.

ISO (2006), "ISO/PAS 28001—Specification on best practices for implementing supply chain security, assessment and plans", Publicly Available Specification. March 2006, Geneva.

Johnston, V.R., (2004), "Transportation security and terrorism: Resetting the model and equations—epilogue", *Review of Policy Research*, 21, 379–402.

Juhel, M.C., (1998), "Globalisation, privatization and restructuring of ports", 10th Australasian Summit "Ports, Shipping and Waterfront Reform". December 1998.

Lewis, B.M., Erera, A.L. and White, III, C.C., (2006), "Impact of Temporary Seaport Closures on Freight Supply Chain Costs", Transportation Research Record, *Journal of the Transportation Research Board*, 1963, 64–70.

Ng A.K.Y., (2007), "Port Security and the Competitiveness of Short Sea Shipping in Europe: Implications and Challenges", in Bell, M., Bichou, K., and Evans, A. (eds), *Risk Management in Port Operations, Logistics and Supply Chain Security*, London: Informa, 303–333.

Notteboom, T.E. and Rodrigue, J.P., (2005), "Port regionalization: Towards a new phase in port development", *Maritime Policy and Management*, 32, 3, 297–313.

Notteboom, T.E. and Winkelmans, W., (2002), "Stakeholders relations management in ports: Dealing with the interplay of forces among stakeholders in a changing competitive environment", International Association of Maritime Economists (IAME) 2002 Conference, Panama, December 2002.

Pallis A.A., (2002), *The Common EU Maritime Transport Policy: Policy Europeanisation in the 1990s*, Aldershot: Ashgate.

Pallis A.A., (2006), "Institutional dynamism in the EU Policy-making: The evolution of the EU Maritime Safety Policy", *Journal of European Integration*, 28, 2, 137–157.

Pallis A.A., (2007), "EU Port Policy Developments: Implications for Port Governance", in: Brooks M.R. and Cullinane K. (eds), *Devolution, Port Governance and Performance*, London: Elsevier, 161–176.

Pallis, A.A. and Vaggelas, G.K., (2005), "Methods for measuring public and private benefits from port services provision: A comparative study", International Association of Maritime Economists (IAME) 2005 Conference. Limassol, Cyprus, June 2005.

Power, V. (1992), *The EC Shipping Law.* London: Lloyd's of London Press.

Rice, J.B. Jr. and Spayd, P.W., (2005), *Investing in Supply Chain Security: Collateral Benefits*, Cambridge, US: Massachusetts Institute of Technology.

Robinson, R., (2002), "Ports as elements in values-driven chain systems: The new paradigm", *Maritime Policy and Management*, 29, 3, 241–255.

Rotterdam Maritime Group (RMG) (undated), "Study on maritime security financing—Final report", TREN/05/ST/S07.48700. In cooperation with the Swedish Maritime Administration, Rotterdam: RMG.

Slack, B., (1998), "Intermodal Transportation", in: Hoyle, B.J., Knowles, R.D. (eds), *Modern transport geography*, (2nd edn) Chichester: Wiley, 263–289.

UNCTAD, (2004), "Container Security: Major initiatives and related international developments", Report by the UNCTAD Secretariat: February 2004, New York and Geneva: UN.

UNCTAD, (2006), "Maritime Security: Elements of an Analytical Framework for Compliance Measurement and Risk Assessment", UNCTAD/SDTE/TLB/2005/4. New York and Geneva: UN.

World Customs Co-Operation Council (WCO), (2004), "Resolution of the customs co-operation council on global security and facilitation measures concerning the international trade supply chain", June, Geneva: WCO.

CHAPTER 19

STRATEGIC RISK MANAGEMENT IN PORTS

S.N. Srikanth

Senior Partner, Hauers Associates, India

Ramesh Venkataraman

CEO-Asia, CurAlea Management Consultants, India

Abstract
Risk management has evolved from risk transfer or risk avoidance to one of proactively managing risk to create higher value. This approach sees risks as opportunities rather than threats. Good risk management is about enabling organizations take more and better informed risks. The emphasis today is shifting from management of financial and operational risks to management of strategic and reputation risks. The latter have much greater impact on the success or failure of an enterprise and the value that can be created for the stakeholders. Yet, the concept of risk management in ports continues to be overwhelmingly associated with operational risks such as security. This chapter makes the case for due consideration to be given to major strategic risks that ports face, including those linked to global economic trends, political instability, change in vessel sizes and competition from existing and new ports. This would involve the drawing up of a risk portfolio, with clear actions to build adequate safeguards that will help in bringing the risks to acceptable levels. The chapter also refers to the clear linkage that needs to be established between the safeguard actions identified and the business planning process to ensure that the safeguard actions get the priority they deserve.

1 STRATEGIC RISK MANAGEMENT

1.1 Risk and Profit

The word risk is often associated by the layman with luck or fate. Modern risk management, however, defines risk very differently, as something that can be influenced, something that we can profit from. The emphasis today is on proactively seeking out ways of taking acceptable risks. Profits are seen largely as a reward for successful and informed risk taking. This is a paradigm shift from the thinking that risks are associated only with losses.

1.2 Strategic and Other Risks

There is significant importance attached to risk management in ports today, but not quite enough to the management of what we may call strategic risks. Strategic risks can be defined as the array of external events and trends that can significantly impact an organization's growth trajectory and shareholder value (Adrian Slywotsky and John Drzik, *Harvard Business Review*, April 2005).

An analysis[1] of companies across 43 industries by the authors indicates that only around 30% of the shareholder value created by the corporation, and a port must be viewed as a corporation even if it may happen to be a department of the government, is constituted by its net asset value as appearing on its balance sheet while the remaining 70% is represented by the corporation's intangible assets such as business strategy, brands and goodwill. Risks related to the net asset value are unlikely to have a major impact on growth or shareholder value as the underlying assets can be secured through a variety of hedging techniques, and in case the risks materialize these assets can also be reinstated. To the contrary, risks related to the intangible assets have the potential of impacting the growth prospects of the firm significantly. Other noteworthy features of risks facing intangible shareholder value are that they are often inter-linked, complex and difficult to manage. Strategic risks, therefore, are largely related to the intangible assets of a firm. The focus of this chapter is on these risks.

1.3 Risk Management as an Opportunity

Traditional responses to risk consist of avoidance, transfer and control. For example, a port management company may opt not to venture into geographies with high security risks. A state-run port that mandates a minimum throughput guarantee when privatizing a terminal would be transferring the risk of volume fluctuations to the private operator. And a code such as the ISPS is essentially an attempt to control security risks. Modern corporations have progressed beyond these traditional risk responses to the proactive management of risks. The management of risks in general and strategic risks in particular, while embracing the components of avoidance, transfer and control, also sees risk as an *opportunity.* corporate social responsibility—for example, commitment to sustainable development or preservation of the environment—could be seen as a threat that erodes the bottom-line. Progressive corporations, however, view such commitments as opportunities to enhance shareholder value. Recyclable packaging, eco-friendly hotels and energy saving computers are some examples of the resultant response. Of course, this is not an easy task as one cannot take risks blindly. One has to take better informed risks, risks that are acceptable and within the risk appetite of

[1]. Analysis of companies listed on the NYSE across 43 industries comparing the market capitalization with the Book Value of the shares.

the corporation. The challenge of strategic risk management is thus to empower businesses to take more and better informed risks and to successfully manage them to maximize shareholder value.

1.4 Types of Strategic Risks

The different kinds of strategic risks are discussed below with examples. No attempt has been made by the authors to make the list comprehensive.

Risk type	*Examples of risk*
Macro-economic risks	Economic instability, slow down in GDP growth, hyper-inflation
Political risks	War, political instability
Industry risks	Excess capacity creation, tariff control by the state
Competition risks	New ports likely to open in the vicinity, expansion of existing nearby ports, price wars
Technology risks	Obsolete technology leading to competitive dis-advantage, technology mismatch with emerging vessel and cargo traffic mix
Customer risks	High concentration of business with a few shipping lines or a few large cargo interests, inadequate understanding of customer priorities
Environmental risks	Natural disasters, adverse change in land use pattern surrounding the port, action from NGOs against a new port project

Table 1: Risk Type with Examples

2 STRATEGIC RISK MANAGEMENT PROCESS

The process of managing strategic risks involves a series of key activities.

2.1 Risk Identification

This involves the identification of the key risks that could impact the organization in the near to medium term. This is normally achieved through brainstorming sessions among senior managers that are organized by the risk management co-ordinator, who presents an initial risk universe drawn from diverse sources of information as well as from interviews with board members. The brainstorming results in a short list of risks for further evaluation.

2.2 Assessment of Impact and Probability

This step involves the assessment of the possible impact and the probability or likelihood of occurrence of the risks identified. The objective here is to arrive at a robust judgement on the materiality of the risk rather than to achieve an accurate quantification. A reasonably accurate evaluation of the financial impact of the risk will, however, help in prioritizing the risk management plan.

2.3 Evaluation of Existing Safeguards

This is a key activity that involves the evaluation or assessment of the safeguards that are currently in place to manage the risks identified.

2.4 Net Risk Assessment

The next step is to assess the net risk level after taking into account the existing safeguards. This helps in determining whether the net risk level is acceptable or not in relation to the risk appetite of the corporation. The risk appetite varies between organizations and also between geographies. For instance, high employee turnover may be an acceptable risk in the IT industry in India where demand vastly outstrips supply. Even within the same industry, the risk appetite may vary between enterprises based on factors like the management philosophy, ownership structure, stage in the life cycle of the firm, etc.

2.5 Development of the Risk Management Action Plan

Where the net risk level is found to be unacceptable, further safeguards need to be planned to bring the risk to an acceptable level. This step is at the heart of strategic risk management. Even where the risk is at an acceptable level, further safeguards might be planned to strengthen its management.

2.6 Integration into the Business Planning Process

The risk management action plan, to be effective, needs to be integrated with the business planning process. This will require the key safeguard actions planned to be incorporated in the business targets, budgets and score cards.

The strategic risk management exercise would normally result in a risk grid or portfolio matrix that depicts the risk profile of the corporation in a summarized form. The grid would include all risks that merit monitoring by the board at least twice a year to ensure that changes in the portfolio are reflected on a timely basis.

3 CASE STUDY: PORT X

We would like to walk you through the construction of a risk portfolio for a port we had occasion to study. Let's call it Port X for this exercise, as we are unable to reveal the name of the port for reasons of confidentiality. Certain specifics have also been altered for the same reason.

3.1 Background Information

Located in a developing country, this port handles somewhat less than 100 million tonnes of cargo a year. Of the three most important customers of Port X, two are importers of coal and together they account for 25% of the traffic through the port. The third and the largest—a government-owned refinery that receives crude oil through the port—accounts for another 25%. Port X is government-owned and operated. The workforce is excessive and the wage bill exorbitant. Militant labour unions force frequent work stoppages. The government has a significant say in labour management at the state-run ports in view of the strong political affiliations of the trade unions, making retrenchment plans difficult to implement. The current wage agreement with the workers will expire in a year's time and the unions are expected to demand a steep increase in wages. It is feared that labour unrest will grow as the time for the new wage agreement draws closer.

Port X is in a cyclone prone area and faces the constant threat of a natural disaster. However, it has reasonably good crisis management systems and a trained team to tackle such emergencies. The port has inadequate draught and ageing equipment, and the assets are largely depreciated. Equipment productivity is poor. The port currently handles small container feeder vessels. With vessel sizes increasing the mainline vessels of today may become the feeders of tomorrow with draughts too deep for Port X and requiring advanced facilities for loading, discharge and evacuation. If Port X does not upgrade it may lose the container trade if current trends in vessel size continue.

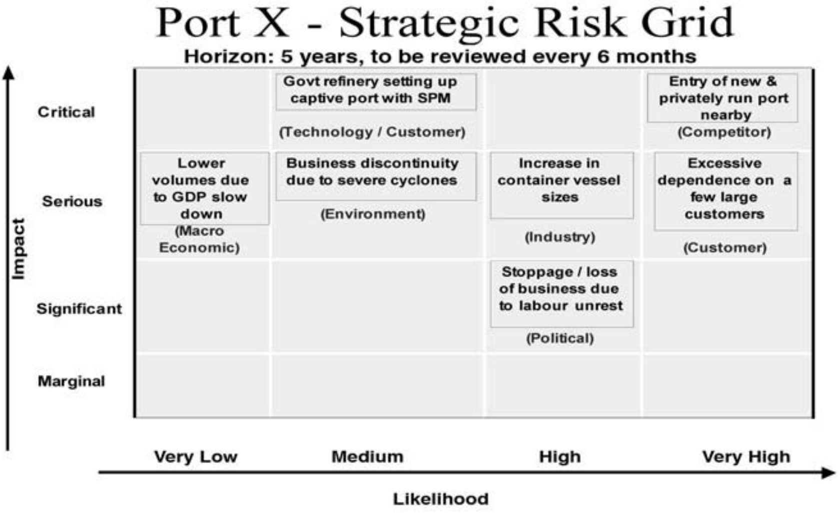
Importantly, a new private port Y is under construction barely 150 kms to the south. The new port will have deeper draught than Port X and will be capable of handling larger vessels. Mechanized handling systems are also being proposed. Being a private operation, the port is expected to be run more effectively, with higher productivity levels than in Port X. The management of the private port will have greater flexibility in regard to tariffs and should be able to respond swiftly to attract and retain users, unlike the management of Port X. The private port management has been aggressively wooing the two large coal importers, currently users of Port X, with low tariffs, modern infrastructure, preferential berthing facilities and other incentives. The government refinery, the largest customer of Port X today, is toying with the idea of building a captive port closer to the refinery and with a single point mooring (SPM). Needless to say, this would mean a huge loss of business to Port X.

The economy is growing briskly in the hinterland of Port X and an economic slowdown seems unlikely in the immediate future. However, if this happens Port X will be affected.

3.2 Port X: Strategic Risk Grid

The strategic risks faced by Port X are represented in the grid below. Each risk is assessed in terms of likelihood and impact and categorized by type of risk. The safeguards that the port presently has against each of the risks in the grid and the resultant profile of the risk are given below. Exposures to the risks are classified as unacceptable with urgent action required, acceptable but requiring further action and acceptable with periodic monitoring required.

Port X is now ready to meet the challenge of strategic risk management, of converting strategic risks into opportunities. If existing safeguards are inadequate and render a risk unacceptable, additional safeguards are proposed to make it acceptable within a specified time frame. Taking such informed risks is expected to translate into opportunities for Port X to enhance shareholder value.



Port X - Strategic Risk Grid

Horizon: 5 years, to be reviewed every 6 months

Impact	Very Low	Medium	High	Very High
Critical		Govt refinery setting up captive port with SPM (Technology / Customer)		Entry of new & privately run port nearby (Competitor)
Serious	Lower volumes due to GDP slow down (Macro Economic)	Business discontinuity due to severe cyclones (Environment)	Increase in container vessel sizes (Industry)	Excessive dependence on a few large customers (Customer)
Significant			Stoppage / loss of business due to labour unrest (Political)	
Marginal				

Figure 1: Strategic Risk Grid

Risk	*Existing safeguards*	*Profile of risk*
Entry of new privately run port nearby	None	Exposure unacceptable, urgent action required
Excessive dependence on a few large customers	Two-year contract with largest customer expiring 14 months from now	Exposure unacceptable, urgent action required
Government refinery's plans to set up captive port with SPM	– Long-term contract with refinery valid for another two years – Discussions between oil and shipping ministries with the latter arguing for the continued use of port X	Exposure unacceptable, urgent action required
Stoppage/loss of business due to labour unrest	Detailed negotiation strategy in place	Exposure acceptable, but needs further action
Volume drop due to GDP slowdown	None	Exposure acceptable, but needs further action
Increasing container vessel sizes	None	Exposure unacceptable, urgent action required
Business discontinuity due to severe cyclones	– Detailed crisis management plans in place – Regular monitoring of weather forecasts and trends through the Met department	Exposure acceptable, monitor periodically

Table 2: Strategic Risks—Existing Safeguards and Risk Profile

Risk	*Proposed safeguards*
Entry of new privately run port nearby	– Privatize coal terminal to achieve higher efficiencies and competitiveness. Private operator to modernize terminal and take over existing labour on present scales. Minimum throughput to be guaranteed by private operator – Apply to government for budgetary support for deepening draught to handle larger vessels – Negotiate three to five year contracts with the two coal customers with volume based discounts – Institute competitor tracking mechanism
Excessive dependence on a few large customers	– Short term: Offer contracts with volume based tariffs for the top six customers other than coal – Medium term: Broaden customer and cargo base and reduce dependence on the coal customers to 15% of total volumes
Government refinery setting up own port with SPM	– Lobby with government to retain refinery business – Offer to construct SPM at port X or enter into joint venture with the refinery for the proposed captive port
Stoppage/loss of business due to labour unrest	– Institute voluntary retirement scheme ahead of settlement
Volume drop due to GDP slowdown	– Outsource activities such as pilotage and dredging to reduce fixed costs and lower the break-even level
Increasing container vessel sizes	– deepen draught at container berths to 12.5 metres – invest in modern handling equipment – explore other ways of increasing productivity – build additional container stations off-dock – monitor new building sizes regularly
Business discontinuity due to severe cyclones	– Institute early warning systems – Test crisis management plan twice a year

Table 3: Converting Strategic Risks into Opportunities

The strategic risk management action plan for Port X describes each risk in detail, lists the current and proposed safeguards and provides a detailed action plan, indicating the individuals vested with the responsibility for carrying out the actions. It also specifies time deadlines for each action and sets a target date for the level of risk to become acceptable. An example of the risk management action plan for one of the risks is given below.

Short title. *Competitive threat from new privately run port nearby*

Risk definition:

The new private port under construction at Y will be operational in the next 30 months. The port will pose a serious threat of shift of cargo and customers due to:

ability to handle larger vessels;
better equipment;
faster turnaround time;
greater flexibility in pricing;
potential targeting of our two largest customers with attractive pricing.

Our initial estimates show that there could be a potential risk of losing 25% of cargo as well as an overall erosion of operating margins by 35%.

Current safeguards:

Two-year contract with the largest customer A (coal) that expires in 14 months.

New/improved safeguards needed:

Negotiate with second coal customer (B) to enter into a five year contract. Extend contract with customer A by another three to four years.

Negotiate with the other large customers to enter into three to five year contracts, with volume based discounts to be offset by benefits from higher capacity utilization.

Privatize operations of coal terminal on revenue sharing basis. The private operator to modernize equipment, take over coal terminal workers on present pay scales and to provide minimum throughput guarantee

Apply to government for budgetary support for deepening draught to facilitate handling of larger vessels.

Draw up action plan for broadening customer base in the next 24 months to increase tonnage to 130 million tonnes.

Explore potential of tie up with inland dry ports to capture cargo at source.

Institute comprehensive competitor tracking mechanism to closely track the cost structure and evolving business model of the new port. Also study impact of other private ports that have commenced in the last two years on the industry dynamics and price structure.

Draw up action plan for improving turnaround time by 30% by June 2007.

Detailed Action Plan

Action	*By*	*Deadline*
Initiate negotiations with large customers and submit initial proposal to the Board	AS	Jan 07
Finalize contract with customers A and B	AS	March 07
Finalize contracts with at least five out of 10 top customers	AS	June 07
Present action plan for throughput improvement to Board	PH	Dec 06
Draft proposal for tie up with two inland ports	KJ	Dec 06
Quarterly competitor tracking mechanism to be started	SK	Jan 07
Technical proposal for improving turnaround with capital cost estimates to be submitted	PH	June 07

Assessment of risk:

Impact?	Critical
Likelihood?	Very high
Risk profile	Unacceptable and required immediate attention

With the implementation of the above actions, when will the level of risk become acceptable? 12 months

Figure 2: Strategic Risk Management Action Plan

Finally, the risk management plan is integrated into the planning process of Port X. This is necessary for the plan to be recognized as an essential part of the strategy of Port X and to secure the support of the entire organization. The integration involves the steps described below.

- Key actions planned to be reflected in the annual plans of the respective functions.
- All critical actions to feature in the balanced score cards of the organization
- Capital and revenue budgets to include the outlay on the risk management actions.
- All critical risk management actions to feature in the group and individual targets and thereby linked to the performance bonuses.

4 CONCLUSIONS

A successful strategic risk management programme needs some key enablers:

- senior management buy-in and sponsorship of the programme;
- active involvement of line managers in the process;
- rigour in risk identification to ensure that the net is spread wide to capture all relevant risks;
- inculcation of the risk management philosophy in the corporation rather than treat this as a one-off exercise, with integration of the initiative with the other business processes;
- effective follow-through and completion of the safeguard actions planned;
- capture and review of learnings, to improve and customize the process according to the needs of the corporation; and
- adequate resourcing of the risk management activity, with clear ownership and appropriate expertise.

REFERENCES

Adrian J. Slywotsky and John Drzik, *Countering the Biggest Risk of All.* Harvard Business Review, April 2005.

Thomas L. Barton, William G. Shenkir and Paul L. Walker, *Making ERM Pay Off: How Leading Companies Implement Risk Management.* Financial Times/ Prentice Hall.

Protiviti, *Guide to Enterprise Risk Management*: *www.protiviti.com*

James Lam, *ERM: From Incentives to Controls.* Wiley Finance

Peter C. Young and Steven C. Tippins, *Managing Business Risk: An organization-wide approach to Risk Management.* American Management Association.

This page intentionally left blank

CHAPTER 20

PORT SECURITY AND THE COMPETITIVENESS OF SHORT-SEA SHIPPING IN EUROPE: IMPLICATIONS AND CHALLENGES

Koi Yu Adolf Ng

Center for Maritime Economics and Logistics, Erasmus University, Rotterdam, The Netherlands

Abstract

Until the early 1990s, short-sea shipping (SSS) was widely regarded as a forgotten component within the European transportation system, with freight transportation within Europe dominated by unimodal transportation means, notably road vehicles. Since then, however, with changes in circumstance, SSS has experienced a change in fortune, with the EU intended to alter the sector's image from being slow, worn-out and poor quality to being efficient, high quality and competitive which can lead to a substantial modal shift from unimodal road vehicles, as well as forming an integral part of an integrated multimodal logistical supply chain within Europe complementing the objectives of trans-European transport network characterized by cohesion, integration and intermodality. In this sense, nodal efficiency i.e. port becomes a critical component in deciding whether such ambitious objectives can be achieved, especially given the existence of serious bottlenecks in many European ports as identified by the EC, e.g. worn-out port infra- and super-structure, non-flexible working hours, lack of IT adapted to SSS, congestion, complicated power relation within ports and poor hinterland connections, etc. Nevertheless, throughout the years, it is interesting, and indeed surprising, to found that the introduction of port security, which is likely to pose significant implications on port efficiency and thus SSS's competitiveness, remains a largely untouched topic, as reflected by the EC approach which largely regards port security and SSS as completely independent and unrelated projects. Recognizing such deficiency, this chapter aims to address this gap by investigating the potential implications of port security measures on the competitiveness of European SSS and providing a critical review on the current EC approach on the issue, as well as discussing the challenges ahead. By rekindling their overlapping relation, it is anticipated that this chapter will play a contributory role in the development of multimodal freight transportation in Europe.

1 INTRODUCTION

Until recently, short-sea shipping (SSS) was largely a forgotten component within the European transportation system. Intra-European transportation, especially freight, was dominated by unimodal means, notably road vehicles. Nevertheless, with changing circumstances since the mid-1990s, SSS has experienced a change in fortune. Attention to the sector increased and the EU intended to alter SSS's image from being slow, worn-out, poor quality and only for transporting low value large bulk products to being efficient and competitive which would form an integral part of the future integrated multimodal logistical supply chain which complements the objectives of trans-European transport network (TEN-T).

Since SSS alone cannot provide door-to-door services, the promotion of SSS also implies the development of multimodal transportation. In this sense, nodal efficiency, i.e. the port, becomes an extremely critical component in deciding whether the EU's objectives in promoting SSS can be achieved. Given the existence of various obstacles and challenges in European ports, it is a very challenging task for the EU to enhance them to an extent that would enable the SSS-included intermodal system to compete effectively with other means. While various traditional problems in ports, e.g. worn-out port infra- and superstructure, non-flexible working hours, lack of IT adapted to SSS, congestion, complicated power relation within ports and poor hinterland connections, etc. (COM (2006) 380 final) are yet to be solved, recently, the issue of port security has further complicated the issue.

Despite such significance, however, it is surprising to see that, while the introduction of port security measures is likely to pose significant implications on port efficiency and thus SSS, such overlapping relations between the two issues remains largely untouched, despite the fact that both issues are hot topics within the EU agenda, as reflected by the its approach which largely regards port security and SSS as completely independent and unrelated projects. Recognizing such deficiency, this chapter aims to shed some light on the implications of port security on the competitiveness of SSS in Europe, as well as discussing the challenges ahead.

However, before illustrating the implications of port security on SSS, it is necessary to provide readers with a comprehensive understanding of the development of European SSS as well as the critical role for port efficiency in deciding SSS's competitiveness. With such understanding, this chapter is structured as follows. Following this introductory section, an analysis will take place on the development of European SSS, as well as the role of ports in deciding SSS competitiveness. Based on such understanding, the implications for port security on the competitiveness of SSS, as well as the problems and challenges ahead, will be discussed.

2 EVOLUTION OF EUROPEAN SHORT-SEA SHIPPING

SSS is far from a homogeneous concept. Generally speaking, it can be subdivided into various categories, e.g. freight vs. passenger, feeder vs. purely intra-European traffic, etc. Analysis of this chapter follows the definition proposed by the EC which defined SSS as (the focus of this chapter focuses on freight transportation):

> "The movement of cargo and passengers by sea between ports situated in geographical Europe or between those ports situated in non-European countries having a coastline on the enclosed seas bordering Europe" (COM (1999) 317 final).

Although the development of SSS can be dated back to 1985 when the EC proposed the application of freedom in providing shipping services in intra-EU and cabotage maritime trades (Pallis, 2002), it did not become a serious topic until 1995 when the EC published its first Communication on the sector. Indeed, during the post-war period, SSS was largely ignored by European statesmen, as indicated by the fact that neither the Treaty of Rome (signed in 1957) nor the Common Transport Policy (CTP) mentioned anything concrete about the sector's development (Nijkamp *et al.*, 1994). Intra-European freight transportation was dominated by unimodal road vehicles and shipping was largely relegated to serve peripheral regions, usually due to geographical restrictions, e.g. Sardinia (Italy), Corsica (France), the Greek archipelago, etc.

Several reasons explained such ignorance during this period. First, the administrative complexity of SSS had made the development of the sector extremely difficult. The existence of poor supporting infrastructure, especially ports, had resulted in bottlenecks and raised their generalized costs of usage to shippers; not helped by the industry's protectionist nature with numerous restrictions on cabotage which further depreciated its reputation (Cholmoudis and Paillis, 2002). According to the EC Communication (COM (1999) 317), several critical factors such as time, flexibility and frequency were of unacceptably low standard and shippers often found other alternatives, especially unimodal road vehicles, more attractive to use. As a consequence, SSS often faced fierce competition from other unimodal transport modes. For example, between Sweden and the rest of Europe, most general cargoes were carried by trucks and SSS often ended up carrying low value bulk products, not helped by the completion of several projects favouring road vehicles, like the English Channel tunnel and the bridge connection over Öresund (opened in 1994 and 2000, respectively). While the former ensured that cargoes can be transported to/from the UK by road, the latter caused all maritime services between Helsingør and Helsingborg to shut down.

Also, inefficiency of SSS further ruined its own reputation and discouraged potential users from investigating its use (Peeters *et al.*, 1995). This was not helped by traditionally diverse views on maritime transportation among the EU Member States, as some favoured stronger links between government and industry while others adopted a more *laissez-faire* approach, leading to the adoption of a common understanding in a generic solution in the development of SSS (and multimodal transportation) extremely difficult (Urrutia, 2006). Indeed, according to Baird's (2004) estimation, if nothing was done, by 2013, unimodal road vehicles used in freight transportation in Europe would grow by 60%.

However, since the mid-1990s, SSS has experienced a change in fortune. For example, the EC's Transport White Paper (COM (2001) 0370), identified SSS as a key mode, which with appropriate links to rail and road could provide an alternative to road-based transport. Thus, attention on it has increased, as characterized by the publication of the first EC Communication on SSS (COM (95) 317), while scholarly works related to this topic also started to be published (for example, see Peeters *et al.*, 1995). There are several reasons to explain such an attitude change. First, it was due to liberalization. By 2005, the opening up of national markets for coastal shipping had largely been completed. Albeit some tough negotiations, based on the regulatory packages of 1986 (Regulations 4055/96) and 1989 (Official Journal C073) which proposed to provide maritime services within the EU freely, maritime cabotage between EU Member States began to liberalize in the 1990s, except a few island–mainland connection routes in the Mediterranean, e.g. Greece, Spain, France, etc., with open market access and prices being negotiated freely. Liberalization had definitely created a more favourable circumstance for SSS to compete.

Also, the signing and enforcement of the Maastricht Treaty in 1992 and 1993, respectively accelerated the requirement of a more comprehensive policy than the CTP, resulting in the introduction of TEN-T. Its objective was to create a system consisting of highly efficient multimodal logistical supply-chain networks within the EU characterized by interoperability, interconnectivity and intermodality. Given the relatively small size of EU Member States and given that shipping alone was inaccessible to inland regions and thus intermodalism often existed, the promotion of shipping actually fitted the bill very well which also encouraged the overall improvement of transport infrastructure, hinterland connection and administrative systems. On the other hand, intra-European transportation before the 1990s, which was characterized by automobile-dominated scene, did nothing to enhance the EU's objectives of creating free and fair competition within the continent, nor did it encourage a balanced modal-split scenario and obviously, the *status quo* was not preferred. Thus, such an initiative is anticipated to boost the overall quality of the European multimodal logistical supply chain.

Environmentally, despite some concerns like ballast water as well as sulphur and nitrogen oxides (Kågesson, 1999), many studies suggested that SSS-included intermodal transport were more environmentally friendly and ships, in general, consumed fewer fossil fuels per unit of cargo being carried (for example, see Nijkamp *et al.* (1994), COM (1999) 317 and the European Conference Ministers of Transport (ECMT) (2001)). On the other hand, despite its flexibility, the sustained use of road vehicles had caused continuous negative consequences like traffic congestion and accidents. This was especially true in northern Germany, the region which traditionally hosted some of

Europe's major urban and industrial centres like the Ruhr district and the meeting point between Scandinavia, Western and Eastern Europe. As the EC (2002c) pointed out:

> "To accommodate anticipated future growth in freight traffic without putting further pressure on Europe's already congested road network, maritime transport will assume an ever more important role. The development of SSS is a central element of the strategy for achieving a clean, safe and efficient European transport system."

As the EC believed, the negative externalities can be relieved only through a substantial modal shift. However, while air transport was out of the equation due to high costs, rail demonstrated weaknesses similar to road, e.g. difficulty in expanding capacity, high sunk costs, connectivity between national borders, etc., leaving shipping as the only feasible option.

Finally, the opening of Eastern European countries since the 1990s signified a substantial increase of coastal length opened to EU-flagged vessels. With the considerable number of states with maritime interests joining the EU in 2004, the promotion of SSS was regarded as a catalyst enhancing the EU's integrity. In fact, priority has already been given to shipping projects which could accelerate the integration of new members, notably with the increasing lending mandate from the European Investment Bank (EIB) to Baltic maritime projects, amounted to €8.7 million between 2002 and 2006 (EIB, 2003).

Indeed, the above analysis clearly indicates that the promotion of SSS was not just only economically motivated, but also environmentally and, more importantly, politically driven. The EC made clear that it aimed to alter SSS's image from being slow, worn-out, poor quality and only for transporting low value large bulk products to become efficient and environmental-friendly, forming an integral part of the future integrated and sustainable European transportation system (COM (1999) 317 final). However, mainly due to its negative image and the competitiveness of unimodal road vehicles, without the EU's initiatives, SSS had little chance of competing successfully.

To facilitate support, the EC included SSS as TEN-T priority projects of European interests. In 2003, the EC presented a programme promoting SSS (COM (2003) 155 final) with several planned and ongoing actions proposed in accordance with the measures outlined in the EC's Transport White Paper (COM (2001) 0370). The programme's objective was to provide a comprehensive framework in promoting the sector with the concept "motorway of the sea" (MS) being introduced. A MS project should fulfil the following objectives:

- to contribute to the objectives of a sea motorway;
- to improve the performance of a port on sea motorway; and
- to fully assess the risks and impacts of the project, with sound financial backup.

Based on the above criteria, the EC had identified four MS, of which all are expected to start operation as early as 2010, as follows:

- motorway of the Baltic Sea (MS Baltic);
- motorway of the sea of Western Europe (MS Western Europe);
- motorway of the sea of SE Europe (MS SE Europe); and
- motorway of the sea of SW Europe (MS SW Europe) (Figure 1).

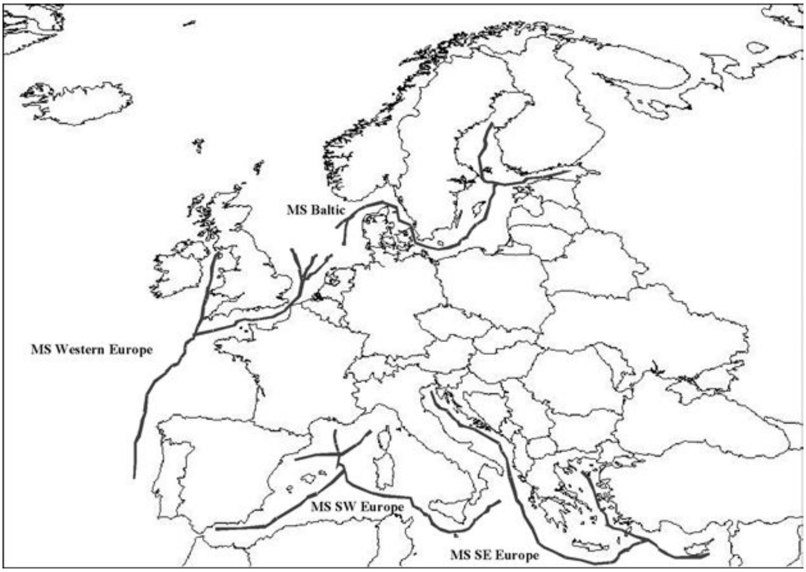


Figure 1: Motorways of the Sea as Identified by the EC (source: EUROPA, 2007)

Through two EC Communications—Communications on Short Sea Shipping (COM (2004) 453 final) and Proposal for Regulation to establish Second "Marco Polo" Programme (COM (2004) 478 final), various legislative, technical and operational actions have also been introduced to increase the role of SSS and the Marco Polo programme in supporting the development of SSS-included multimodal supply chain within Europe. Legislatively, the European Council of Ministers and the European Parliament adopted Directive 2002/6/EC on reporting formalities for vessels arriving in and/or departing from ports within the EU Member States. The Directive simplified the administrative procedures involved by introducing five standard forms (down from the initial 50). Also, multimodal loading units would be standardized and harmonized, while the progress on the development of MS would be closely monitored. Technically, the EU took several initiatives aiming to boost the potential competitiveness of SSS against other modes, notably unimodal road vehicles. These initiatives included the preparation of guidelines to custom procedures, approximation of national applications, identification and elimination of obstacles and research and the computerization of the European

Community's custom procedures. Finally, operational steps would also be taken to complement the programme, including action in creating one-stop offices for administrative and customs formalities so as to enhance interoperability and intermodality within the multimodal supply chain.

Its poor reputation had ensured that publicity work would be highly important for SSS. The last few years have witnessed the opening of short-sea promotion centres (SSPC) in major European cities within EU with the aim of marketing SSS as a decent alternative to unimodal road vehicles and providing concrete information on SSS to stakeholders within the EU, as well as collecting reliable statistical data about the sector (which had been, until recently, lacking). Finally, other EC initiatives involved the harmonization of regulations at the Community level in accordance with the action programme as outlined in the Transport White Paper (COM (2001) 0370), including the conditions in obtaining boat-master certificates and vessels' technical requirements. In particular, the EC proposed that a single system of technical requirements should be introduced to all marine surfaces under the EU's jurisdiction. The EC would also prepare practical guidelines on customs procedures applicable to both SSS and ports within the EU (COM (2006) 380 final).

As mentioned, with its inability to provide direct door-to-door services, the promotion of SSS was equivalent to promoting multimodal transportation. In this sense, it was not difficult to understand that the success of SSS actually greatly depended on whether the whole multimodal supply chain could operate with high frequency, regularity and interoperability, notably on how efficiently cargoes could be transferred between different modes, which implied the criticality of nodal efficiency along the supply chain, i.e. port efficiency.

3 THE ROLE OF PORTS IN SHORT-SEA SHIPPING'S COMPETITIVENESS

In 2004, the EC published a Communication on SSS (COM (2004) 453 final) reviewing the progress of promoting SSS and identified the following continuing major obstacles:

- incomplete integration in the intermodal supply chain;
- perception of being an old-fashioned industry;
- complex administrative procedures; and
- linkage to port efficiency levels.

From the above, it is not difficult to understand that these obstacles were closely linked to port inefficiency, with cargoes being unable to transit smoothly between different modes along the multimodal supply chain. As noted by the EC (2004c):

> "The EU's seaports are vital to the competitiveness of its internal and international trade, and as links to its islands and outlying regions . . . [with] the

> development of SSS . . . as the EC White Paper [published in 2001] makes clear, this will require an increase in the capacity and efficiency of ports and port services, as well as improved intermodal connections between ports and inland transport networks."

Such significance could be reflected by the fact that, in a typical SSS-included multimodal door-to-door service in Europe, about 56% of the total costs were related to loading/unloading in port (De Monie, 2003). Such claim was further strengthened by a study conducted by Napier University (2002), entitled "UK Marine Motorways Project" investigating the feasibility of introducing intermodal ro-ro service between southeast England and Scotland. The study found that, while sea leg cost was cheaper than road vehicle, the overall competitiveness of SSS-included door-to-door service was jeopardized by an extra 40% cost arising from port haulage and connections between port and origin/destination. Overall, SSS-included door-to-door service was estimated to be 15–20% higher than unimodal road vehicles.

Due to similar reasons as discussed before, until the early 1990s, like SSS, ports were another forgotten component within European transportation, as exemplified by the fact that, between 1993 and 1998, out of more than €36 billion of transport loans approved by EIB, only merely 2% was related to port projects (Turró, 1999). Nevertheless, with the increasing importance of SSS on the EU agenda, ports had also experienced a better change in fortune (Bekemans and Beckwith, 1996), as the EU statesmen started to recognize the need of efficient ports in order to realize the TEN-T's ideals of cohesion, integration and intermodality of the European transportation network. According to the Communication COM (1999) 317 final, ports should be reformed so that they could operate commercially while free and fair port competition and the user-pays principle must also be ensured simultaneously. Also, supported by a liberalized environment, ports should set up separate terminals with dedicated and specialized facilities for SSS so as to facilitate their integration into the multimodal supply chain.

However, these objectives could only be achieved through a comprehensive reform programme of the sector coordinating ports and governments of various levels. Thus, in the same Communication (COM (1999) 317 final), it was proposed to establish a framework with sound technical and operational solutions in port improvements, including information exchange between ports and shipping lines and the removal of unnecessary costs induced from ports. Also, given the ports' increasing criticality in deciding the efficiency of logistical supply chains (Heaver, 2002), including SSS-included ones, it implies that the objectives of TEN-T would be unlikely to succeed without inscribing ports into the project. To address this, the Communication had redefined the ports' concept from a simple sea–land interface to "a critical distribution centre along the logistical supply chain in Europe, mobilised by rapidly changing political and economic development" (COM (1999) 317 final) and priority would be given to port projects which were dedicated to the development of SSS-included multimodal supply chain within the EU.

The EC also took an initiative to address the need for harmonization of the charging principles across European ports (Strandenes and Marlow, 2000). The first step in this direction had been taken with the Green Paper, *Sea Ports and Maritime Infrastructure* (COM (97) 678 final), and the EC's White Paper, *Fair Payment for Infrastructure Use: a Phased Approach to a Common Transport Infrastructure Charging Framework in the EU* (COM (1998) 466 final). The EU proposed a pricing system based on short-term marginal social costs (including external costs), i.e. all users should pay for the costs they impose on using the infrastructure, including ports. Under this system, port charges should be set in accordance with real marginal social costs, ensuring cost recovery of new investments in addition to operating and external costs, thereby ensuring fair competition and possibly more strategic port pricing system (Strandenes and Marlow, 2000).

As part of the strategy to ensure that future port planning can be undertaken in a more "European" way, the Port Package had been tabled to the European Parliament in 2001. The Port Package consisted of various generic guidelines related to port service and encouraging port competition (the so-called "EU standard"), e.g. transparency regulations for subventions to port and/or its enterprises, state-aids to ports, advertisement of state-owned surfaces in ports, transition and remuneration regulations, the liberalization of port services by permitting shipping firms to appoint independent contractors to load/unload vessels and ending terminal operator monopolies on cargo stevedoring, etc. Finally, the appointment of a Directive on port service market access was proposed by the EC (COM (2001) 35 final), with the objective of improving port efficiency and reducing costs of certain port services.

Despite such initiatives, the success of SSS was still rather mixed. Although, in terms of tonne-kilometres, SSS within the EU maintained a share of 43%, 39% and 41% of intra-European total freight movement and growth in 1990, 2000 and 2002, respectively (EC, 2004), between 1995 and 2004, SSS and road transport within EU-25 grew by 32% and 35%, respectively. Within the same period, the share was 39% and 44%, respectively (COM (2006 380 final), indicating that preference for road vehicles was still very much prevalent. Indeed, many ports, especially lesser ones, still faced considerable obstacles in terms of capacity constraints and complicated administrative procedures and bureaucracy. In the mid-1990s, while ships spent about 60% of their total time in ports (COM (95) 317), throughout the following decade, this situation did not witness significant improvement, often due to the snail-paced reforms in many ports. While highlighting the importance of port efficiency on multimodal transportation in Europe was initiated since the mid-1990s, until mid-2006, 12 of the 22 identified bottlenecks[1] of European SSS-included multimodal supply chain as identified by the EC were still port-related, e.g. worn-out port infra- and superstructure, non-flexible working hours, lack of IT adapted to SSS, congestion, complicated power relation

[1] Here country-specific bottlenecks were excluded.

within ports and poor hinterland connections, etc. (COM (2006) 380 final). Until very recently, in Italian ports, cargoes were still not allowed to discharge until all paperwork had been completed (EC, 2004c). On the other hand, in many ports, there were no full-time port-based customs officers but at the same time vessels were not allowed to unload until customs officers attended the ship, notably Mediterranean and Baltic ones. Another typical obstacle was pilotage, which was obligatory in some ports (notably Polish ports) even if the shipmaster was certified to execute the duty alone. Not surprisingly, inefficient ports continued to haunt the competitiveness of SSS, especially against unimodal road vehicles. In fact, in its recent Communication, even the EC admitted that SSS, and especially port efficiency, had not improved smoothly and substantial future work would still be needed (COM (2006) 318 final).

Also, a "European" and "multimodal" view in port planning was still lacking. Many port authorities were more interested in providing services demanded by port customers rather than customers with greater interests in multimodal logistical supply chain (Peeters *et al.*, 1995). Ports were often regarded as strategic assets with the persistence of local interests, not helped by the fragmented nature of port systems in administration and management, especially since port state control and the relation between EU Member States and the EU on port affairs were still largely based on the Paris Memorandum of Understanding (MoU), signed in 1982 by 14 countries (including nine EU Member States), which stated that intergovernmental cooperation was voluntary and port regulations were largely outside the EC treaty umbrella (Urrutia, 2006). Thus, in accordance to the Paris MoU, national and regional authorities were not obliged to abide with any common rules on port matters. In a certain sense, this had distorted free and fair port competition and in direct opposition with the objectives laid down by the Green Paper on Sea Ports and Maritime Infrastructure (COM (97) 678 final). The most notable example was the issue of state-aids, of which until recently no EU rule regarding state-aids on ports existed. The EC's Transport White Paper stated:

> "State-aid rules can have application in the field of investment in infrastructure and so eliminate distortions where the provision of public finance favours certain undertakings or the production of certain goods. [. . .] It is, therefore, necessary to define comprehensively where public finance for infrastructure favours particular enterprises in a way which distorts competition and affects trade between [EU] member states" (COM (2001) 0370).

While the European Parliament endorsed the White Paper's opinion and made clear that it considered state-aids on ports as anti-competitive, on the other hand, widely known as a capital-intensive industry, it was argued that ports, especially lesser ones, require substantial financial support to enable them to become effective enough to contribute positively to the competitiveness of SSS-included intermodal transport in Europe, which in turn pressurizes the EU to undertake financial initiatives. Given such dilemma, although a lot of discussions about supporting ports took place, as reflected by the existence of numerous Communications, one could witness that financial support for ports by the EU existed largely in name only, as exemplified by the fact that, until 2003, EIB was not involved in financing any port projects directly related to SSS-included multimodal supply-chain improvements (EIB, 2003). The EC was often caught between the chicken-and-egg paradox where pressure for financial support increased but at the same time not violating its own principle of maintaining a fair competitive platform. Indeed, given such a situation, state-aids to ports, whether necessary or not, continued in most European ports.

Given the above problems, there seemed to be a long way to go for most European ports to become efficient enough to play a positive role in enhancing the competitiveness of SSS-included multimodal transportation in Europe. Port improvement was far from being a finished task, while the issue of port security had only further complicated the issue.

4 IMPLICATIONS AND CHALLENGES OF PORT SECURITY

The 9/11 attack exposed the potential vulnerability of the supply chain, including transport infrastructures like ports, from terrorist attacks[2] and thus various measures were introduced in order to strengthen port security, e.g. International Ship and Port Facility Security (ISPS) Code, Custom-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), etc., while the EU had responded to these new requirements through the introduction of complementary regulations, e.g. Regulation 725/2004 (ISPS Regulation), Authorized Economic Operator (AEO) (the European version of C-TPAT which will come to force in January 2008). Details of the initiatives undertaken by the EU can be found in chapter 18. However, although various initiatives were proposed and executed on port security, more than half a decade after 9/11, the implications of port security measures on the development of SSS in Europe were still largely overlooked, as indicated by the shortage of both academic and non-academic studies on the subject. Recognizing such scarcity, this section aims to shed some light on the implications of port security on SSS, as well as the problems and challenges ahead. Due to such scarcity of literature, apart from documental reviews, much of the analysis here was also based on various in-depth interviews conducted with academic scholars and industrial players involved in the EU ports, SSS, as well as security issues.

The implications of port security measures on SSS-included multimodal supply chain could be several fold. First, due to difference in competitive

[2] Despite the increasing attention on port security, it is worth noting that, until the end of 2006, no major ports had experienced terrorist attacks of any kinds. Thus, until now, the philosophy behind imposing port security measures is still very much based on how to prevent perceived disasters, rather than responding to experienced crisis.

nature, port security measures would be likely to pose even heavier implications on the competitiveness of SSS-included multimodal supply chain than ocean-crossing shipping, in terms of both monetary cost and time. For example, according to information provided by the industry, the execution of security measures on containers (like container scanning) in European ports would typically increase the waiting time in port by about 12 hours and the implications of such additional time was much more visible on SSS when compared to ocean-crossing shipping, as an intra-European journey (both with or without the use of SSS) would typically take no more than a few days. Here it is also worth noting that, when security measures were carried out in ports, it would be executed in exactly the same way with little consideration on whether the final destination of the cargo is within or outside Europe, thus giving a comparative disadvantage to SSS. As a consequence, additional costs would likely pose negative implications in TEN-T's ideals of cohesion, integration and intermodality, as well as affecting the use of SSS as an effective alternative to road vehicles within intra-European transportation, as such measures would inevitably lower the flexibility of SSS and further increase the monetary cost and time required for the whole transportation process.

Secondly, the issue of port security would inevitably lead to difficult negotiations regarding port finance and policies. Unlike the US, by 2007, the EU consists of 27 countries and, as mentioned before, different countries had different policies and perceptions on port operations, management and finance. For example, with substantial financial obligations in fulfilling security requirements (for example, the EC suggested that the installation of major security facilities in a short-sea terminal could cost more than €8 million, while requiring more than €1.5 million annually to operate this system) (SEC (2006) 251), the issue would be likely to further complicate existing questions on the EU agenda regarding who should fund such port security measures, as well as whether the provision of state-aids should continue for the sake of higher security, especially to lesser ports. Here the key question is whether a port should impose a "user-pays principle" and charge port users (like shippers and shipping lines) for security measures. If so, how can the port ensure that its competitiveness (against other ports and other modes in the case of SSS) would not be affected?[3] From previous lessons, one would expect difficult negotiations between different EU members and stakeholders representing different sectors within the supply chain, like the European Seaport Organization (ESPO) and the Federation of Private Port Operators (FEPORT), and compromising a generic solution is by no means an easy task, as typified by the double defeat of the Port Package in the European Parliament in 2003 and 2006, respectively. Port security would be likely to make the creation of "European" and "multimodal" approach in port planning even more difficult to achieve.

[3] In 2006, the average terminal security fees in major ports in Western Europe (including Belgium, France, Ireland, Italy, Spain and The Netherlands) ranged between €6 and €11 per TEU. See chapter 18.

The above analysis clearly indicates that port security would be likely to pose similar problems like the traditional port-related bottlenecks as identified by the EC in affecting the competitiveness of SSS as an alternative in intra-European freight transportation. On the other hand, however, on a positive note, it is argued that the need for enhanced port security, if tackled effectively, can act as a catalyst in boosting the competitiveness of SSS, of which higher security and potentially better coordination between different sectors along the multimodal supply chain would possibly alter shippers' negative perception on SSS's reputation as a poor, worn-out and inefficient mode of transport. Nevertheless, whether security measures would act as an obstacle or catalyst in promoting SSS would largely depend on how the EU perceived the increasingly political demand for higher security measures, as well as its approach in addressing the issue.

The problem was that, unfortunately, the EU seemed to choose to regard port security largely as an obstacle. For example, in response to the global call for higher port security, the EC proposed a programme in establishing a directive on port security, with similar directives on national level with the EU Member States (COM (2004) 76 final). In enforcing this programme, EU members should carry out various port security measures, including port security assessment, development of port security plans, designation of port security authorities and officers in every port and providing inspection procedures, establishing minimum requirements for security assessments and plans. The problem was that many such measures would inevitably imply considerable financial obligations by ports and it was highly doubtful whether lesser ports in Europe, many of which are located within the less developed regions (like Eastern Europe) and rely on local limited hinterlands for survival, would possess the financial muscle to fulfil such requirements. Such worry had not gone unnoticed by European ports. Through ESPO's response to the port security directive programme, ports argued that the programme's enforcement would be likely to result in additional and unnecessary financial obligations in ports (ESPO, 2004).

Under such a situation, perhaps not surprisingly, until August 2006, the ports being recognized as CSI ports in North Europe were still largely the traditional big ports within the region (Antwerp, Bremerhaven, Felixstowe, Hamburg, Le Havre, Rotterdam, Southampton, Thamesport, Tilbury and Zeebruggge), while no ports within the Baltic Sea were recognized as CSI ports. While admitting that the existing trade patterns have largely explained such phenomenon, in the long term this situation would inevitably strengthen the labelling effect of such ports by port users (shipping lines and shippers) in terms of port choice and such concern was also reflected by ESPO, of which they doubted whether the EU could carry out such a programme but without compromising a level-playing platform between different European ports (ESPO, 2004). While the EC often highlighted the necessity of promoting secondary ports to boost the competitiveness of SSS, ironically, the introduction of port security measures posed the risk of strengthening the competitiveness of big ports even further. With the requirement of port security, even the call for even more state-aids in order to ensure that lesser ports could sustain their attractiveness to potential users against the big ports seemed to make sense (which was in direct opposition to the European Parliament's claim that state-aid is anti-competitive in nature, see previous section). As noted by Turró (1999), given the political nature of most European transportation projects and the lack of a unified EU policy on state-aid, including the promotion of SSS, it was already difficult enough to evaluate whether a particular aid was encouraging or distorting competitions, and the question of financing port security had simply further complicated the issue, especially on whether the lesser ports could reach the critical mass to keep pace with the traditionally big ports in Europe with any financial backups from national/regional governments. Indeed, maritime security measures could actually create competitive advantages which would distort competition.

Another problem for the EU's approach was that there was a clear segregation between the port security and SSS projects within the EC, of which the removal of port-related bottlenecks in enhancing SSS-included multimodal supply chain and port security were largely treated as separate issues. For example, the potential implications of port security on the efficiency and competitiveness of SSS were not even mentioned in the most recent EC Communications on ports and SSS (see COM (2004) 453, COM (2004) 478 and COM (2006) 380 final). Such lack of communication was confirmed by an interviewee who was deeply involved in port security himself. He noted that, discussions and cooperation on the implications of port security measures on SSS were at best minimal, if they existed at all. As a consequence, in many ways, advice and proposals provided by the EC were largely piecemeal. On the one hand, while the EC highlighted the importance of simplifying administration in order to make SSS more competitive against other modes, on the other hand, in responding to the request for higher security, the EC's response was to add more bureaucracy to port operation with little consideration on the fact that the efficiency of many European ports was already seriously scrutinized; as typified by the case of Portugal where, until 2006, each of its ports was still controlled by five different authorities (COM (2006) 380 final). Indeed, the lack of communications within the EC had ensured that some of the advice was self-defeating without even consideration of the potential implications on its ongoing projects.

The issue of port security also exposed the deficiency that the evolving role of ports as part of the network along the multimodal logistical supply chain (Heaver, 2002) was still overlooked by the EU, of which the solutions provided by the EC on security measures were still largely port-oriented. Indeed, while in its Communication the EC tried to redefine port as a critical distribution centre along the logistical supply chain so as to solve its insufficiency of well-functioning as interconnection points in seamless intermodal chains (COM

(1999) 317), in practice, ports still largely regarded as a simple interface between land and sea and such an approach would not help ports in becoming a real catalyst to enhance SSS's competitiveness at all. Such deficiency was fully exposed in the recent EC Communication on enhancing supply-chain security within the EU, stated:

> "Recently considerable improvements have been made to transport security in Europe for aviation and maritime transport. Further improvements are expected following the recent adoption of security measures for ports [. . .] Supply chain security levels outside the above-mentioned areas remain unsatisfactory without Community rules in place. [Thus], it is necessary to improve the security level of the European land transport supply chain" (COM (2006) 79 final).

The above quotation clearly reflected the strong belief within the EU that previous initiatives on enhancing port and maritime security (see above) had largely been addressed and thus the next step, "supply-chain" security, should mainly focus on land transport. This was further exemplified by the fact that, in the question on what types of companies can be qualified as secure operators (SO), sea port terminals were simply excluded.[4] More importantly, this proposal had also exposed the fact that, even in addressing "supply-chain security", the approach undertaken by the EU was still largely segregated and piecemeal, not to mention inscribing ports and SSS into the multimodal supply chain. The Communication mainly focused on how operators could qualify to being awarded the SO status while nothing was proposed on how to cohere different operators so as to achieve the objective of enhancing supply-chain security throughout Europe.[5] In fact, the EC did not even seem to be enthusiastic in enforcing the programme other than requesting voluntary actions from stakeholders within the maritime industry, as its impact assessment report noted:

> "A voluntary scheme [. . .] is the most cost beneficial option. It seems practically impossible to establish, for all operators in the supply chain, in one single all-embracing operation (mandatory) security rules and measures [. . .] [Conclusively], the introduction of a mandatory scheme has a negative trade-off, because: it needs huge investments; [it] will cause a big bang in the supply chain; [it] covers many companies which have hardly any importance for security; can easily disrupt the normal functioning of the supply chain" (SEC (2006) 251).

Given the estimation that the implementation and enforcement costs would cost the EU Member States an annual extra €60 billion and €235 million respectively (SEC (2006) 251), of which the former had to be shared by all transport and logistics companies within the EU, it had actually left a big

[4] According to the Communication, it was proposed that, in order to qualify to be awarded the SO status, an operator must undertake at least one of the following activities: (i) preparation of goods of shipment and shipment from the production site; (ii) transportation of goods; (iii) forwarding of goods; and (iv) warehousing, storage and inland terminal operations. Clearly, seaport terminals fit in neither of the above categories.

[5] According to Article 4 of the Communication, the task of coordination would be left to the EU member states. Nevertheless, given the transnational nature of supply chains, it would be doubtful whether national initiatives alone could achieve these objectives.

question mark on how companies would participate in such voluntary actions as requested by the EC.[6]

The above analysis indicates that coordination within the EC in providing a constructive solution in inscribing security issues in ports while not affecting the competitiveness of SSS was clearly lacking. Despite the fact that port security seemed to pose similar implications on SSS's competitiveness like other port-related problems as identified by the EC, until recently, it was still largely regarded as a separate issue which was unrelated to SSS development. There were also strong doubts on whether the statesmen in Brussels really possessed the vision and enthusiasm in inscribing the issue of port security into SSS and improved its competitiveness. Until now, the issue of promoting SSS, port security and, indeed, supply-chain security, are largely regarded as segregated issues which should be resolved separately. Such segregation seemed to indicate that, within the EC, there was a clear lack of communication on the implications of new issues on ongoing projects, of which it ensured that port security would be destined to impose an extra obstacle to the development of SSS. Analysis here also seemed to indicate that the EC was more interested attempting to self-justify that it had fulfilled its obligation in addressing the increasingly political demand for higher port security rather than conducting a comprehensive investigation on enhancing the overall quality of European ports, SSS and supply chain in terms of both competitiveness and security. Put simply, from the EU's perspective, port security was a problem to be solved rather than an opportunity to be exploited. In fact, port security, if tackled effectively, could actually provide an ideal platform for SSS to alter the prejudice of shippers and enhance its image (notably higher security and efficiency along the supply chain). However, such golden opportunity is likely to be missed, with the mistaken approach undertaken by Brussels in addressing the issue largely to be blamed.

5 CONCLUSION

While largely a forgotten component of European transport before the mid-1990s, with changes in circumstances, SSS gained a better change in fortune since then, where the EU statesmen were finally convinced that SSS should be promoted within Europe in order to achieve a better modal-split and realize the objectives of TEN-T on developing multimodal logistical supply chains within the European continent. In this sense, it also highlights the criticality of

[6] It was estimated that the introduction of security measures for micro (<10 employees), small (<50), medium (<250) and large (>250) companies would cost approximately €5,000, €50,000, €135,000 and €300,000 respectively (annual operation costs not included) (SEC (2006) 251). Such obligations could impose a substantial financial burden, especially on micro, small and even medium-sized companies. Moreover, for many micro and small-sized companies, as the same study also admitted, security was hardly a serious issue for them at all. Thus, it would be a big question on how many such companies would be keen to invest such a substantial amount in return for obtaining the SO status.

port efficiency in deciding the competitiveness of SSS-included multimodal supply chain.

Throughout the last decade, although the EU had taken various policy and regulatory initiatives in encouraging the development of ports and SSS, it was clear that there would be still a long way to go before the EC could achieve its objective of improving nodal efficiency and thus Europe's SSS-included logistical supply chain. While traditional problems continued to exist, namely incomplete integration in the intermodal supply chain, image of an old-fashioned industry, complex administrative procedures and linkage to port efficiency levels, as well as the lack of a European and multimodal view in port planning as a major obstacle in port and SSS improvements, it was surprising to find that the implications of port security, which it was anticipated would pose significant implications on the efficiency and competitiveness of SSS, had been largely overlooked by the European statesmen, as illustrated by the fact that most of the port security measures proposed by the EC were piecemeal and, in some cases, self-defeating in enhancing the competitiveness of SSS in Europe. The EC approach in treating port security and SSS as purely segregated issues also indicated that, in practice, the changing role of ports as components of the multimodal logistical network was still largely ignored.

Although the EC had undertaken some initiatives in enhancing port and supply-chain security, what it had proposed was rather segregated and coordination between different related issues was poor, if it existed at all. It seemed that the EC largely regarded the security issue as a problem to solve, rather than an opportunity to improve the overall quality of European multimodal supply chain. This chapter argued that, rather than the potential negative implications which port security could pose on SSS competitiveness in Europe, it was mainly the irrelevant approach of the EU in addressing the issue which posed the major challenge. Better internal coordination within the EC would be necessary so as to provide a more comprehensive package in order to avoid the cancelling out of constructive solutions in achieving the objectives of TEN-T in the foreseeable future. Effective strategies, like detailed cost-benefit analysis, would be necessary to tackle the need for higher security while not compensating for the smooth development of SSS and multimodal supply chain. The recent impact assessment study conducted by the EC on the cost and benefits of different approaches in possible EU legislations to improve supply chain security (SEC (2006) 251), albeit only providing rather some rough ideas, could be a good starting point for such purpose, while the EU could also consider extending the "Green Lane" concept[7] to SSS (especially the identified MS) so as to substantially reduce the

[7] Green Lane is a concept established to confer additional benefits to participants of C-TPAT and CSI. A particular maritime route which meets certain prerequisites set by C-TPAT and CSI e.g. submission of shipping data before loading cargo, loading cargo at a CSI-designated port, approved vessel security, making cargo available for screening and examination before loading, using supply-chain visibility procedures, using container security devices that meet regulations, etc. would be awarded the Green Lane status and would enjoy fewer and less strict (thus faster and more efficient) customs and security inspections. An example of Green Lane (until early 2007) is

negative externalities imposed on the competitiveness of SSS-included multimodal supply chain due to enhanced port security.

It is anticipated that this chapter has played its role as a critical evaluation in assessing the progress of European SSS and port developments so far, as well as shedding some light on identifying the implications that port security is affecting the efficiency of this rising mode in European freight transportation, and its challenges ahead. The author firmly believes that port security, albeit looking like a complicated problem to be resolved, can actually act as a catalyst in accelerating the competitiveness of SSS-included multimodal supply chain in Europe. The only question is whether the EU statesmen recognize such opportunity and revise their rather passive approach and undertake more proactive actions in tackling an issue which would completely change the face of global transportation in the twenty-first century.

REFERENCES

Baird, A.J. (2005): "'EU motorways of the sea policy". Paper submitted to the European Conference on Sustainable Goods and Passenger Transport, held in Kristianstad, 31 May–01 June.

Bekemans, L. and Beckwith, S. (1996): *Ports for Europe: Europe's Maritime Future in a Changing Envionment.* Brussels: European Interuniversity Press.

Chlomoudis, C.I. and Pallis, A.A. (2002): *European Union Port Policy: The Movement towards a Long-Term Strategy.* Edward Elgar: Cheltenham.

Communication of the EC (1995): *The Development of Short Sea Shipping in Europe: Prospects and Challenges.* EC: Brussels (COM (95) 317).

Communication of the EC (1997): *Green Paper on Sea Ports and Maritime Infrastructure.* EC: Brussels (COM (97) 678 final).

Communication of the EC (1998): *White Paper—Fair Payment for Infrastructure Use: A Phased Approach to a Common Transport Infrastructure Charging Framework in the EU.* EC: Brussels (COM (1998) 466 final).

Communication of the EC (1999): *The Development of Short Sea Shipping in Europe: A Dynamic Alternative in a Sustainable Transport Chain—Second Two-Yearly Progress Report.* EC: Brussels (COM (1999) 317 final).

Communication of the EC (2001): *White Paper—European Transport Policy for 2010: Time to Decide.* DG TREN: Brussels (COM (2001) 0370).

Communication of the EC (2003): *Programme for the Promotion of Short Sea Shipping: Proposal for a Directive of the European Parliament and of the Council on Intermodal Loading Units.* EC: Brussels (COM (2003) 155 final).

Rotterdam–Hong Kong. Here it is believed that the Green Lane concept, if applied effectively in SSS, could help in raising the efficiency (and also the reputation) of SSS, although whether peripheral ports could realistically achieve CSI (or similar) status (see last section) would be a question which the EU should address seriously.

Communications of the EC (2004): *Proposal for a Directive of the European Parliament and of the Council on Enhancing Port Security.* EC: Brussels (COM (2004) 76 final).

Communication of the EC (2004): *Amended Proposal for a Directive of the European Parliament and of the Council on Intermodal Loading Units.* EC: Brussels (COM (2004) 361 final).

Communication of the EC (2004): *Communication from the Commission on Short Sea Shipping.* EC: Brussels (COM (2004) 453 final).

Communication of the EC (2004): *Proposal for a Regulation of the European Parliament and of the Council establishing the second "Marco Polo" programme for the granting of Community financial assistance to improve the environmental performance of the freight transport system.* EC: Brussels (COM (2004) 478 final).

Communication of the EC (2006): *Proposal for a Regulation of the European Parliament and of the Council on enhancing Supply Chain Security.* EC: Brussels (COM (2006) 79 final).

Communication of the EC (2006): *Mid-Term Review of the Programme for the Promotion of Short Sea Shipping.* EC: Brussels (COM (2006) 380 final).

Communication of the EC (2006): *Proposal for a Regulation of the European Parliament and of the Council on enhancing Supply Chain Security—Impact Assessment.* EC: Brussels (SEC (2006) 251).

De Monie, G. (2003): "Strategic vision of shortsea shipping in Europe". Presentation to Shortsea Conference: Brugge (October 2003).

European Commission (2002a): *Maritime Policy: European Union Legislation and Objectives for Sea Transport.* DG TREN: Brussels.

EC (2002b): *Transport by Sea: National and International Intra- and Extra-EU.* Eurostat: Luxembourg.

EC (2002c): *Seaports: Gateways to Sea Transport Growth.* DG TREN: Brussels.

EC (2002d): *Statistics on Short Sea Shipping Development: Statistical Evidence of Success.* DG TREN: Brussels.

EC (2002e): *Short Sea Shipping: A Transport Success Story*, DG TREN: Brussels.

EC (2004a): *EU Energy and Transport in Figures 2004.* DG TREN: Brussels.

EC (2004b): *Motorways of the Sea: Implementation through Article 12a TEN-T.* DG TREN: Brussels.

EC (2004c): *Synoptic Table of Bottlenecks in Short Sea Shipping.* DG TREN: Brussels.

ECMT (2001): *Short Sea Shipping in Europe.* European Conference of Ministers of Transport: Paris.

EIB (2003): *EIB Group Activity Report 2003.* EIB Group: Luxembourg.

ESPO (2004): "Response of ESPO to the draft report of the directive proposal on enhancing port security-COM (2004) 76". ESPO: Brussels.

EUROPA: *http://ec.europa.eu.* Last accessed March 2007.

European Parliament (1996): *Resolution on the Communication from the Commission on the development of Short Sea Shipping in Europe—Prospects and Challenges*. European Parliament: Brussels.

Heaver, T.D. (2002): "The evolving roles of shipping lines in international logistics". *International Journal of Maritime Economics*, 4(3): 210–230.

Kågesson, P. (1999): *Economic Instruments for Reducing Emissions from Sea Transport*. The European Federation for Transport and Environment and the European Environmental Bureau: Stockholm.

Napier University (2002): *United Kingdom Marine Motorways Study*, Future Integrated Transport (FIT) Link Programme, Department for Transport and Engineering and Physical Science Research Council (EPSRC). Napier University: Edinburgh.

Nijkamp, P., Vleugel, J.M., Maggi, R. and Masser, I. (1994): *Missing Transport Networks in Europe*. Avebury: Aldershot.

Pallis, A.A. (2002): *The Common EU Maritime Transport Policy: Policy Europeanisation in the 1990s*. Ashgate: Aldershot.

Peeters, C., Verbeke, A., Declercq, E. and Wijnolst, N. (1995): *Analysis of the Competitive Position of Short Sea Shipping: Development of Policy Measures*. Delft University Press: Delft.

Strandenes, S.P. and Marlow, P.B. (2000): "Port pricing and competitiveness in short sea shipping". *International Journal of Transport Economics*, XXVII (3): 315–334.

Turró, M. (1999): *Going Trans-European: Planning and financing transport networks for Europe*. Pergamon: Oxford.

Urrutia, B. (2006): "The EU regulatory action in the shipping sector: a historical perspective". *Maritime Economics & Logistics* 8: 202–221.

INDEX

(*all references are to page number*)