ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

COMPARATIVE ANALYSIS OF THE ISPS CODE NON-CONFORMITIES FROM TOTAL QUALITY MANAGEMENT AND COGNITIVE MAPPING PERSPECTIVE

M.Sc. THESIS

Burcu ÖZTÜRK

Department of Shipbuilding and Ocean Engineering

Shipbuilding and Ocean Engineering Programme

JANUARY 2014

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

COMPARATIVE ANALYSIS OF THE ISPS CODE NON-CONFORMITIES FROM TOTAL QUALITY MANAGEMENT AND COGNITIVE MAPPING PERSPECTIVE

M.Sc. THESIS

Burcu ÖZTÜRK
(508111104)

Department of Shipbuilding and Ocean Engineering

Shipbuilding and Ocean Engineering Programme

Thesis Advisor: Prof. Dr. Serdar BEJİ
Thesis Co-Advisor: Assis. Prof. Dr. Taner ALBAYRAK

JANUARY 2014

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

ISPS KOD UYGULAMA SÜRECİNDEKİ UYGUNSUZLUKLARIN TOPLAM KALİTE YÖNETİMİ VE BİLİŞSEL HARİTALAMA YÖNTEMİ KULLANILARAK KIYASLAMALI ANALİZİ

YÜKSEK LİSANS TEZİ

Burcu ÖZTÜRK
(50811104)

Gemi ve Deniz Teknolojisi Mühendisliği Anabilim Dalı

Gemi ve Deniz Teknolojisi Mühendisliği

Tez Danışmanı: Prof. Dr. Serdar BEJİ
Eş Tez Danışmanı: Yrd. Doç. Dr. Taner ALBAYRAK

OCAK 2014

Burcu Öztürk, a **M.Sc.** student of ITU **Graduate School of Science Engineering and Technology** student ID **508111104**, successfully defended the **thesis** entitled "**COMPARATIVE ANALYSIS OF THE ISPS CODE NON-CONFORMITIES FROM TOTAL QUALITY MANAGEMENT AND COGNITIVE MAPPING PERSPECTIVE"**which she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor : **Prof. Dr. Serdar BEJI** ....
İstanbul Technical University

Co-advisor : **Assis.Prof.Dr. Taner ALBAYRAK** ....
Piri Reis University

Jury Members : **Prof. Dr. Deniz ÜNSALAN** ....
Piri Reis University

Assoc. Prof.Dr. Özcan ARSLAN ....
İstanbul Technical University

Assoc. Prof.Dr. Metin ÇELİK ....
İstanbul Technical University

Date of Submission : 16 December 2013
Date of Defense : 20 January 2014

To my grandfather,

FOREWORD

This thesis was written for my Master degree in Shipbuilding and Ocean Engineering of Institute of Science, Istanbul Technical University.

I would like to thank the following people, without whose help and support, this thesis would not have been possible. For their interest and support during the conducting of this study, I extend my thanks to my thesis advisor Prof. Dr. Serdar BEJİ and my co-advisor Ass. Prof.Dr. Taner ALBAYRAK.

I owe a dept of gratitude to Prof.Dr. Oya OKAY who has brought me in academic life, whose academic success and personality I admire and who supported my works both earthly and emotionally. I extend my thanks to Deniz Mehmet IRAK, who did not preserve his help and support during my thesis study; to Ins. Emre AKYÜZ, to Ins. Dr. Murat Selçuk SOLMAZ; to my precious teachers in PUSEM of Piri Reis University; to the junior and senior students of Piri Reis University who has become my joy and to all my friends whose time i occupied during the study. Finally, I owe a dept of gratitude to my beloved family and my fiance Umut TAÇ, who are my most important support in life.

January 2014 Burcu ÖZTÜRK
(Maritime Transport and Management Engineer)

TABLE OF CONTENTS

Page

ABBREVIATIONS

AEO	: Authorized Economic Operator
ALARP	: As Low As Reasonably Practicable
CCTV	: Closed-circuit television
CSI	: Container Security Initiative
CSO	: Company Security Officer
C-TPAT	: Customs- Trade Partnership Against Terrorism
GDP	: Gross Domestic Product
HAZID	: Hazard Identification
ICS	: International Chamber of Shipping
ID	: Identity Document
IMO	: International Maritime Organization
ISPS	: The International Ship and Port Facility Security
OSC	: Operation Safe Commerce
PFSO	: Port Facility Security Officer
PFSP	: Port Facility Security Plan
PT	: Potential Target
ROV	: Remotely Operated Vehicle
RSO	: Recognized security organizations
SOLAS	: International convention for the Safety of Life at Sea
SPC	: Statistical Process Control
SSO	: Ship Security Officer
SSP	: Ship Security Plan
STCW	: International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
TQM	: Total Quality Management
TRAM	: The Threat and Risk Analysis Matrix
UNCTAD	: United Nations Conference on Trade and Development
U.S	: United States

LIST OF TABLES

LIST OF FIGURES

Page

COMPARATIVE ANALYSIS OF THE ISPS CODE NON-CONFORMITIES FROM TOTAL QUALITY MANAGEMENT AND COGNITIVE MAPPING PERSPECTIVE

SUMMARY

Maritime transport is generally regarded as an important enabler of the world trade and plays a crucial role in the global system. Maritime transport is also a significant exportable service in many countries and in the process contributes directly to national Gross Domestic Product (GDP) and essential to the proper operation of any country’s economy and a vital part of a nation’s infrastructure. Most of the world trade’s is being conducted by maritime transport system. Maritime transportation is carried out in water environment. Ports shape the start and the end point of this kind of transportation. Seaports are very important, which are an inseparable part of this transport, in terms of presence, necessity and economic activity. In addition to their commercial effects, seaports have also strategic and socio-economic effects on their regions. Clearly, due to their effects on maritime trade, seaports are the doors opening to the outside world and breathing points for a country. Because of transnational flows of goods and people; ports and maritime transport has been exposed to several types of security threats. Piracy, robbery attacks, terrorist attacks, illegal migrations, smuggling, human and drug trafficking are the most noticeable threats.

Building the defences against any threat to maritime security is essential in order to achieve safe, secure and efficient shipping, which is the prime objective of the International Maritime Organization (IMO). The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The International Ship and Port Facility Security (ISPS) Code set new standards of security for ships and port facilities around the world. However, recent security breaches and incidents have shown that ISPS Code did not provide desired level of security neither for ships nor for port facilities.

This study addresses analytical analysis of the ISPS Code from quality perspective by using Fishbone Diagram (Ishikawa Diagram) and Pareto Chart techniques and brainstorming sessions for quality defect prevention in order to identify potential factors causing an overall effect process. Fish-bone diagram is prepared to illustrate the problems effecting the ISPS Code’s implementation and Pareto charts are prepared for all the criteria to identify major causes in implementation of the ISPS Code. Finally, Cognitive-mapping method is used to determine the relationship between the causes and sub causes which was identified in Fish-bone diagram to see how the causes and sub causes affect each other.

ISPS KOD UYGULAMA SÜRECİNDEKİ UYGUNSUZLUKLARIN TOPLAM KALİTE YÖNETİMİ VE BİLİŞSEL HARİTALAMA YÖNTEMİ KULLANILARAK KIYASLAMALI ANALİZİ

ÖZET

Denizyolu taşımacılığı sistemi, küresel tedarik zinciri içerisinde üretilen malların tüketici pazarlarına ulaştırılmasında multi-modal ulaştırma ağının limanlar arasındaki deniz geçişinin gemilerle sağlandığı kısmını kapsamaktadır. Günümüzde dünya ticaretinin yaklaşık % 90'ı denizyolu ile gerçekleştirilmektedir. Dünya deniz ticaretinden yılda 400 Milyar Dolar gelir elde edilmektedir. Bu rakamlar denizyolu taşımacılığının ne derecede önemli bir konuma geldiğini göstermektedir. Deniz taşımacılığının ülke ekonomilerindeki yeri gelişmekte, bu sebeple limanlar ve deniz araçlarının önemi de artmaktadır. Özellikle sanayi hammaddelerini oluşturan yükleri bir seferde büyük tonajlarda taşıma özelliği, diğer taşıma yöntemlerine göre ucuz maliyeti (denizyolu ile yapılan taşımalar, demir yoluna göre 3,5; karayoluna göre 7; havayoluna göre ise 22 kat daha ucuz gerçekleşmektedir), denizyolu taşımalarının önemli avantajları arasındadır. Petrol, doğalgaz ve madenlerin önemli bir kısmının denizler altında bulunması, dünyanın dörtte üçünün sulardan oluşması, denizyolu ticaretinin önemini artıran unsurlar arasındadır. Kuru yük ticareti ve konteynerlerdeki büyüme ile alevlenen dünya deniz ticareti 2011 senesinde yüzde dörtlük bir büyüme göstermiştir. 50.000'den fazla yük gemisi uluslararası olarak ticaret yapmaktadır ve her türlü kargo ulaşımını sağlamaktadır. Dünya ticaret filosu 150'den fazla ülkede kayıtlı ve bir milyondan fazla, hemen hemen her milletten denizci ile güçlendirilmiş durumdadır. Bu sayılar denizcilik ve ticaret arasındaki ilişkiyi ve gelişimi net bir şekilde gözler önüne sermektedir. Denizyolu ticareti birçok ülkede kayda değer bir ihraç edilebilir servistir ve süreçte direkt olarak ulusal Gayri Safi Yurtiçi Hasıla'ya (GSYH) katkıda bulunmaktadır. Bu yüzden, ticaret, GSYH ve denizyolu taşımacılığı dünya finansal sisteminin ayrılmaz birer parçalarıdır. Denizyolu ticareti dünyanın dört bir yanındaki müşteriler için rekabete dayanan taşıma masrafları açısından yarar sağlayarak büyümeye devam etmektedir. Bu sebeple, modern dünya için gerekli ölçekte malların ithalat ve ihracatı denizcilik olmadan mümkün değildir. Denizyolu ticaretinin küresel ekonomideki rolü dikkate alındığında, herhangi bir saldırı veya tehdit olasılığının dahi bir limanı olumsuz olarak etkilemesi ve birkaç gün içerisinde bölge ekonomisini yıkıma uğratması söz konusu olabilecektir. Denizyolu taşımacılığı limanlarda başlayıp, limanlarda tamamlanan bir süreçtir.

Liman, feribot ve yolcu gemisi terminalleri genellikle çok sayıda insanın yaşadığı ve çalıştığı kalabalık bölgelere kurulmuştur. Milyarlarca yük ve binlerce insanın her gün girip çıkmakta olduğu dünya limanlarında personel ve gemileri, barınak ve iskeleleri, rıhtım tesisleri ve kargoları olası tehditlerden sürekli olarak koruma gerekliliği güvenlik personeline oldukça stresli önemli görevler yüklemiştir. Uluslararası mal ve insan akışı sebebiyle; limanlar ve deniz yolu taşımacılığı çok sayı ve tipte güvenlik tehdidi ile karşı karşıya bulunmaktadır. Tedarik zincirinin en önemli halkalarından olan limanlarda bir an bile yaşanacak duraksama telafisi zor ekonomik kayıplara yol

açmaktadır. Limanlar ekonomik anlamda ulaşım hatları üzerindeki düğüm noktaları olmalarından dolayı sahip oldukları önemin yanı sıra ülkelerin dış dünyaya açılan pencereleri olarak da büyük önem taşımaktadırlar. Ekonominin yanı sıra sosyal ilişkilerin ve kıtalar arası etkileşimlerin idamesinde önemli roller oynamaktadır. Hem ekonomik hem de sosyal hayata katkı sağlamaktadır. Bu denli stratejik önemi haiz olan deniz limanları yapısal ve kurumsal, ekonomik, finansal, yönetsel, çevresel ve rekabet açılarından pek çok risk ve tehlikeler ile karşı karşıyadır. Bu risk ve tehlikelerin tespit ve tanımının yapılması, alınacak tedbirler ve yapılacak eylemler için son derece önemlidir. Korsanlık, hırsızlık ve terör saldırıları, yasadışı göçler, kaçakçılık, insan ve uyuşturucu kaçakçılığı en çok göze çarpan tehditlerdir. Tüm bu bilgiler ışığında, deniz taşımacılığının, düzenli olarak gelişimi ve sürdürülebilmesi için, tüm nakliye süreci boyunca korunması gerekmektedir.

Denizyolu taşımacılığının dünya ticaretinin belkemiğini oluşturmasından dolayı, uluslararası ulaşım sisteminin yukarıda belirtilen tehlikelerden korunması maksadı ile etkili ve uygulanabilir önlemlere ihtiyaç duyulmuş, limanların uluslararası anlaşmalar ve düzenlemelere uygunluğunun sağlanması için Uluslararası Denizcilik Örgütü (International Maritime Organization – IMO) tarafından güvenlik konusunda bütüncül bir yaklaşımla güvenli, emniyetli ve etkili bir deniz ulaştırması için deniz yoluyla oluşabilecek güvenlik tehditlerinin önlenmesi ve karşı tedbirlerin geliştirmesine yönelik önemli adımlar atılmıştır.

Denizlerde terör olaylarının 2000'li yılların başında gözle görülür biçimde artması dikkatleri denizlerin güvenlik ihtiyacına çevirmiştir. Özellikle 2000 yılında Yemen'in Aden Limanı'nda ABD'nin USS Cole muhribine yapılan 17 denizcinin ölümü ve 39 denizcinin yaralanması ile sonuçlanan terör saldırısı denizlerdeki terör olaylarının farklı şekilde değerlendirilmesinin miladı kabul edilebilir. Çünkü bu saldırıdan önce hakim olan "limanlarda olabilecek terör eylemlerinin genellikle karadan denize doğru olacağı" fikri ortadan kalkmış, "terör tehditinin öncelikle denizden gelebileceği" düşüncesi hakim olmaya başlamıştır. (Solmaz, 2012). 11 Eylül 2001'deki trajik olayları takiben, gemi ve liman tesisleri güvenliği ile bağıntılı yeni önlemler geliştirilmesine Uluslararası Denizcilik Örgütü Meclisi tarafından yirmi ikinci oturumda oybirliği ile karar verilmiştir (ISPS Code). IMO Deniz Emniyeti Komitesi tarafından denizde ya da deniz yoluyla olabilecek terör eylemlerinin önlenmesine yönelik yeni kuralların belirlenmesi amacıyla çalışmalara başlanmıştır. Çalışmalar devam ederken 2002 tarihinde Fransız süper tankeri Limburg'a yapılan terör saldırısı, deniz güvenliği konusunda çalışma yapılmasına olan ihtiyacı bir kez daha ortaya koymuştur. ISPS Kuralları, 1974 yılındaki Uluslararası Denizde Can Güvenliği Sözleşmesi (SOLAS) Bölüm XI-2 Deniz güvenliğini arttırmak için özel önlemler başlığından yola çıkarak uygulanmıştır. Hem SOLAS Bölüm XI-2 hem de ISPS Kod Kuralları, 1 Temmuz 2004 senesinde yürürlüğe girmiştir. ISPS Kod Kuralları uluslararası alanda ve yaygın olarak kabul gören, denizcilik endüstrisini, denizyolu ticaretini ve dünya ekonomisini terörizm konusunda emniyet altına almaya ve limanlar ile gemiler arasındaki işbirliği ve koordinasyona odaklanmış ilk proaktif düzenleyici çerçevedir.

ISPS Kod'un amaçları; güvenlik tehditlerini tespit etmek ve uluslararası ticaretle iştigal eden gemileri ve liman tesislerini etkileyen güvenlik eylemlerine karşı önleyici tedbirler almak amacıyla SOLAS 74 Sözleşmesine taraf olan Devletler, Hükümet kuruluşları, yerel makamlar, denizcilik ve liman işleticileri arasında işbirliğini kapsayan uluslararası bir yapı tesis etmek; denizde güvenliği temin etmek için SOLAS 74 Sözleşmesine taraf olan Devletler, Hükümet kuruluşları, yerel makamlar, denizcilik ve liman işleticilerinin görev ve sorumluluklarını belirlemek, güvenlikle ilgili bilgilerin erken ve etkin bir şekilde toplanmasını ve bilgi alış-verişini temin etmek, Değişen güvenlik seviyelerine hazırlıklı olarak hareket edebilmek için yeterli ve düzgün plan ve prosedürlere sahip olabilmek maksadıyla, güvenlik değerlendirmeleri için bir metodoloji temin etmek, denizlerde güvenliği tesis etmek üzere uygun ve yeterli tedbirlerin alınabilmesi için gerekli ortamı sağlamaktır.

Bu çalışma, ISPS Kod sözleşmesi uygulama süresindeki genel etki sürecine neden olan potansiyel problemleri tespit etmek amacıyla kalite kusurlarının önlenmesi için Balık Kılçığı (Ishikawa) Diyagramı ve Pareto Diyagramı tekniklerini ve beyin fırtınası oturumlarını kullanarak, ISPS Kod Kurallarının kalite perspektifinden çözümsel ve sistematik analizini sunmaktadır. Balık Kılçığı diyagramı kalite problemlerinin kök nedenlerini tanımlamak için kullanılan bir araçtır. Balık Kılçığı diyagramı, etkilere ve bu etkileri yaratan veya onlara katkıda bulunan sebeplere sistematik bir bakış sağlayan bir analiz aracıdır. Diyagramın şekli bi balığın iskeletine benzer. Ana problem balığın baş bölgesinde belirtilir ve problemlerin olası sebepleri diyagramın 'balık kılçığı' bölgesinde gösterilir. Sürecin dört ana adımı bulunmaktadır: problemin tespit edilmesi; dahil olan ana faktörlerin irdelenmesi; olası sebeplerin tanımlanması; ve sebep ve sonuç diyagramının analiz edilmesi Bu çalışmada, "Limanlar için Güvenlik İhlalleri ve Olaylar'' ana problem olarak belirlenmiştir. Beklenen güvenlik seviyesini etkileyen 6 temel neden olduğu bulunmuştur. Risk Yönetimi Süreci, Güvenlik Farkındalığı, Standardizasyon, İzleme ve Denetleme Süreci, Eğitim ve Gemi Tipleri ISPS Kod Kurallarının uygulama prosedürü sırasında asıl problemi etkileyen sebepler olarak tespit edilmiştir. Pareto analizi, kullanıcılara problemin %80'ini çözmek için ilgilenilmesi gereken en önemli nedenlerini tespit etmekte yardımcı olan bir tekniktir. Pareto çizelgesi, yükseklikleri problemlerin frekans veya etkilerini gösteren sütunlar dizidir. Sütunlar soldan sağa yüksekliklere göre azalan sırayla düzenlenir. Daha uzun sütunlarca temsil edilen soldaki kategoriler sağdakilere göre daha fazla önem sahibidir. Bu sütun grafik "gerekli az" ile "gereksiz çok"u ayırmakta kullanılmaktadır.

Balık Kılçığı Diyagramı ile nedenler bulunduktan sonra, majör olanların tespiti için anket hazırlanmıştır. Ankette, akademisyenlere, liman yetkililerine ve gemi kaptanlarına Risk Yönetimi, Güvenlik Farkındalığı, Standardizasyon, Gemi Tipi, Eğitim, İzleme ve Gözetleme Süreci gibi ISPS Kod Kurallarının kalitesine dair problemlerin değerlendirilmesi hakkında sorular sorulmuştur. Bu sonuçlara Pareto analizi uygulanarak sebeplerin öncelik sırası gösterilmiştir. Daha sonra ise, Balık kılçığı diyagramıyla bulunan ana sebep ve alt sebeplerin birbiriyle olan ilişkisini bulmak amacıyla bilişsel haritalama yöntemine başvurulmuştur. Bilişsel harita, kavramlar ve bu kavramlar arasındaki bağlantıların bir bileşimidir. Bağlantılar, kavramlar arasındaki ilişkiyi ifade eder.

1. INTRODUCTION

Maritime transport is generally regarded as an important enabler of the world trade and plays a crucial role in the global system. The origin of it dates back over 5000 years to Mesopotamia. As actualized 5000 years ago, today seas and mariners continue to connect the people and continents. Today around 90% of the world trade is carried by this sector. Fuelled by strong growth in container and dry bulk trades, world seaborne trade grew by 4 per cent in 2011, taking the total volume of goods loaded worldwide to 8.7 billion tons. Besides, world fleet reached more than 1.5 billion deadweight tons in January 2012 (UNCTAD, 2012). There are over 50,000 merchant ships trading internationally, transporting every kind of cargo. The world fleet is registered in over 150 nations, and manned by over a million seafarers of virtually every nationality. The worldwide population of seafarers serving on internationally trading merchant ships is estimated to be in the order of 466,000 officers and 721,000 ratings (ICS, 2013).These numbers certainly shows the development and relation between trade and maritime transportation. Maritime transport is also a significant exportable service in many countries and in the process contributes directly to national Gross Domestic Product (GDP) (Yarbrough and Yarbrough, 2006). So, we can mention that trade, GDP and maritime transportation are the integral parts of world financial system. Seaborne trade continues to expand, bringing benefits for consumers across the world through competitive freight costs. That’s why without shipping the import and export of goods on the scale necessary for the modern world would not be possible.

Ports are defined as geographical, physical and juridical entities; the word “port” usually encompasses waterway connections, i.e. the regions of sea, lake, river, inner waterways and canals (Wood et al., 2002).Maritime transportation is carried out in water environment. Ports shape the start and the end point of this kind of transportation. Thus, a port can be defined, in broad terms, as the start or the end point of maritime transportation or as a transportation infrastructure where the medium of the transport changes during the transportation service (Akten, 1992). In the process of globalization, the restrictions on production and commercial activity have lessened, and the volume of production has increased, the distance between the centres of production and consumption have increased; the importance of maritime transportation has increased and even more this has led to the growth of the share of maritime transportation in logistic costs. In this respect, the condition of ports is highly crucial from the point of total cost of logistics systems. Most of the world trade's is being conducted by maritime transport system manifests the particular importance of sea ports, which are an inseparable part of this transport, in terms of presence, necessity and economic activity. In addition to their commercial effects, sea ports have also strategic and socio-economic effects on their regions. Clearly, due to their effects on maritime trade, sea ports are the doors opening to the outside world and breathing points for a country (Marlow, 2000).

In general, the type of a port is built on a basis of many different aspects, such as scale, service influence area (service influence area) access, location, etc. In literature, there are different classifications such as upstream and downstream ports, city ports and industrial ports and small, medium, large ports, and so on (Langen, 2002). Additionally, in the studies conducted, stylized port classifications have also been developed. Types of ports are classified in terms of their establishment, geographical properties and fields of service (Keskin, 2006). In addition, the definition of port is used not only for seaports but also for air terminals due to legal necessities (Bolat, 2010).

While selecting the position for a port, the geographical properties of the region have a crucial role. First, port freight traffic must be on international sea routes or very close to such an arterial route. So, the distance to the main arterial does not grow much and the time and cost losses are minimized. Behind a port, for the continuous flow of commodities coming from sea, primarily land and railway, additionally air transport must be provided (Gedik, 2007). Traditionally, site selection of ports usually takes place in natural harbors which have geographical advantages that can fulfil the future needs of population growth. The suitability of a port site is controlled by conducting land and environmental survey, by examining coastal motions and water depths, and by doing boring and other necessary ground studies to obtain a complete idea about the characteristic of the ground (Topaloğlu, 2007). In establishment stage of ports, many natural factors such as depth of water, suitable structure of land, feasibility of docking area, effect of wave motions, sedimentation, etc. affect the location selection. The depth which a port has or will have will create a constraint in the properties of the docking ships during the port's commercial life. Meteorological and oceanographic analyses such as determining prevailing winds' magnitude and directions, recurrence of storms, wave heights and impacts, tide durations, amounts and level changes of high and low water levels, directions and speeds of prevailing streams must be conducted (Topaloğlu, 2007). Inside the port, adequate amount of space for ships' easily approaching to docks, manoeuvring and turning must be taken into account. To determine technical factors such as coastal condition, depths, shore condition, topography of the area, streams, and sand motions, hydrologic, seismic, geologic, geophysical, meteorological, and topographic studies are conducted (Branch, 1986). Being located in a strategically important geographical position provides a competitive advantage in achieving the mentioned objectives. However, geographical position alone is not a sufficient factor. The region must be open in terms of economic factors, for industrial investment and industrial development. In addition, land costs should be low since large scale land investments are needed for port area and land expanding costs should be economical when needed. Incentives and tax practices prepared for development priority regions and industrial parks should be considered. With regard to the labour provided from the region, regional wage levels should be taken into account. Port construction costs, the inputs and outputs of the business, transportation costs and energy expenditures should be analysed (Yüksel, 1998). The future sea trade potential of the region should be determinable. Additionally, by considering political and military priorities, the port's location should be evaluated in terms of being in parallel to the country's political, economic and strategic priorities. Ports are a source of cost for carriers and carries want to stop by in ports with larger load potential. In this sense, since there will be an interaction with other ports in the region, it must be evaluated whether there is another port in the area and if there is, its effect on the port to be built, while selecting the location for ports (Gedik, 2010).

Ports are not only the connection points of land and sea in freight and passenger transportation; at the same time, they also have the production function. For countries having a coast, ports have great shares in economies. Via the economic boost which a port creates by being a part of the social structure of the region it belongs, it feeds many other sectors in the background. It increases not only regional and international trade, but at the same time industrial activities (Baran, 2010). When it is thought that the 90% of the world maritime trade is conducted on seas, the effect of ports on economy can be understood better. Even a small stop in ports, which are among the most important links of supply chains results in hard-to-recover economic losses. The interruption of the supply chain in Japan and Thailand due to natural disasters was listed among the main reasons of the slowdown of the world trade and GDP in 2011(TÜRKLİM, 2012). In addition to the economic importance the ports; they have great importance for being countries' windows to the outside world. Along with the economy, they play an important role in maintaining social relations and intercontinental interactions. They contribute to both economic and social life. Ports, which have such strategic importance, face many risks and threats in terms of structural and institutional, economic, financial, administrative, environmental and competition aspects. Determining and defining these risks and threats is very important for measures and actions to be taken (Gedik, 2007).

1.1 Maritime Security

Ports, ferry and liner terminals are usually established in crowded regions where many people live and work. Every day, billions of cargos and thousands of people go in and out of ports all around the world. On the other hand, ports can be referred as border posts as well. When considered in this manner; ports, which are the doors of countries opening to the outside world, can become targets for terrorist groups seeking a global impact. In this sense, security management cannot be left aside from the installation and operating processes of ports.

Considering the role of maritime trade in the global economy, an attack or any threat can affect adversely a port for and within a few days could destroy the regional economy. Taking all these information into account, maritime transportation needs to be protected during all transportation process. This process begins in ports and ends in ports. Port, ferry, and cruise-ship terminals are often located in highly congested areas where large numbers of people live and work. With billions of goods and thousands of people moving in and out of world ports every day, the incredible pressure on security personnel that should constantly safeguard vessels, harbors, ports, waterfront facilities, and cargo from various threats can be an overwhelming task (*url 1*). Because of transnational flows of goods and people; ports and maritime transport has been exposed to several types of security threats. Piracy, robbery attacks, terrorist attacks, illegal migrations, smuggling, human and drug trafficking are the most noticeable threats. “The maritime realms of ports are key intersections of insecurity and security” (Chalk, 2008). The broadly conceptualized “maritime terrorism” in both literature and legislation covers insecurities such as “human causalities, economic losses environmental damage or other negative impacts, alone or in combination, of minor or major consequences” (Parfomak and Frittelli, 2007). Since maritime transportation generates the backbone of the world trade, effective and applicable security measures are needed to ensure that the international transport system is protected from the acts of above mentioned threats. To effectively deter or deny these threats, ports must develop a security strategy that identifies the potential threats, defines critical assets and information, integrates security resources and capabilities, and ensures the successful design, implementation and management of a world class seaport security program (McNicholas,2002).As an effect, a more unified approach of security has been laid upon ports by the International Maritime Organization (IMO) to make sure that ports comply with international treaties and regulations (Wenning et al.,2007).

1.2 The ISPS Code

Building the defenses against any threat to maritime security is essential in order to achieve safe, secure and efficient shipping, which is the prime objective of the International Maritime Organization (IMO). Following the tragic events of 11th September 2001, the twenty-second session of the Assembly of the International Maritime Organization in November 2001, unanimously agreed to the development of new measures relating to the security of ships and of port facilities (*url 2*). Besides 9/11 as the prioritized just cause for the ISPS to take effect, two other attacks also influenced the design of the ISPS Code: the 12 December 2002 ‘attack on the French tanker “Limburg” off the coast of Yemen in October 2002 and the ramming of “USS Cole” by a small boat laden with explosives in 2000’ (Burmester, 2005). The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The ISPS Code is implemented through chapter XI-2 Special measures to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS), 1974. Both SOLAS Chapter XI-2 and ISPS Code entered into force on the 1 July 2004. The IMO is determined to design a more systematic maritime security training scheme and this was agreed with a set of three-level security training and knowledge requirements for the Ship Security Officer, for shipboard personnel having specific security related duties and for all other shipboard personnel (Albayrak et al., 2010). The ISPS Code is the first ever internationally and widely agreed proactive regulatory framework to safeguard the maritime industry, seaborne trade, and the world economy from terrorism and aimed to focus on the cooperation and coordination between ports and ships (Yılmazel & Asyalı, 2005). The dialectic between post-9/11 rhetoric of insecurity actual presence of physical insecurity in ports, multifaceted and interconnected, pushes all ports ‘to perceive and manage security threats through integrating local/domestic threat- level into a global awareness-level ‘(Bichou, 2004).

The objective of this code is to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect/assess security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade. It aims to establish the respective roles and responsibilities of all these parties concerned, at the national and international level, for ensuring maritime security. To ensure early and efficient collation and exchange of security-related information it provides a methodology for security assessments to have in place plans and procedures to react to changing security levels that adequate and proportionate maritime security measures are in place. The objectives are to be achieved by the designation of appropriate officers/personnel’s on each ship, in each port facility and in each shipping company to prepare and to put into effect the security plans that will be approved for each ship and port facility. Part A and B of the Code are, respectively, the mandatory requirements regarding the provisions of chapter XI-2 of SOLAS,1974, as amended, and guidance regarding the provisions of chapter XI-2 of SOLAS,1974, as amended, and part A of the Code. Table 1.1 indicates the mandatory requirements of the ISPS Code.

This Code applies to; passenger ships, including high-speed passenger craft, cargo ships, including high-speed craft, of 500 gross tonnages and upwards; mobile offshore drilling units; and port facilities serving such ships engaged on international voyages. In essence, the ISPS Code sets out to ensure security of ships and port facilities through a risk management process. To determine what security measures are appropriate, an assessment of each of these risks has to be made. In terms of the ISPS Code, a security risk is seen as the threat of an attack, coupled with the vulnerability of the target and the consequences of such an attack taking place. As a standardized, consistent framework for evaluating risks is provided by the ISPS Code; this also allows the contracting governments to circulate any increased change in the overall perceived threat, confident in the knowledge that pre-approved increased responses to security measures on ships and within port facilities will take place. Within the ISPS Code and the security framework it strives to ensure, minimum security-related requirements have been introduced for ships and port facilities. The basic concepts are outlined below.

For ships, these requirements include:

- Creation of ship security plans (SSPs);
- Appointment and training of ship security officers (SSOs);
- Appointment and training of (shipping) company security officers (CSOs);
- Ongoing training of crew and carrying out drills and exercises;
- Identification of onboard items of security related equipment.

For port facilities, these requirements include:

- Creation of port facility security plans (PFSPs);
- Appointment and training of port facility security officers (PFSOs);
- Ongoing training of staff and carrying out drills and exercises;
- Identification of items of security related equipment.

In addition, the ISPS Code further demands that ships and port facilities have in place measures to ensure effective:

- Monitoring and control over access to the ship or port facility;
- Monitoring of the activities of people and cargo;
- Readily available security communications.

Recognizing that each ship (or even class of ship) and each port facility will undoubtedly present different security related risks, the methods by which they meet their obligations in terms of the ISPS Code will vary greatly. These differing response measures are in effect formulated into either ship or port facility security plans, with these plans ultimately being approved by the administration (flag state) or contracting government.

In terms of the ISPS Code, contracting governments have various responsibilities, including; setting the security level; approving SSPs and any amendments to a previously approved plan; verifying compliance of ships with the provisions of SOLAS chapter XI-2 and part A of the ISPS Code; issuing the relevant international ship security certificates (ISSC); determining which port facilities located within their territory are required to designate and train a PFSO; ensuring completion and approval of the PFSA and PFSP or any subsequent PFSP amendment; issuing statements of compliance for port facilities; exercising control and compliance measures over ships. The contracting government is also responsible for communicating security-related information to IMO and to the shipping and port industries. In order to communicate the security threat to a port facility or a ship, the contracting government will firstly set the appropriate security level based on its assessment of all available current security intelligence.

Security levels are identified as security level 1, 2, or 3 and these in-general terms correspond to a normal, heightened and exceptional threat situation, respectively:

- Security Level 1 - The level for which minimum appropriate protective security measures shall be maintained at all times.
- Security Level 2 - The level for which appropriate additional protective security measures must be maintained for a period of time as a result of heightened risk of a security incident.
- Security Level 3 - The level for which further specific protective security measures must 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.

The identification and communicating of the security levels by the contracting government further helps establish good links between ships and port facilities as each security level change triggers the implementation of pre-arranged, relevant security measures each will have to have in place. To do this effectively requires there to be in place a means of good liaison between the CSO, SSO and PFSO. Under the terms of the ISPS Code, shipping companies are required to designate and train a CSO (at least one per company) and to have in place designated and trained SSOs for each of their ships. The CSO's responsibilities include making sure a SSA is properly carried out for each ship and that suitable ship-specific SSPs are thereafter prepared and submitted for approval. Approval of each SSP is normally by the administration (flag state). Thereafter, the SSP is used onboard the ship with responsibility falling onto the SSO to oversee successful implementation. In general terms, the SSP indicates the operational and physical security measures the ship will take to ensure it always is able to operate at security level 1. The SSP also indicates additional, or intensified, security measures the ship must take to move up to and operate at security level 2 when instructed to do so. Furthermore, the SSP indicates possible preparatory actions the ship could take to allow prompt response to any instructions that may be issued to the ship at security level 3. The setting of a security level is solely the responsibility of a contracting government. However, a Master or SSO can enhance the security measures that are in place on board the ship at any time. An example could be when the vessel is sailing through an area of increased vulnerability. The training of the ship's crew in terms of security practices linked to the SSP and the carrying out of regular security related drills and exercises are the responsibility of both the CSO and SSO.

These individuals are also responsible for ensuring proper security-related records are maintained and that any security equipment used on board the ship is functioning properly. Ships are issued an international ship security certificate (ISSC) by their administration, indicating they comply with the requirements of SOLAS chapter XI-2 and part A of the ISPS Code. Ships must thereafter maintain documentary evidence of continued compliance with this legislation, as when a ship is in or proceeding to a port it can be subjected to various control and compliance measures by the contracting government. These can include the ship being subjected to port state control inspections or additional control measures if the contracting government has reason to believe the security of the ship or the port facility has been compromised. There may even be circumstances in which entry into a port could be denied. The

ISPS Code also introduces a number of significant changes to the way ships operate, even at the basic security level 1. One aspect is the need to effectively control access to the vessel at all times. Depending on the security measures in place on a ship, personnel may find they have to sign on and off when joining or leaving. This can include sub-contractors or visitors who may well have to produce adequate identification/photographic identification before being al owed on board. Unexpected/unauthorized personnel may not be al owed on board and often appropriate notices warning of this will be on display. They may also be liable to a search of both their persons and baggage. Cargo and project equipment may also be subjected to similar levels of security search prior to being loaded on board.

Every contracting government will ensure a PFSA is conducted for each of its port facilities located within territory that serves ships engaged on international voyages. This PFSA helps the contracting government determine which port facilities require to appoint and train a PFSO and have a suitable PFSP prepared. The preparation and subsequent implementation of the PFSP is the responsibility of the PFSO. As is the case with ships, this security plan indicates operational and physical security measures the port facility must have in place to ensure it always operates at security level 1. The plan will also indicate additional or intensified security measures the port facility will take to move up to and operate at security level 2 when instructed to do so. It will also indicate the possible preparatory actions the port facility could take to allow prompt response to any instructions that may be issued at security level 3.

The training of port staff in terms of the PFSP procedures and the carrying out of regular security related drills and exercises is the responsibility of the PFSO. The PFSO is also responsible for ensuring proper security-related records are maintained and that any security equipment used within the facility is subject to regular maintenance. In some areas of the world ships may be requested by the PFSO to provide information on a number of matters, such as ship’s cargo, details of passengers or ship's personnel and, very often, information identifying the ship’s last ten ports of call . Some countries seek this information no later than 24-hours prior to the ship's entry into the port. This is because ships using designated port facilities may be subject to port state control inspections/additional control measures.

To facilitate the latter part of this obligation, the PFSO will provide relevant information highlighted by the ship to the port’s contracting government, who will dictate any further action necessary. A ship already operating at a higher security level than that of the port will remain at that higher security level. There is no requirement for the port to increase its security level to match the ship. In these circumstances, however, the Master/SSO and PFSO may follow an additional procedure within the ISPS Code and communicate with one another to agree on any other necessary security measures to be put in place. However, if a ship is operating at a lower security level than the port, then the ship must raise its security level to equal that of the port. This means that the ship's crew, visitors, project staff, contractors and al others onboard must be prepared to respond to any instruction from the SSO as part of complying with this requirement, as ships must have the ability to immediately achieve this change and to be able to maintain the higher security level required.

Table 1.1: The mandatory requirements of The Isps Code.

Section 1 General
Section 2 Definitions
Section 3 Application
Section 4 Responsibilities of Contracting Governments
Section 5 Declaration of Security
Section 6 Obligations of the Company
Section 7 Ship Security
Section 8 Ship Security Assessment (SSA)
Section 9 Ship Security Plan (SSP)
Section 10 Records
Section 11 Company Security Officer (CSO)
Section 12 Ship Security Officer (SSO)
Section 13 Training, Drills and Exercises on Ship Security
Section 14 Port Facility Security
Section 15 Port Facility Security Assessment
Section 16 Port Facility Security Plan
Section 17 Port Facility Security Officer
Section 18 Training and Drills on Port Facility Security
Section 19 Verification and Certification

1.3 Aim of the Thesis

The introduction of the ISPS Code may have significantly reduced maritime attacks by terrorists since 1 July 2004 (Surhone et al., 2010). But, the ISPS Code is not a panacea against all maritime threats (Goh, 2006). Recent security breaches and incidents have shown that ISPS Code did not provide desired level of security neither for ships nor port facilities. Although these regulations have improved maritime security, gaps and regulatory bottlenecks remain (Ferriere et al., 2005). Mazaheri and Ekwall, 2009 summarized the disadvantages of the ISPS Code as higher operative expenses and a high implementation cost and also ISPS Code Part B may lead to problems due to existence of discordance. The improper implementation of the ISPS Code in some countries created some difficulties to the seafarers', such as refusal of shore leave, identity cards, piracy procedures and stowaway prevention (Balbaa, 2005). Several authors (Griffett, 2005; Stevenson, 2005) point out the effects that the ISPS Code has on seafarers' lives and it may restrict human rights and limit access to the ship. Ran (2005) and Stevenson (2005) believe that different interpretations of the code in different countries are one of the ISPS Code's weaknesses. Effective implementation in port facilities in different countries varies significantly, experiencing numerous difficulties. These difficulties are mostly caused by limited economic potentials, differing positions on the status of national and international maritime security system, and finally, different understanding what mitigation measures should be accepted as appropriate in different countries (Zec et al., 2010). Differing risk profiles and standards applied between nations, applicability of the code to different vessel types are also pointed out by Ran, 2005.As seen above many academicians evaluated the effectiveness of the ISPS Code from different point of view and commented on shortcomings of the ISPS Code. A literature table is given in Table 1.2 chronogically.

Table 1. 2: Literature table related to The Isps Code

Aim of the paper	*Methodology*	*Authors & Date*
To analyze and assess operational risk within the port terminals at the RO–RO activity.	AHP multicriteria approach	Mabrouki, C., Bentaleb, F., Mousrij, A. (2014)
To facilitate the quantitative analysis of port facility security assessment (PFSA).	Fuzzy evidential reasoning	Wang, J., NG, Adolf., Yang, Z. (2014)
To identify level of risk on sea ports.	Interviev survey, questionnaire survey, risk map	Chang, C., Xu, J., Song, D. (2014)
To develop a port security economic model to evaluate the impacts of port security policies to container volumes.	System Dynamics (SD)	Gi-Tae Yeo, G., Pak, J., Yang, Z. (2013)
To analyse and discuss the United States (US) and the European Union (EU) approaches on maritime transport and port security, in a comparative way.	Analysis of Policy and regulatory frameworks	Papa, P. (2013)
To focus on the strategic issues, policy framework and its consequences for the future Indian scenario.	Evaluation of Indian Maritime Policy	Panigrahi, J., Pradhan, A. (2012)
To describe and evaluate the associated risk factors within the ports and terminals operations and management.	Fuzzy set theory and evidential reasoning approach	Mokhtari, K., Ren, J., Roberts ,C., Wang, J. (2012)
To propose a generic bow-tie based risk analysis framework to identify and evaluate risks.	Fault Tree Analysis (FTA) and Event Tree Analysis (ETA)	Mokhtari, K., Ren, J., Roberts ,C., Wang, J. (2011)
To explore the ISPS Code practice at ports.	Cognitive mapping	Celik, M.,Topçu, İ. (2010)
To implement of security measures in small to medium developing countries.	Legal framework & port status evaluation of Croatia	Zec, D., Frančić, V., Hlača, M. (2010)
To evaluate ISPS Code port security implementations' effectiveness and Turkey's implementations.	Analysis of terrorist attacks	Solmaz, M. (2010)
To investigate if containers equipped with a small passive detector will register during transport the neutron irradiation by fissionable material such as plutonium in a measurable way.	Monte-Carlo simulation	Maenhout,G., Roo,F., Janssens,W. (2010)
To find the impact of the ISPS code from a total port perspective.	Electronic Questionnaire	Mazaheri, A., Ekwall, D. (2009)

To increase the speed of post-incident recovery amongst the APEC economies and the US to facilitate a resumption of trade after a terrorist incident.	The APEC Trade Recovery Programme (TRP)	Ho, J. (2009)
To examine the adequacy of The ISPS Code in addressing post 11/09/2001 maritime security threats faced by ships and ship’s crew.	Overview of the Code	Goh, R. (2006)
To highlight the need for enhanced crisis management capabilities within ports as part of a standard management repertoire and suggests a new classification scheme for mapping vulnerability within ports and across supply networks.	Analysis of anti-terrorism maritime initiatives	Barnes, P., Oloruntoba, R. (2005)
To identify critical maritime security gaps andto explore adapting existing commercial off-the-shelf technologies as possible solutions.	Canada United States Cargo Security Project	Ferriere, D., Pysareva, K., Rucinski, A. (2005).
To enhance maritime security.	Anlaysis of threats and SUA Convention	Roach, J. (2004)
To develop port security strateji.	Analysis of “Defense-In-Depth” and world class seaport security program	Nicholas, M. (2002)

While assessing the ISPS Code deficiencies, I used the quality techniques differently from them. This study addresses analytical analysis of the ISPS Code from quality perspective by using Fishbone Diagram (Ishikawa Diagram) and Pareto Chart techniques and brainstorming sessions for quality defect prevention in order to identify potential factors causing an overall effect process. Fish-bone diagram is prepared to illustrate the problems effecting the ISPS Code’s implementation and Pareto charts are prepared for all the criteria to identify major causes in implementation of the ISPS Code. Finally, Cognitive-mapping method is used to determine the relationship between the causes and sub causes which was identified in Fish-bone diagram to see how the causes and sub causes affect each other.

This thesis intends to:

1. Define the problem and its causes affecting the ISPS Code’s implementation
2. Realize the order of importance of the causes affecting the ISPS Code’s implementation
3. Find the relationship among the causes and sub causes that affect the ISPS Code’s implementation

2. METHODOLOGY

2.1 Motivation

In the process of globalization, the restrictions on production and commercial activity have lessened, and the volume of production has increased, the distance between the centres of production and consumption have increased; the importance of maritime transportation has increased and even more this has led to the growth of the share of maritime transportation in logistic costs. In this respect, the condition of ports is highly crucial from the point of total cost of logistics systems.Considering the role of maritime trade in the global economy, an attack or any threat can affect adversely a port for and within a few days could destroy the regional economy. Taking all these information into account, maritime transportation needs to be protected during all transportation process.

Building the defences against any threat to maritime security is essential in order to achieve safe, secure and efficient shipping, which is the prime objective of the International Maritime Organization (IMO). The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The International Ship and Port Facility Security (ISPS) Code set new standards of security for ships and port facilities around the world. However, recent security breaches and incidents have shown that ISPS Code did not provide desired level of security neither for ships nor for port facilities.

In the third part of this thesis; it is aimed to define the problems affecting The ISPS Code’s implementation, to realize importance of problems and to find the relationship among the problems. At last part of the thesis, suggestions are represented. When the defined problems clear up, we believe that the ISPS Code provide aimed level of security both for ships and port facilities.

2.2 Total Quality Management (TQM)

The concept of quality has existed for many years, though it's meaning has changed and evolved over time. In the early twentieth century, quality management meant inspecting products to ensure that they met specifications. In the 1940s, during World War II, quality became more statistical in nature. Statistical sampling techniques were used to evaluate quality, and quality control charts were used to monitor the production process. In the 1960s, with the help of so-called "quality gurus," the concept took on a broader meaning. Quality began to be viewed as something that encompassed the entire organization, not only the production process. Since all functions were responsible for product quality and all shared the costs of poor quality, quality was seen as a concept that affected the entire organization *(url 3)*. The concept of quality means different things depending on the nature of the business and industry, as well as the means of how performance characteristics of a particular product are especially when compared with the standards set in advance by the beneficiary or organization. Quality is to meet the expectations of the beneficiary or exceed them. Quality is defined as the suitability of the product to meet the intended use, or to meet the beneficiary expectations (Bank, 2000).

Since the 1970s, competition based on quality has grown in importance and has generated tremendous interest, concern, and enthusiasm. Companies in every line of business are focusing on improving quality in order to be more competitive. In many industries quality excellence has become a standard for doing business. Companies that do not meet this standard simply will not survive. The term used for today's new concept of quality is total quality management or TQM. Oakland (2000) views TQM as a comprehensive approach to improve competitiveness, efficiency, flexibility through planning, organization, and understanding each activity. The involvement of everyone at all levels including the adoption of a strategic view for management quality. Focusing on preventing problems before they occur requires attention to remove existing barriers. TQM can be defined through the description of the basis adopted by the principle of "total dedication to the beneficiary". The description of the output to achieve beneficiary's loyalty to reach time and cost effectiveness. The continuous improvement through discussing various instruments and techniques to create climate of support and encouragement team work. TQM means a commitment to meet or exceed the needs of the beneficiary. The application of the principle adoption to search for quality in any place of work, starting to identify the needs of the beneficiary, and the end the assessment the beneficiary is satisfaction (Oakland, 2000).

The U.S. Department of Defence (1989) defines Total Quality Management as “both a philosophy and a set of guiding principles that represent the foundation of a continuously improving organization”. TQM integrates fundamental management techniques, existing improvement efforts, and technical tools under a disciplined approach focused on continuous improvement (Schellong, 2008). Total Quality Management tools and techniques divided into categories as quantitative and non-quantitative. The basic quantitative ones are statistical process control (SPC). Statistical process control often called ‘The Magnificent Seven’ consists of seven tools; Pareto Chart, Histogram, Process Flow Diagram, Control Charts, Scatter Diagram, Check Sheets and Cause & Effect (Fishbone) Diagram (Besterfield, 2009).

In the first part of this paper, the above mentioned two of seven methods were used. These are fishbone diagrams and Pareto chart techniques. First and foremost, the effects of potential factors causing an overall effect process were detected by the assistance of conducted studies and experiences given from port security personnel. In the second step, the potential factors were designed as a fishbone diagram. After the completion of the Fishbone diagram so as to realize the order of importance of causes Pareto chart were used.

2.2.1 Cause & Effect (Fishbone) Diagram Techniques

Fishbone diagrams are casual diagrams created by Kaoru Ishikawa. The Fishbone (also known as Cause &Effect and Ishikawa) diagram is a tool for identifying the root causes of quality problems. Fishbone diagram is an analysis tool that provides a systematic way of looking at effects and the causes that create or contribute those effects. Because of the function of the fishbone diagram, it may be referred to as Cause and Effect diagram (Watson, 2004). The shape of the diagram looks like a skeleton of a fish. Main problem is stated in fish head and possible causes of the problems are stated in the ‘fish bones’ of the diagram. Fish bones’ are also subdivided into smaller bones. The representation can be simple, through bevel line segments which lean on an horizontal axis, suggesting the distribution of the multiple causes and sub-causes which produce them, but it can also be completed with qualitative and quantitative appreciations, with names and coding of the risks which characterizes the causes and sub-causes, with elements which show their succession, but also with other different ways for risk treatment (Hekmatpanah, 2011). The process has four major steps: identifying the problem; working out the major factors involved; identifying possible causes; and analysing the cause and effect diagram (Dey, 2004). Fishbone diagrams are often used in needs assessment to assist in illustrating and/or communicating the relationships among several potential (or actual) causes of a performance problem. Likewise, these graphical representations of relationships between needs (i.e., discrepancies between desired and actual results) offer you a pragmatic tool for building a system of performance improvement interventions (for instance, a combination of mentoring, job aids, training, motivation, new expectations) around the often complex relationships found across potential (or actual) causes. Though the fishbone diagram originated in the field of management studies, it is now widely used in other fields, such as medicine, engineering, and the pure sciences, manufacturing science, computer science and IT. In medicine, it has been used to investigate the causes of infection (Frankel et al, 2005); in the field of industrial engineering, it has been applied to analysing the direct and indirect factors involved in accident prevention (Chang and Lin, 2006); in information science, it is mainly applied to the development of computer software (Bjornson et al, 2009); for business market research, fishbone diagrams are a useful tool for analysis of product marketing strategies (Mazur, 1998). Advantages and disadvantages of Cause & Effect Diagram are shown below.

Advantages;

- Fishbone diagrams permit a thoughtful analysis that avoids overlooking any possible root causes for a need.
- The fishbone technique is easy to implement and creates an easy-to-understand visual representation of the causes, categories of causes, and the need.
- By using a fishbone diagram, you are able to focus the group on the ″big picture″ as to possible causes or factors influencing the problem/need.
- Even after the need has been addressed, the fishbone diagram shows areas of weakness that - once exposed - can be rectified before causing more sustained difficulties.

Disadvantages;

- The simplicity of a fishbone diagram can be both its strength and its weakness. As a weakness, the simplicity of the fishbone diagram may make it difficult to represent the truly interrelated nature of problems and causes in some very complex situations.
- Unless you have an extremely large space on which to draw and develop the fishbone diagram, you may find that you are not able to explore the cause and effect relationships in as much detail as you would like to (Gupta et al., 2007).

2.2.2 Pareto Analysis

The Pareto analysis, which is also known as 80-20 rule, is named after Italian economist Vilfredo Pareto . The principle states that for many events, roughly 80% of the effects/problems come from 20% of the causes (Surhone et al., 2010). It is a type of chart that contains both bars and a line graph, where individual values are represented in descending order by bars, and the cumulative total is represented by the line. This technique helps the users to identify the top causes that need to be addressed to resolve 80% of the problem. A Pareto Chart is a series of bars whose heights reflect the frequency or impact of problems. The bars are arranged in descending order of height from left to right. This means that the categories represented by the tall bars on the left are relatively more significant than those on the right. This bar chart is used to separate the “vital few” from the “trivial many”.

How to Use the Tool;

- Step 1: Identify and List Problems – First, write a list of all of the problems that you need to resolve. Where possible, talk to clients and team members to get their input, and draw on surveys, helpdesk logs and suchlike, where these are available.
- Step 2: Identify the Root Cause of Each Problem – For each problem, identify its fundamental cause. (Techniques such as Brainstorming, the 5 Whys, Cause and Effect Analysis, and Root Cause Analysis will help with this.)
- Step 3: Score Problems – Now you need to score each problem. The scoring method you use depends on the sort of problem you're trying to solve. For example, if you're trying to improve profits, you might score problems on the

basis of how much they are costing you. Alternatively, if you're trying to improve customer satisfaction, you might score them on the basis of the number of complaints eliminated by solving the problem.

- Step 4: Group Problems Together by Root Cause – Next, group problems together by cause. For example, if three of your problems are caused by lack of staff, put these in the same group
- Step 5: Add up the Scores for Each Group – You can now add up the scores for each cause group. The group with the top score is your highest priority, and the group with the lowest score is your lowest priority.
- Step 6: Take Action – Now you need to deal with the causes of your problems, dealing with your top-priority problem or group of problems first. Keep in mind that low scoring problems may not be worth bothering with; solving these problems may cost you more than the solutions are worth (*url 4*).

2.3 Cognitive Mapping

Cognitive maps are directed graphs used in understanding and capturing the cause-effect relationships in complex causal systems and facilitate to understand the interconnections within the elements of the systems. Cognitive mapping technique is a popular technique in investigating individuals` cognitive representations in strategic decision making. (Hodgkinson et.al, 2004). Eden and Ackerman, (1998) define cognitive mapping as a technique designed to capture the thinking of an individual about a particular issue or problem in a diagrammatic format. The map also reveals how the elements of the issues relate to each other and how changes in the character of one element may have effects on another. Similar to Eden and Ackerman's (1998) definition, Tegarden and Sheetz (2003) define cognitive mapping as a technique that captures the individuals' view of a particular issue in a graphical representation. Özesmi and Özesmi (2004) define cognitive map as a qualitative model of how a given system operates and state that they are especially applicable and useful tools for modelling complex relationships among variables.

A cognitive map approach ensures participations of the decision makers' motivation through creative decision-making. In addition, it is an active tool, which allows modification of dynamic attributes in problem environment in accordance with the prior settings and goal. (Çelik, 2010) Cognitive map was utilized by Axelrod (1976) for political analysis and decision making.

It has been used widely by researchers in a variety of different contexts such as management and administrative sciences (Eden, 1992; Eden et al, 1992; Langfield-Smith and Wirth, 1992; Clarke and Mackaness, 2001; Ross and Hall, 1980; and Diffenbach, 1993), game theory (Klein and Cooper, 1982), information analysis (Montezemi and Conrath, 1986), popular political developments (Taber, 1991), analysing political decisions (Hart, 1977), electrical circuits analysis (Styblinski and Meyer, 1988), decision analysis (Zhang et al 1989), a distributed decision process model in the internet domain (Zhang et al 1994), the process of way-finding (Chen and Stanney, 1999), IS/IT project risk management (Al-Shehab et al, 2005), business process redesign (Kwahk and Kim, 1999), new product development (Carbonara and Scozzi, 2006), knowledge management (Noh et al, 2000), online community voluntary behaviour (Kang et al, 2007), Bosphorus crossing problem (Ulengin et al, 2001), design of electronic commerce web sites (Lee and Lee, 2003), modeling the strategy building process (Carlsson and Fuller, 1996), and modelling IT projects success (Rodriguez-Repiso et al, 2007).

Generally, the basic elements of a cognitive map are simple. The concepts an individual uses are represented as *points*, and the causal relationships between these concepts are represented as *arrows* between these points. This representation gives a graph of points and arrows, called a *cognitive map*. The strategic alternatives, all of the various causes and effects, goals and the ultimate utility of the decision-making agent can all be considered as concept variables, and represented as points in the causal map. Causal relationships can take on basic values + (such as promotes, enhances, helps, is benefit to, etc.), - (such as retards, hurts, prevents, is harmful to, etc.) and 0 (such as has no effect on, does not matter for, etc.). With this representation, it is then relatively easy to see how concepts and causal relationships are related to each other and to see the overall causal relationships of one concept with another. (Chaib-Draa & Desharnais, 1998)

3. APPLICATION

3.1 Scope

In this part, analytical and systematical analysis of the ISPS Code from quality perspective by using Fishbone Diagram (Ishikawa Diagram) and Pareto Chart techniques and brainstorming sessions for quality defect prevention in order to identify potential factors causing an overall effect process has done. Fish-bone diagram is prepared to illustrate the problems effecting the ISPS Code's implementation and Pareto charts are prepared for all the criteria to identify major causes in implementation of the ISPS Code. Finally, Cognitive mapping method is used to determine the relationship between the causes and sub causes which was identified in Fish-bone diagram to see how the causes and sub causes affect each other. The path during this study is shown in figure 3.1.

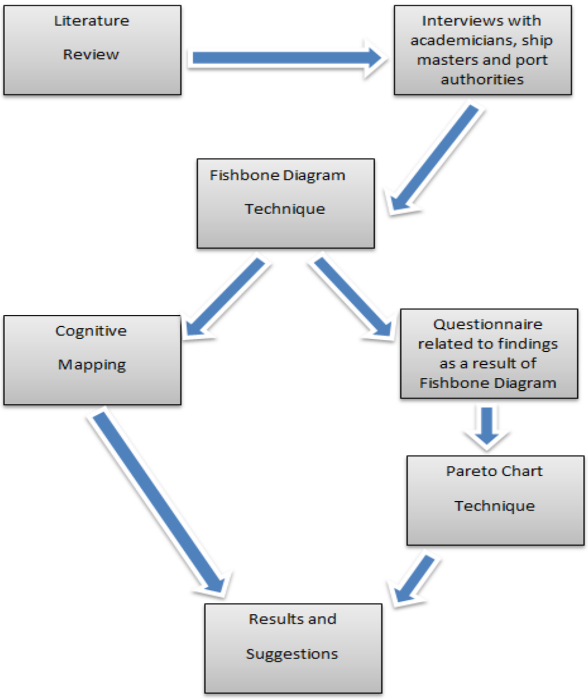
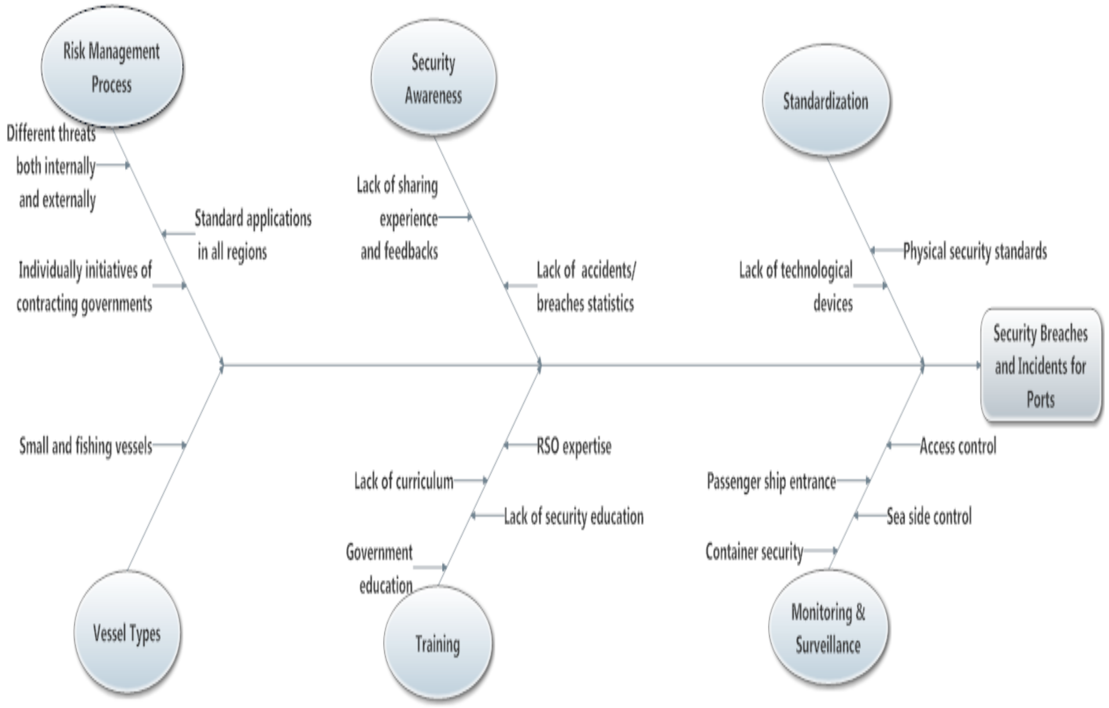

Literature Review
Interviews with academicians, ship masters and port authorities
Fishbone Diagram Technique
Cognitive Mapping
Questionnaire related to findings as a result of Fishbone Diagram
Pareto Chart Technique
Results and Suggestions

Figure 3. 1 : Path of the study.

3.2 Assesment of the ISPS Code via Fish-bone Diagram

In this study “Security Breaches and Incidents for Ports” is determined as main problem in fish head. Through brain-storming sessions academic researches; and literature review; Risk Management Process, Security Awareness, Standardization, Monitoring and Surveillance Process, Training and Vessel Types are determined as the causes affecting main problem during implementation procedure of the ISPS Code. Figure 3.2 shows the fishbone diagram, which represents the main causes for all six aspects of analysis



Risk Management Process
Different threats both internally and externally
Standard applications in all regions
Individually initiatives of contracting governments
Security Awareness
Lack of sharing experience and feedbacks
Lack of accidents/ breaches statistics
Standardization
Physical security standards
Lack of technological devices
Security Breaches and Incidents for Ports
Small and fishing vessels
Vessel Types
RSO expertise
Lack of curriculum
Lack of security education
Government education
Training
Access control
Passenger ship entrance
Sea side control
Container security
Monitoring & Surveillance

Figure 3.2 : Fishbone diagram of “Security Breaches and Incidents for Ports”.

3.2.1 Training

The program of IMO model training courses developed out of suggestions from a number of IMO Member Governments, following the adoption of the International Convention on Standards of Training, Certification and Watch keeping for Seafarers, (STCW), 1978, as amended. Assisted by contributions from various Governments, IMO has designed the series of courses to help implement this Convention and, further, to facilitate access to the knowledge and skills demanded by increasingly sophisticated maritime technology. The courses are flexible in application: maritime institutes and their teaching staff can use them in organizing and introducing new courses or in enhancing, updating or supplementing existing training material. The model courses each include a course framework (detailing the scope, objective, entry standards, and other information about the course), a course outline (timetable), a detailed teaching syllabus (including the learning objectives that should have been achieved when the course has been completed by students), and guidance notes for the instructor and a summary of how students should be evaluated.

The list of the IMO Model Courses related to ISPS Code is;

- Model Course 3.19 **-** Ship Security Officer,
- Model Course 3.20 - Company Security Officer,
- Model Course 3.21 - Port Facility Security Officer,
- Model Course 3.22 - Flag State,
- Model Course 3.23 - Actions to be taken to Prevent Acts of Piracy and Armed Robbery,
- Model Course 3.24 - Security Awareness Training with DSD,
- Model Course 3.25 - Security Awareness Training for All Port Facility Personnel,
- Model Course 3.26 - Security Training for Seafarers with Designated Security Duties
- Model Course 3.27 - Security Awareness Training for All Seafarers

The Global Program on ISPS implementation was launched in 2002. By the end of 2005, 22 regional seminars/workshops and 87 national training courses/advisory missions have been organized, resulting in some 4.000 people being trained globally (*url 5*). Despite these numbers; the academicians and port security managers stated that the ISPS training level was not in an expected level. There is no standardization in training of ISPS implementation neither in different nations nor different courses in same nations. So, training has been identified as another major cause for Security Breaches and Incidents for ports. During our brainstorming sessions RSO's complained about the unsatisfied level of ISPS training program. The training courses are carried out under different curriculums. That's why lack of standard curriculum is detected as one of the sub-causes. All countries set their course program according to their risk assessment and experiences. Hence, the ISPS Code's training curriculum varies regionally. IMO has to examine the course program and establish a generally accepted curriculum and compel the governments to put into force these courses. Deficiencies in training are not limited with curriculum. The instructors' experiences are also important. To take the control of security breaches, well-educated instructors are in need. That's why; universally accepted certificate program can be put into force for instructors. Thus, they will have an internationally recognized certification and will be in satisfied information level all over the world. But education problem goes on with contracting government's personnel. Contracting governments are not only a signature station. They are responsible for implementing of ISPS Code and they have to realize the significance of this code. For regular implementation governments' personnel (Designated authorities) have to be included in the course program.

3.2.2 Standardization

For a successful security management use of technological devices and equipment is very important. But, port authorities are complaining about the standardization because the ISPS Code does not oblige the use of any security devices and mention standards for them. The ISPS Code set some rules, but in some cases, it is unable to clarify the standards, especially during the process of determining technological devices using in ports and physical security standard. These non-standard applications induce to some vague areas, especially in port security management systems and physical security issues such as the number of security personnel. Most terminals are operating under tight financial and competing conditions and need to make a profit. The result is that the incentive for security is minimal and in many cases a non-effective security operation is put in place just for show. In some ports, port managers try to keep the number of security personnel in limited numbers due to financial restrictions. Therefore, surveillance and controlling the port area become difficult. When the issue is evaluated from this perspective, the need of setting new standard emerges about the standardization of security personnel depending on the traffic intensity and area size of the port. The vague areas on physical security issues are not limited with security personnel numbers. Fencing is another problem. Designated authorities and also ports experiences problems regarding fences type. A fence is often described as the first line of defence. However the level of protection offered will depend on a number of variables, including the size and layout of the area that needs protecting, the height required, the construction, material used and any other security extras which may need to be added on to the perimeter. The same problem arises concerning the technological devices. The importance of technology on maintaining security is known. There are some initiatives that mega ports put in force such as CSI and C-TPAT but no mandatory devices mentioned in ISPS Code like CCTV, fingerprint, X-ray scan, facial recognition, underwater security devices and etc. As a result, we detected in our searches that, the need of review emerges about the use of technological devices and physical security standard by evaluating the security and cost analysis.

3.2.3 Monitoring and surveillance process

Monitoring and surveillance has been identified as another major cause because many security breaches occur due to surveillance and monitoring process deficiencies. Being able to control the movement of the inner harbor could minimize the possible security threats. That’s why seaside, underwater, access control and container security are important problems. Especially, container security becomes more important with each passing day. Unlike tankers, container vessels are more likely to be used as a tool for the delivery of terrorist weaponry rather than as the subject of an attack. Millions of containers arrive in Europe, Japan, and the United States each year, and each could potentially contain explosives, biological agents, or weapons of mass destruction (Goh, 2006). The United States has developed unilateral initiatives to address cargo security, including the Container Security Initiative (CSI) and the Customs–Trade Partnership against Terrorism (C–TPAT). These initiatives target security measures along the entire supply chain, thereby expanding the more narrow focus of the ISPS. These initiatives may very well provide a model for the WCO in developing internationally binding cargo security measures (Ran, 2005).

But the problem is not limited only with container security. Controlling the port area is another cause which consists of seaside, underwater and access control. Seaside control and underwater control is important from the perspective of terrorism and sabotage. The land-based section of maritime security can be divided into two main parts: Port & Terminal protection and Shore & Waterway protection. Of course the shores and waterways reach the ports and terminals, but because of the difference in the environment and the extensiveness of the areas the solutions are very different (Kahn, 2003). Terrorist can use sea side in case of any control deficiency. Therefore, some technological measures could be put into practice to prevent any possible attack. Remotely operated vehicle (ROV) is a robotic system for underwater operation. ROVs vary in size and configuration, e.g., number and type of cameras, mechanical tools, presence of sonar and other sensors. There are a number of commercially available ROVs specifically designed for harbor security (Ferriere et al., 2005). Another solution method could be using the diver. This is not exact solution but can be preferred depending on financial conditions of port facility. Access control is also another sub-cause. This problem can be solved by using devices like fingerprint, face recognition and CCTV system. An access control deficiency was experienced in the case of Kartepe Ferry's hijacking. The passenger vessels transport millions of people in a day so the access points of ferry's ports are easy to enter for professional terrorists.

Gate access control is the simplest to achieve, and operates by checking the identity of people entering the port and giving a temporary access pass. But it remains essential to also physically check the vehicles entering and leaving to make sure that no "extra" people enter the terminal. This costs extra manpower and effort, but without it, access control is meaningless. The tools to be used can vary from simple ID cards to smart cards and biometric cards (Kahn, 2003). Each person entering the port should be issued an identification badge. The ID badge program should be managed by a computer-based system which functions with proximity or magnetic strip badges, assigns zones of access, permits or denies a person's access into a specific zone, and records this activity into a data base. The front of the employee ID badge should have a colour photo, the employee's name and signature, government identity document or passport number, position, and an expiration date. The back of the ID card should note the employee's date of birth, height, weight, colour of hair and eyes, complexion, and the signature of the Port Director. Each employee's badge should be programmed to allow access to specific zones; this being based on his/her job or position requirements. Employees who have forgotten or lost their badges should be issued a "temporary badge" for the day or while a new badge is being prepared. Visitor badges generally are for "one-day use", disposable, and should note the name of the visitor, government identity document or passport number, area or zones visiting, and the date issued. Non-employees who temporarily or frequently work in the port - such as contractors, clients, and government representatives - should be issued a badge similar to the employee ID badge (but a different colour). A permanent record of the issue all non-employee badges (with the captured data) should be maintained for at least two years. Alternatively, if financially possible, container X-ray stations should be positioned at the vehicle and container entrance points to screen for narcotics. Special attention should be given to suspicious mail and delivery packages and unattended vehicles positioned at access points or near key assets or buildings (McNicholas, 2002).

When considering shore and waterway protection one must first clarify what the threats are. In many cases the sinking of a ship in narrow waterways can disrupt traffic for a long period of time, causing major economic damage. Sinking an oil tanker and causing an oil spill will add an ecological (and further financial) dimension to the attack. Another threat may be the landing of illegal's or even terrorists on the shores. Since shores cannot be closed with fences, and the public normally demands free access to them, it is necessary to intercept such operations before they are able to land ashore (McNicholas, 2002).

The number of port entrances and exits should be limited to a minimum and their purposes specifically defined. There should be separate gates for pedestrians and vehicles. Likewise, there should be separate gates for the entrance and exit of trucks transporting containers/cargo and those vehicles driven by employees, vendors, clients, and visitors. Physically, the gates should be constructed so as to meet the same minimum standards as the chain link perimeter barrier. These gates should lock with heavy-duty padlocks and the keys controlled by security personnel. A security gatehouse should be located at each primary access point. The gate house should have the basic items required to accomplish the tasks, such as a fire extinguisher, first aid kit, flashlight, rain gear, vehicle and visitor gate logs, 24-hour chronological security logbook, personnel authorization roster, telephone, emergency telephone notification list, security post orders, and a copy of the Emergency Action Plan. (MC Nicholas, 2002)

All access points (gates) into the port should be strictly controlled and there should be a comprehensive policy and specific written procedures which define the access of persons (employees, visitors, contractors, truck drivers, ship chandlers, etc.), vehicles (employee and visitor cars, trucks, etc.), and items (cargo, containers, trailers, ship's goods, spare parts, etc.) into and out of the port. "Authorized Personnel only", "Identification Checkpoint" and "Subject to Search upon Entry and Exit" signs should be posted and highly visible at all access points. Security officers posted at pedestrian gates should stop and challenge all persons, inspect their identification badges, and search any boxes, briefcases, or other items for contraband. Employees should present their ID badges to the security officer upon entrance and exit and wear their badges at all times while in the port. All visitors (clients, vendors, contractors, etc.) should be stopped at the gate, their visit confirmed with the sponsoring port employee, a temporary badge issued and visitor log completed, and any items opened and inspected for contraband. The interior and trunks of all vehicles should be visually checked for contraband. No privately-owned vehicles should be permitted inside the terminal. All trucks entering the cargo gates should be stopped, the driver's license checked for validity, the cab inspected for contraband and unauthorized persons, container seals inspected, and relevant information recorded on a comprehensive gate log (McNicholas, 2002).

3.2.4 Security awareness

Security awareness is vital to the safety, security and health of port personnel and others having a place of work in the port, which should be made aware of their responsibilities to fellow workers, the port community and the environment. Appropriate training of personnel working in the port should maximize personal awareness of suspicious behaviour, incidents, events or objects when going about daily tasks, and the invaluable contribution to be made to the security of the port and its personnel by each individual. Security awareness has been identified as another major cause for Security Breaches and Incidents ports. During the interviews with port authorities and recent academic researches; we detected two main sub-causes about security awareness. Lack of accidents/breaches statistics is the first part. Lots of ports and ships do not report the accidents or any security breaches especially comparing with other subjects relating to the shipping such as statistic of non-conformities during the inspections, near miss reporting, vessels performances, etc. That's why, a question; "Do the statistics give reliable information?" emerges. Unless the authorities can detect the security breaches and incidents, evaluation of the ISPS Code cannot be done in a reliable manner. Hence, security awareness notion must be mentioned in all areas regarding the ISPS Code and security. In the second sub-cause of this part; lack of sharing experience and feedbacks was detected. Sharing information is significant to prevent security breaches. Historical part of security and every type of experience must be shared. And also this notion can be put into the ISPS Code courses’ curriculum.

3.2.5 Vessel types

Given the role small vessels have played in the tragic 2000 attack on the *USS Cole*, and the apparent maritime link to the 2008 Mumbai attacks, it is understandable that in recent years attention have turned to small vessel security. The Strategy identified the following four scenarios of greatest concern that small vessels could pose in terrorist-related attacks (*url 6*):

1. Domestic use of waterborne improvised explosive devices
2. Conveyance for smuggling weapons (including weapons of mass destruction)
3. Conveyance for smuggling terrorists; and
4. Waterborne platform for conducting a stand-off attack

It would be relatively easy for a terrorist organization to acquire or commandeer a small vessel to conduct a terrorist attack. Another major concern was that, depending on the target, terrorists would be more likely to acquire small vessels to be used in terrorist attacks from foreign countries to other countries. Terrorists have demonstrated their intention to use small vessels to harm U.S. interests. For example, on October 12, 2000, the USS COLE was attacked by al-Qaida suicide bombers using a small vessel loaded with explosives while she was harboured in the Yemeni port of Aden. The resulting explosion killed 17 sailors and injured 39 others. Moreover, the use of a small vessel as a platform for conducting a stand-off attack cannot be discounted. In August 2005, terrorists fired rockets at two U.S. warships docked in Aqaba, Jordan. While in that case the platform was a local warehouse, pirates have also used small vessels as a platform for stand-off attacks. In November 2005, a cruise liner was attacked by two 25-foot rigid hull inflatable boats 100 miles off the coast of Somalia. The pirates used rocket-propelled grenades and automatic weapons, and were repelled by the crew of the passenger vessel M/V SEABOURN SPIRIT using a sonic blast, and by increasing to full speed and outrunning the pirates *(url 6).* The problem at that point is detection of the small vessels. Small crafts packed with explosives are very effective in their attacks, as demonstrated in the attacks on the USS Cole and the M/V Limburg (Murphy, 2008).

Small crafts are possibly threats for ports due to their size and high speed. The results of an attack by a speed craft filled with bombs to a port which stationed in the metropolis can be very painful. That’s why the academicians and port authorities pay attention to the detection of small vessels. Their negative impact is proved several times. Therefore, fishing vessels are also important in this type. This was clearly demonstrated in the Mumbai attack when the attackers arrived in a hijacked fishing trawler (Goh, 2006). As a result, we can mention that small vessels are a sub cause of “vessel type” problem and possible threats for ports.

3.2.6 Risk Management

In the past, safety management and regulation was usually introduced as a result of an accident/incident or a series of accidents/incidents. It has now become necessary to take a proactive approach toward safety that aims to identify risks and then to control them. This has to be undertaken in a way that constantly updates identification and mitigation of risks in any process or organization. In marine organizations interfacing with or influencing marine operations this has never been more important, due to the very high cost and wider implications of maritime accidents (*url 7*).

The terrorist events of September 11, 2001 provide a good illustration of the challenges facing states and metropolitan areas in preparing for and responding to unexpected security incidents or natural disasters. Given the suddenness of the terrorist incidents and their unexpected nature, it is not surprising that there was some confusion and lack of coordination in managing the transportation system in the aftermath. One lesson from September 11th is paramount—effective coordination and communication among the many different operating agencies in a region and across the nation is absolutely essential. Such coordination is needed to allow enforcement/security/safety responses to occur in an expeditious manner, while at the same time still permitting the transportation system to handle the possibly overwhelming public response to the incident. Complementary to this is the need to make sure the public has clear and concise information about the situation and what actions they should take. The September 11, 2001 terrorist incidents have focused attention on large scale, area wide responses to sudden terrorist incidents. There is a wide range of such incidents that could cause varying levels of disruption to the transportation system (Mayer, 2008).

In fishbone diagram, six generic headings are created to prompt ideas. According to our research “Risk Management Process” is detected as one of the six causes. In our interviews and brainstorming sessions, we realized that most of the academicians and port authorities pay attention to risk management problem. They believe that a risk management which carried out in an intelligent way can solve most of the problems. But, risk profiles vary regionally. The problem begins at that point. Threats consist of internal and external effects which change depending on social and political effects. The port managers and security personnel must be wise and well-educated to evaluate the possible risks in a correct way by paying attention both internal and external effects. When the topic is evaluated from the context of ISPS implementations, it is noticed that ISPS Code is only guidance to assess these threats and take suitable measures against any of them. ISPS Code determines the frame for assessing and managing risks changing all around the world. Therefore, standard applications for all nations which are in different regions are suggested by ISPS. This is another sub-cause. In brief; different threats but standard applications. For example, the Port of Rotterdam focuses primarily on the dangers of terrorist attacks on containers or mass goods (such as oil), while the Port of New Orleans has faced natural disaster (e.g. hurricane Katrina) and its consequences (Wenning et al., 2007). At that point, countries fell them under threat and produce their own solutions. Australia, Canada, Sweden and New Zealand, for example, have legislated new measures to strengthen their cargo security programmes in line with American security standards, for example the Container Security Initiative (Peterson & Treat, 2008). On a European level, American security standards are integrated by the EU’s Authorized Economic Operator (AEO), almost entirely similar to the American Customs-Trade Partnership against Terrorism (C-TPAT) (Url 8). As a result, we can mention that threats vary both internally and externally according to regions but applications are standard in all regions. Therefore, the duties of contracting governments begin at that point. To access and manage the possible risks, well-educated and experienced security personnel need is obvious. Governments also have to assess and manage risks with balancing financial limitations. Financial limitations prevent to make a risk management and security in a successful way. But, every government must meet up to the expectations of the IMO, and ports have thus become barometers of security, to be subject to unannounced inspections by Port State Control and to Port Facility Security Assessments (George & Whatford, 2007). But, vague regulations and suggestions about risk management compel governments to execute their own initiatives. Hence, the applications can be different in the same region and states produce their own solutions to security breaches. According to Pedersen (Pedersen, 2010), different principles must be used to formulate risk criteria depending on the nature of the consequence in question. For example, there must be a special focus on incidents with several fatalities because society considers these incidents more severe than multiple incidents with few fatalities. It is therefore reasonable to assume that the risks associated with ship security, that is, piracy and other types of crime at sea, require specific risk criteria as the consequences (possible great human suffering and multiple fatalities) that are incomparable with the traditional operational risks encountered in shipping. According to NATO, security measures are used not only to minimize the vulnerability of personnel and material but also to preserve freedom of action and operational effectiveness (NATO Standardization Agency, 2007).

Some examples of Risk Assessment Management Systems & Methods and security initiatives are given below:

3.2.6.1 AS/NZ 4300-1990 port & harbour risk assessment and safety management systems in New Zealand

According to this system; the assestment has to start with identification of hazards. Once a hazard is identified, frequency ((likelihood, probability or chance) of a hazard realisation) and consequence ((severity or impact) of the hazard reaching its potential) data can be added, the result is risk. It is beneficial for a regional council or port company to adopt this approach as it provides answers to determine the priority of risk control within the harbour or port. This allows a Port and Harbour Safety Management System to be introduced in manageable stages, concentrating first on those defenses which control higher risks.

Risk assessment techniques are fundamentally the same for large or small ports or harbours, although the execution and detail will vary considerably. For a large port or harbour, the task is large and, if done to a sufficient level of detail, complex. It is thus much better to insert a structure through the whole assessment from the beginning and carve the work needed into manageable packages. In a port or harbour risk assessment, the following five stages are appropriate:

- Stage 1 Data Gathering and System Assessment
- Stage 2 Hazard Identification (HAZID Meeting)
- Stage 3 Risk Analyses
- Stage 4 Assessment of existing risk management strategies, development of new measures; Assessment of Control Adequacy Rating
- Stage 5 Managing and Treating the Risk via the Port and Harbour Safety Management System.

3.2.6.2 The threat and risk analysis matrix (TRAM)

The threat and risk analysis matrix (TRAM) is a simplified risk-based method and tool to assist in carrying out a port security assessment (PSA). Its purpose is to identify threats with a view to initiating and recommending countermeasures to deter, detect and reduce the consequences of any potential incident, should it occur. In addition to the more obvious threats, the list of potential targets should be as comprehensive as possible with due regard to the function(s) of the port, legal, political, social, geographic and economic environment of the country, and the security environment specific to the port.

3.2.6.3 The container security initiative

The globalization of the world economy and the increasing threat of terrorism have placed pressure on the world's governments, especially Customs administrations. Merchants have demanded faster, more standardized and uniform service while governments require more revenues and more secure borders. At the same time Customs must produce trade statistics and enforce other agency laws (i.e. health, intellectual property, etc.) at the nation's border. Customs are faced with the prospect of balancing the requirement of facilitation with the increased importance of security enforcement as a consequence to the emerging terrorist threats. To deal with security threats posed by container shipping, The US Custom Service is proposed The Container Security Initiative to identify high-risk containers and secure them with tamper-detection systems. The initiative aims to expedite processing of containers pre-screened at points of embarkation in overseas mega ports participating in the initiative (Stanford, 2003). The US CSI consists of four core elements (Banomyong, 2005). These are:

1. to establish security criteria to identify high risk containers;

2. to pre-screen those ocean going containers identified as high risk before they arrive at US ports;

3. to use advance technology to quickly pre-screen high-risk containers;

4. to develop the use of smart and secure ocean going containers.

3.2.6.4 The customs trade partnership against terrorism

C-TPAT is a US Customs and Border Protection (CBP) voluntary joint government-business initiative to build cooperative relationships that strengthen overall supply chain and border security. C-TPAT recognizes that Customs can provide the highest level of security only through close cooperation with the ultimate owners of the supply chain, importers, carriers, brokers, warehouse operators, and manufacturers. This initiative asks that business work to ensure the integrity of their supply chain processes and business partners, and successfully maintain open communication of their status (*url 9*).

3.2.6.5 Operation safe commerce

OSC funds pilot programs that are meant to enhance and complement other security initiatives, such as C-TPAT and CSI, by testing technologies and business processes that protect commercial shipments from tampering all along the supply chain, from point of origin to point of destination. For a project to be funded, it must accomplish one or more of the following tasks to secure the supply chain:

- Validate security at the point of origin, to include the security of the shipment itself and the information that describes it;
- Secure the supply chain from the point of origin to its final destination and all the points in between; and Monitor the movement and integrity of the cargo while in transit using available technology (Haveman, 2005).

3.3 Assessment of the ISPS Code via Pareto Analysis

In this paper, Pareto charts were prepared for all the criteria to identify major causes in implementation of the ISPS Code. After the causes were found via Fishbone Diagram, questionnaire was prepared in order to identify major causes. In the questionnaire; academicians, port authorities and ship masters were asked about the evaluation of problems regarding quality of the ISPS Code such as Risk Management, Security Awareness, Standardization, Vessel Type, Training and Monitoring & Surveillance Process. In the questionnaire the participants graded the causes to 1 to 6 point according to importance level. The most important cause point was 6. It decreased one by one up to one that was defined as most trivial cause. The results of the questionnaire regarding the importance level of causes of deficiencies are shown in the table 3.1.

After graphing the marks, table 3.1 was constituted. The percentages and the cumulative percentage which would be helpful to find the breakpoints was calculated and indicated in the below table.

Table 3.1 : The pareto analysis of "Security Breaches and Incidents for Ports".

Causes	**Resultsof Questionnaire**	**Percentages**	**Cumulative Percentage**
Training	207	25,2	25,2
Security Awareness	171	20,8	46,1
Risk Management	156	19,04	65,2
Standardization	150	18,31	83,5
Monitoring and Surveillance	96	11,7	95,2
Vessel Types	39	4,76	100

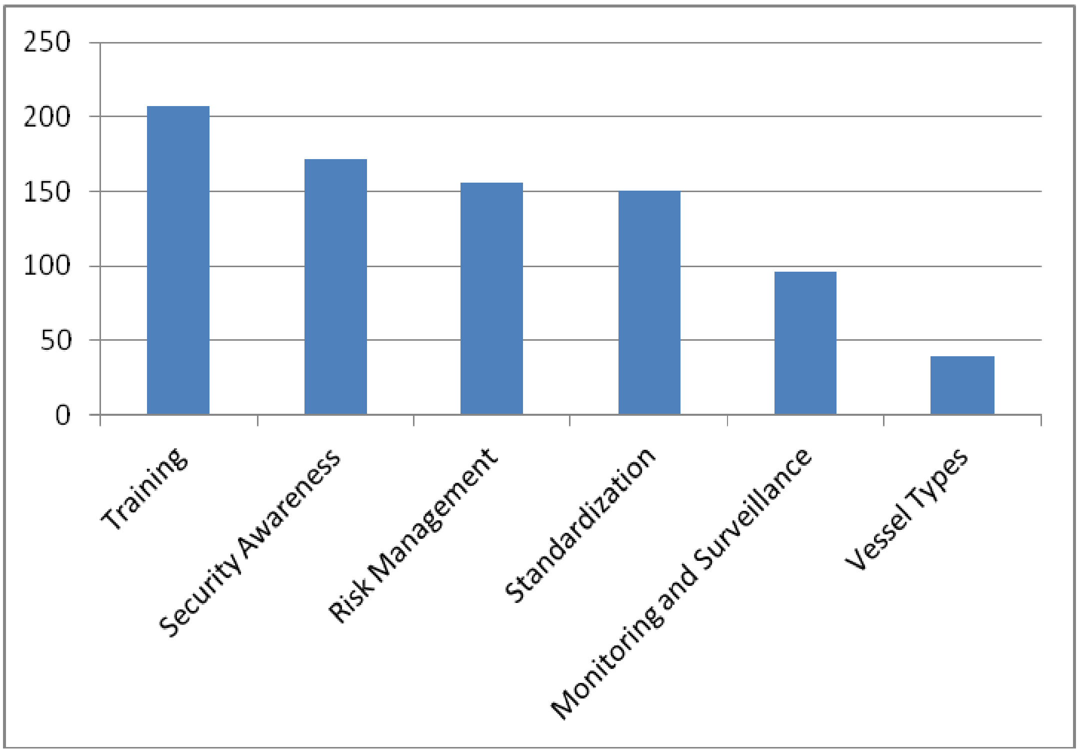


Figure 3.3 : The results of the questionnaire - bar chart.

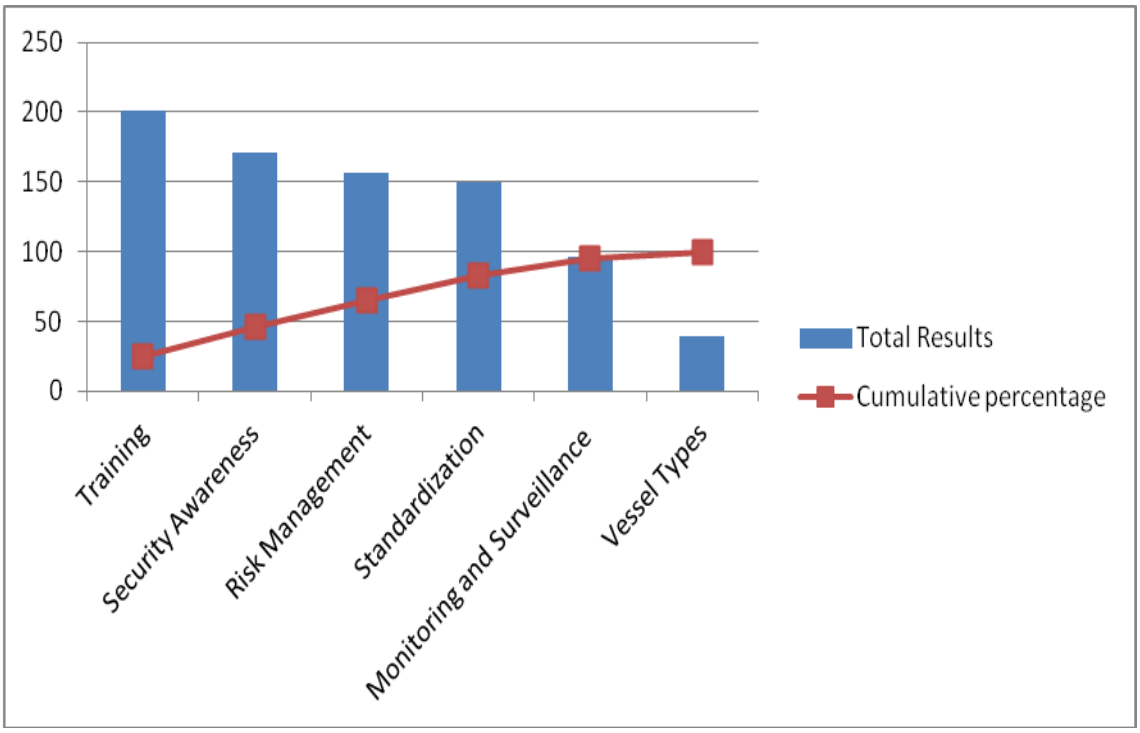


Figure 3.4 : The pareto analysis - bar chart and line chart.

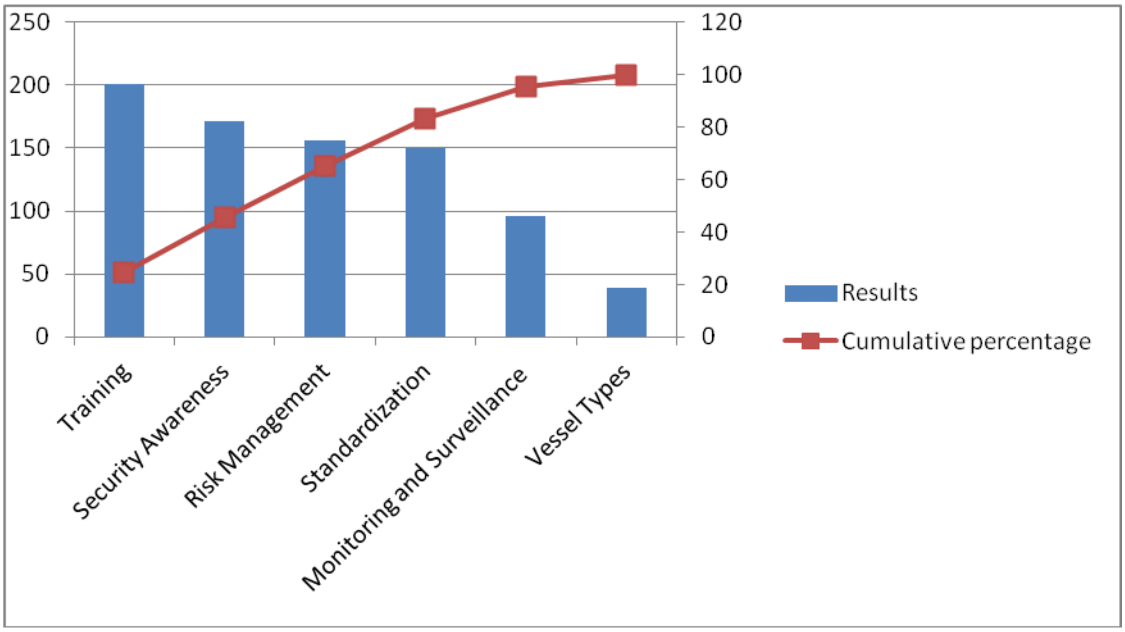


Figure 3.5 : The pareto analysis - bar chart and line chart.

As seen in the diagrams, there are 2 break points in the cumulative percentage line. These points occur when the scope of the line begins to flatten out. The factors under the steepest part of the curve are the most important. Hence, training has the most significance level compared to other causes. Security awareness, risk management and standardization have approximately same importance level and more important when compared to the monitoring & surveillance process and vessel types. According to break points; monitoring & surveillance process and vessel types have the lesser significance level compared to the causes in left side which is illustrated in figure 3.4 and figure 3.5 respectively.

3.4 Assessment of the ISPS Code via Cognitive Mapping

Cognitive-mapping method is used to determine the relationship between the causes and sub causes which was identified in Fish-bone diagram to see how the causes and sub causes affect each other.

3.4.1 Analysing of the causes of security breaches and incidents for ports

When the Risk management process (Cause A), which is determined one of the main cause of Security Breaches for Port, analysed; its sub-causes as follows: Different threats both internally and externally, Standard applications in all regions, Individual initiatives of contracting governments

Table 3.2 : Cause A: risk management process.

A_1= Different threats both internally and externally

A_2= Standard applications in all regions

A_3= Individually initiatives of contracting governments

When the Security awareness (Cause B), which is determined one of the main cause of Security Breaches for Port, analysed; its sub-causes as follows: Lack of accidents / breaches statistics, Lack of sharing of experience and feedbacks

Table 3.3: Cause B: security awareness.

B_1= Lack of accidents / breaches statistics

B_2= Lack of sharing of experience and feedbacks

When the Standardization (Cause C), which is determined one of the main cause of Security Breaches for Port, analysed; its sub-causes as follows: Lack of technological devises, Physical security standards

Table 3.4: Cause C :standardization.

C_1= Lack of technological devises

C_2= Physical security standards

When the Vessel types (Cause D), which is determined one of the main cause of Security Breaches for Port, analysed; its sub-cause as follows: Small and fishing vessels inspection

Table 3.5: Cause D: vessel types.

D_1= Small and fishing vessels inspection

When the Training (Cause E), which is determined one of the main cause of Security Breaches for Port, analysed; its sub-cause as follows: Lack of curriculum, Government education, RSO expertise, Lack of security education

Table 3.6 : Cause E: training.

E_1= Lack of curriculum

E_2= Government education

E_3= RSO expertise

E_4= Lack of security education

When the Monitoring and surveillance process (Cause F), which is determined one of the main cause of Security Breaches for Port, analysed; its sub-cause as follows: Passenger ship entrance, Container security, Access control, Sea side control

Table 3.7 : Cause F: monitoring and surveillance process.

F_1= Passenger ship entrance

F_2= Container security

F_3= Access control

F_4= Sea side control

3.4.2 Establishment of relationship matrix

The cognitive map may be transformed into a matrix format and the relationships may be represented in this matrix called the “valency matrix”. The valency matrix A is a square matrix of n X n where n is the total number of concepts in the corresponding cognitive map. A is a signed matrix composing of the values (vij) representing the strength of the relations between the variables in the map. vij =1 If a positive relationship from i to j is present in the cognitive map, -1 if a negative relationship from i to j is present and 0 if the variables are unrelated. The diagonal elements in the map are considered to be 0. The valency matrix has a number of useful properties: The sum of the absolute values of the elements of a row i gives the outdegree (od) of concept i, that is, the number of concepts perceived to be affected directly by concept i. Similarly, the column sum of the absolute values of the elements of column i gives the indegree (id) of concept i, the number of concepts perceived to affect concept i directly. The sum of the indegree and outdegree for concept i gives the total degree (td) of concept i, a useful operational measure of the concept’s cognitive centrality in the decision maker’s belief structure (Nozicka et.al., 1976).

3.4.3 Detection of centrality values for concepts

Centrality of a concept is a measure in application of cognitive mapping approach. Centrality means a reference point to indicate the importance of a concept in a map (Eden et al., 1992). To compute the centrality, the row/column sums of the absolute values (means the direction of the links is ignored) of existing relations are principally considered (Çelik, 2010). Figure 3.6 gives the computed centrality values for each concept of the problem at hand.

	A1	A2	A3	B1	B2	C1	C2	D1	E1	E2	E3	E4	F1	F2	F3	F4
A1		0	+	0	0	0	0	0	0	0	0	0	+	+	+	+
A2	-		0	0	0	-	+	0	-	+	+	-	+	+	+	+
A3	-	0		0	0	-	+	+	-	+	+	-	+	+	+	+
B1	0	0	0		+	0	0	0	+	0	-	+	0	0	0	0
B2	0	0	0	+		0	0	0	+	0	-	+	0	0	0	0
C1	+	0	0	0	0		-	-	+	-	-	+	-	-	-	-
C2	-	0	0	0	0	-		+	-	+	+	-	+	+	+	+
D1	-	0	0	0	0	0	0		0	0	0	0	0	0	+	+
E1	+	0	0	0	0	0	0	0		-	-	+	-	-	-	-
E2	-	0	+	0	0	0	0	+	-		+	-	+	+	+	+
E3	-	0	+	0	0	0	0	+	-	+		-	+	+	+	+
E4	+	0	0	0	0	0	0	0	+	-	-		-	-	-	-
F1	-	0	0	0	0	0	0	0	0	+	+	0		0	+	0
F2	-	0	0	0	0	0	0	0	0	+	+	0	0		+	0
F3	-	0	0	0	0	0	0	+	0	+	+	0	+	+		+
F4	-	0	0	0	0	0	0	+	0	+	+	0	0	+	+	

Figure 3.6 : Centrality values for concepts.

Centrality values for each concept		**Priority order of centrality values**	
Causes	Centrality values	**Causes**	**Centrality values**
A1	18	**E3**	23
A2	11	**E2**	21
A3	15	**F3**	19
B1	5	**A1**	18
B2	5	**E1**	17
C1	14	**E4**	17
C2	14	**F4**	17
D1	10	**F2**	15
E1	17	**A3**	15
E2	21	**F1**	14
E3	23	**C1**	14
E4	17	**C2**	14
F1	14	**A2**	11
F2	15	**D1**	10
F3	19	**B1**	5
F4	17	**B2**	5

Figure 3.7 : Centrality values for each concept /Priority order of centrality values.

In the above table, six causes and sub causes of each, which have been found by fishbone diagram was applied to cognitive mapping method and their centrality values are determined. If we array each causes in itselves;

The graphical representation of centrality values of the sub-causes of Cause A is shown in figure 3.8.

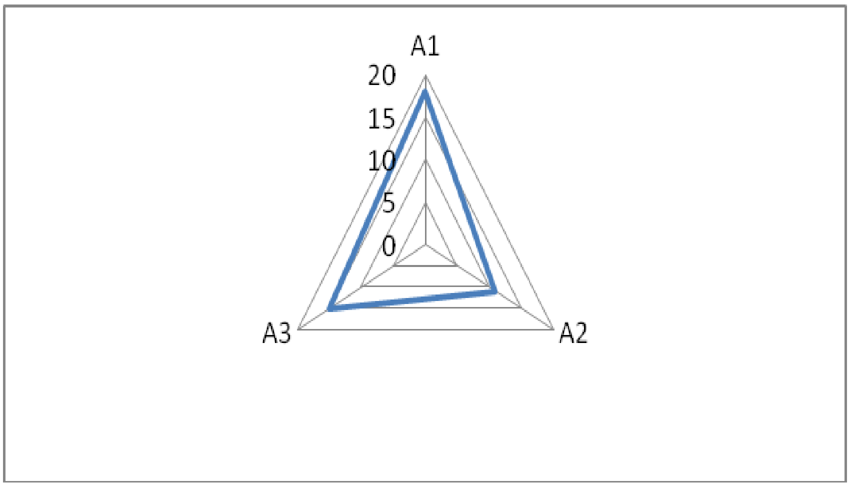


Figure 3.8: Centrality values of cause A.

The graphical representation of centrality values of the sub-causes of Cause B is shown in figure 3.9.

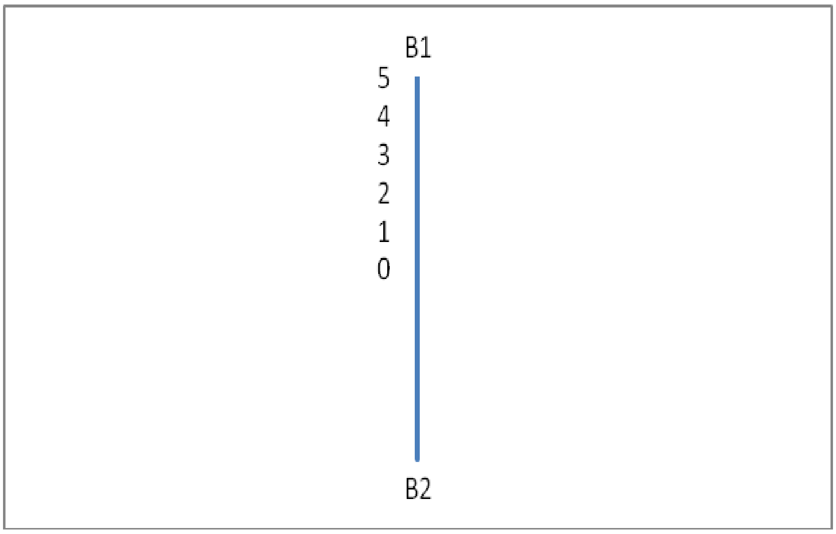


Figure 3.9 : Centrality values of cause B.

The graphical representation of centrality values of the sub-causes of Cause C is shown in figure 3.10.

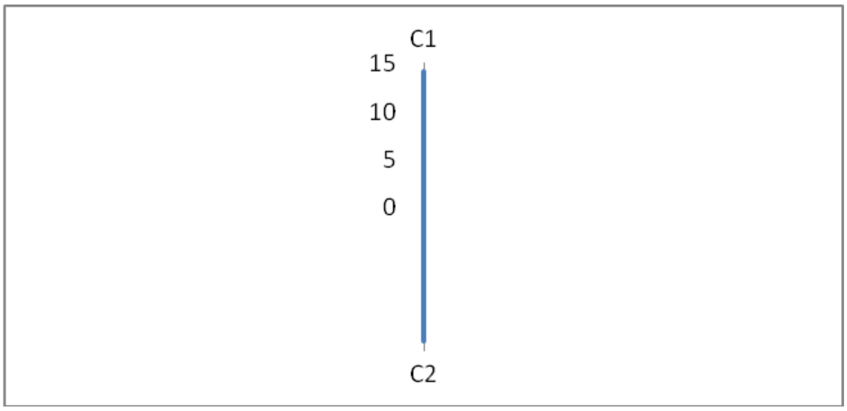


Figure 3.10 : Centrality values of cause C.

Because of Cause D has only one sub-cause, no comparison can be done.

The graphical representation of centrality values of the sub-causes of Cause E is shown in figure 3.11.

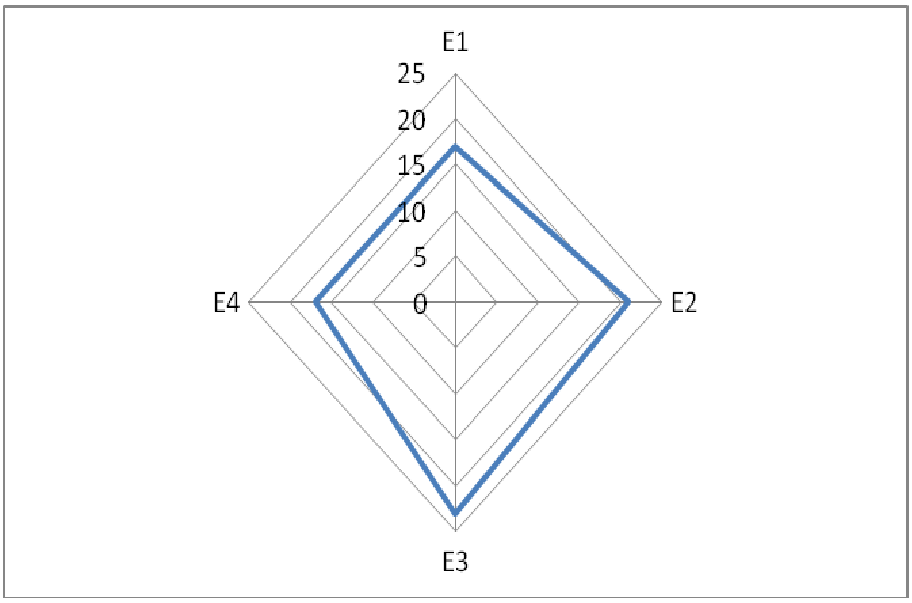


Figure 3.11 : Centrality values of cause E.

The graphical representation of centrality values of the sub-causes of Cause F is shown in figure 3.12.

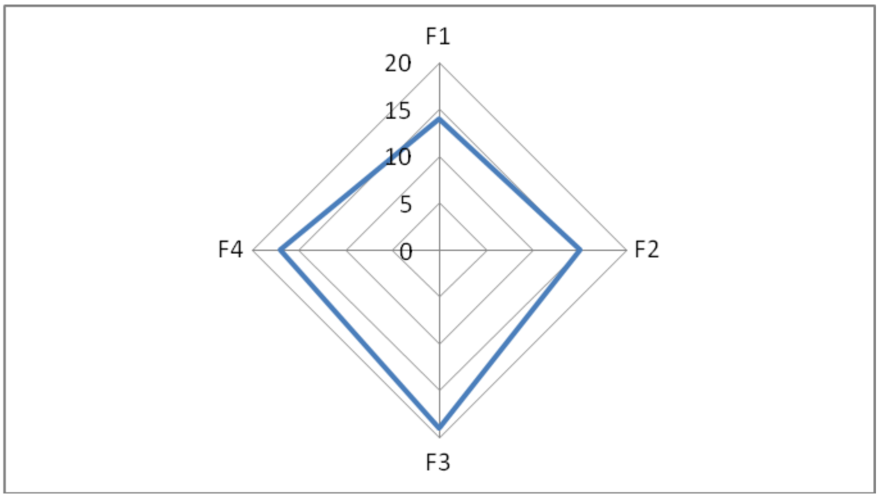


Figure 3.12 : Centrality values of cause F.

Furthermore, after analyzing the centrality values of six causes and sub causes of each in itselves, cognitive mapping technique is applied to find the casual relationship among all causes and sub causes. Below figures schematize the focused problem in accordance with the cognitive mapping principals. It is discussed for each cause separately from other causes. The blue lines show the negative casual relation (-) while the lines with red color indicate the positive casual relation (+).

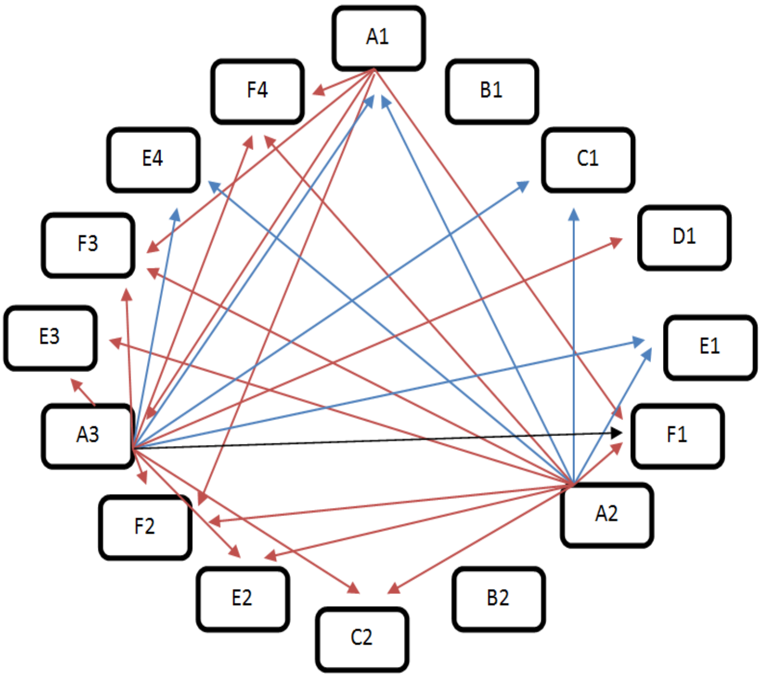


Figure 3.13: Cognitive mapping of Isps Code implementation/Cause A.

When the Cause A is analysed; centrality values of sub causes A1, A2 and A3 are respectively 18, 11 and 15.

A_1= Different threats both internally and externally

A_2= Standard applications in all regions

A_3= Individually initiatives of contracting governments

If we approach the analysis in itself, A1 has the biggest importance in comparison with A3, and A3 is more important rather than A2. If we approach the analysis in whole sub causes A1 is the 4th rank in among the 16 sub causes while A2 is the 13th and A1 is the 9th rank.

When cognitive mapping technique results and Pareto analysis results are compared with each other related to Cause A; results are compatible with the rank 3rd among 6 causes.

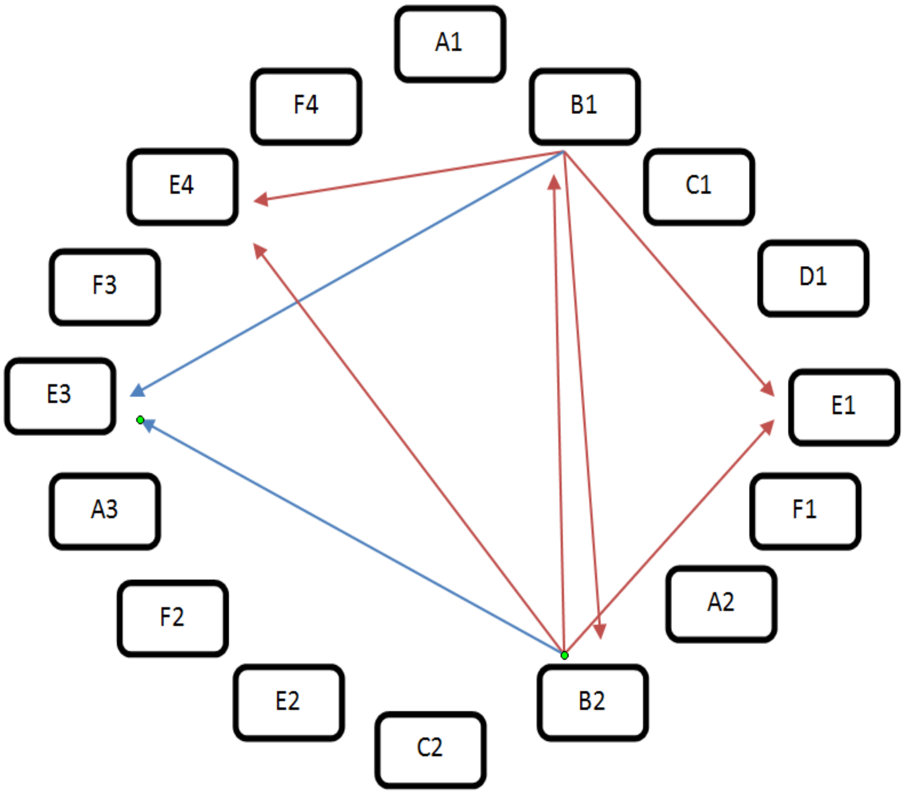


Figure 3.14 : Cognitive mapping of Isps Code implementation/Cause B.

When the Cause B is analysed; sub causes B1 and B2 has the same centrality values with 5 and when compared with the whole sub causes in this study, Cause B is one of the least important according to the cognitive mapping diagram.

B_1= Lack of accidents / breaches statistics

B_2= Lack of sharing of experience and feedbacks

When cognitive mapping technique results and Pareto analysis results are compared with each other related to Cause B; results are not compatible. While Cause B is the 2nd rank among 6 causes in Pareto analysis, it is the 6th in cognitive mapping technique. In this case, we can say that even the security awareness in one of the most important reason that affect implementation of the ISPS Code, but not stimulate other causes.

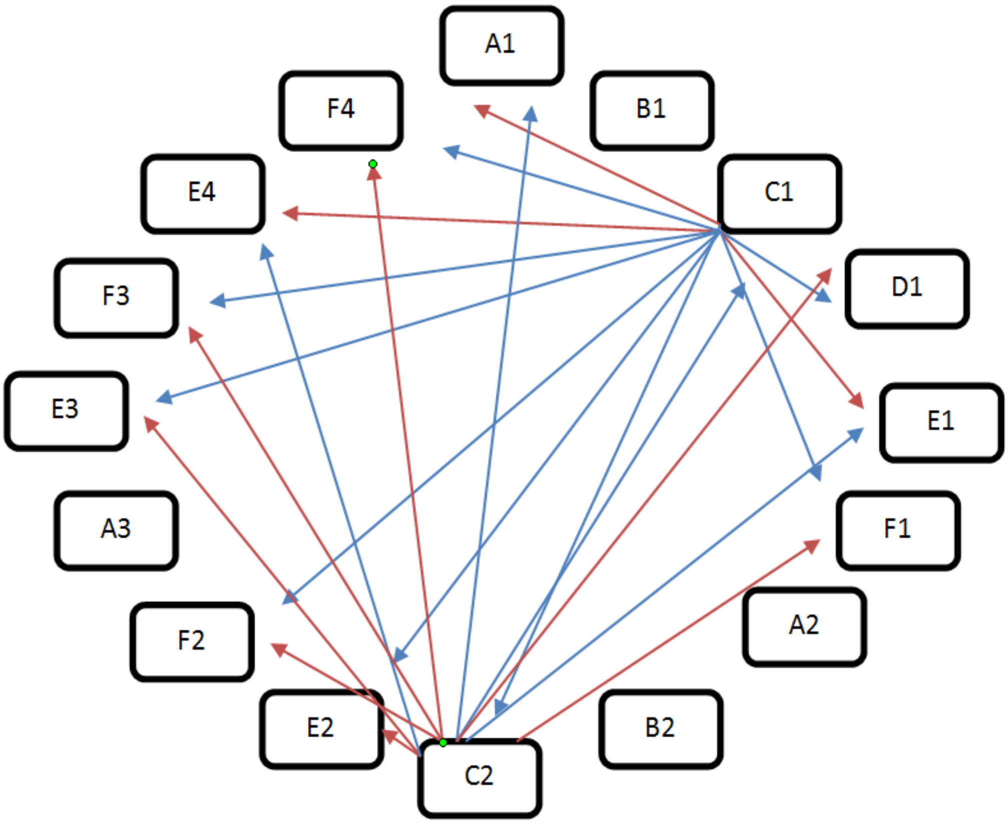


Figure 3.15 : Cognitive mapping of Isps Code implementation/Cause C.

When the Cause C is analysed; sub causes C1 and C2 has the same centrality values with 14 and when compared with the whole sub causes in this study, Cause B is the least important according to the cognitive mapping diagram.

C_1= Lack of technological devises

C_2= Physical security standards

If we approach the analysis in itself, C1 and C2 have the same centrality values with 14. When cognitive mapping technique results and Pareto analysis results are compared with each other related to Cause C; results are compatible with the rank 4th among 6 causes.

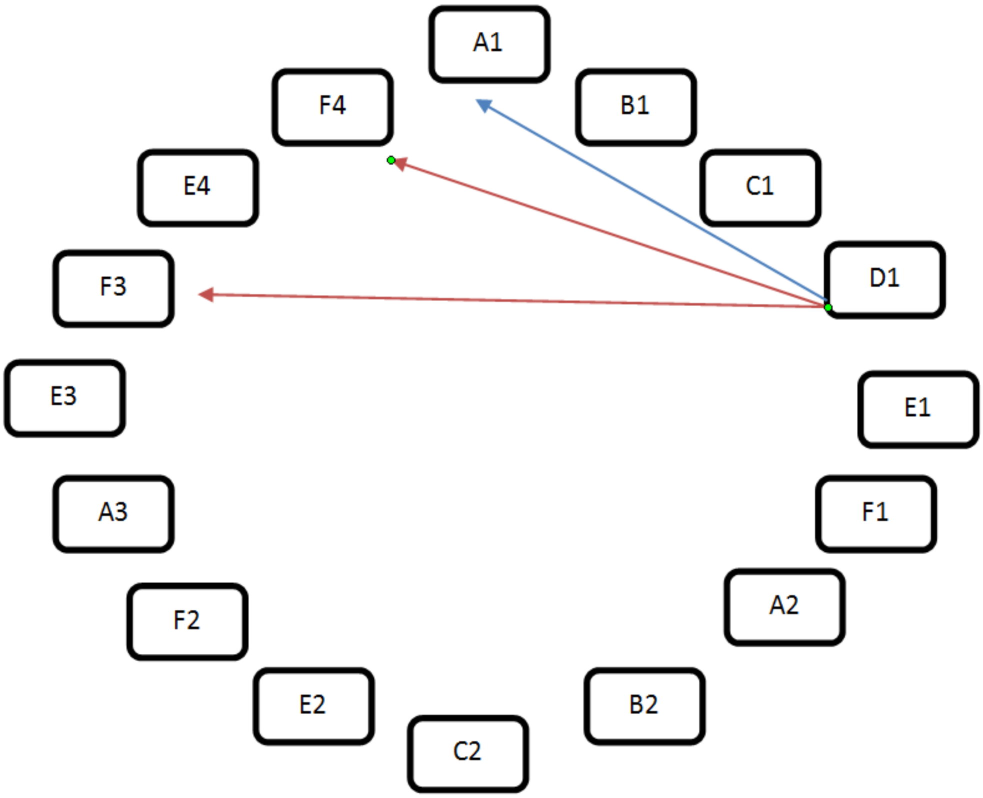


Figure 3.16 : Cognitive mapping of Isps Code implementation/Cause D.

When the Cause D is analysed; its sub cause has centrality value with 10. When compared with the whole sub causes in this study, Cause D has very less importance according to the cognitive mapping diagram.

D_1= Small and fishing vessels inspection

When cognitive mapping technique results and Pareto analysis results are compared with each other related to Cause D; results are compatible with the rank 5th among 6 causes in cognitive mapping techniques, and 6th among 6 causes in Pareto analysis.

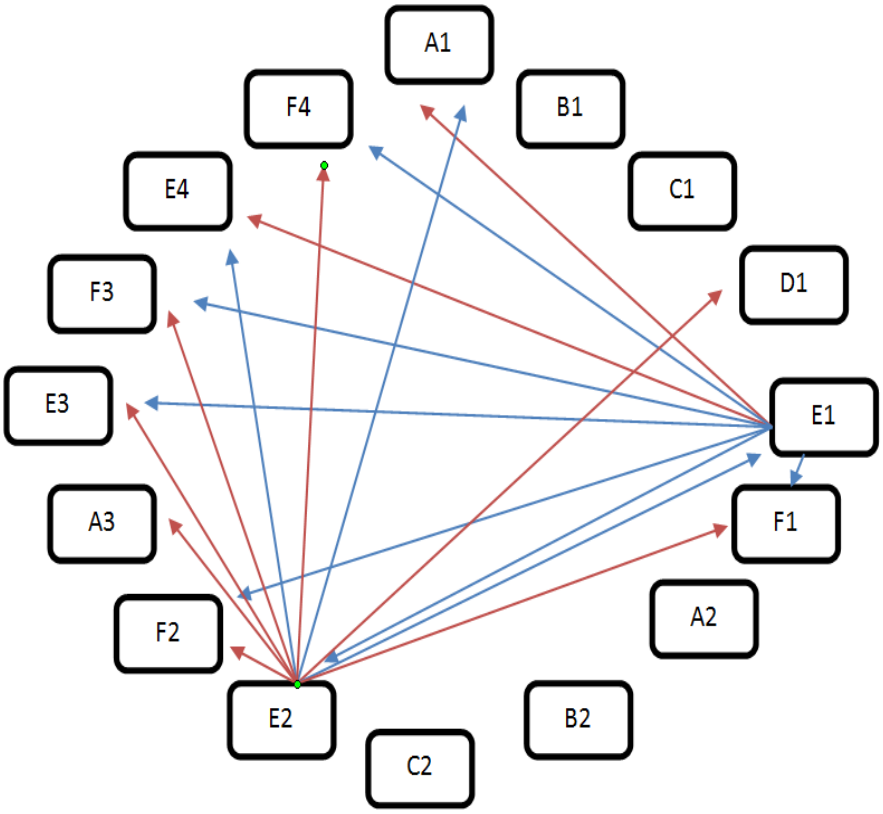


Figure 3.17 : Cognitive mapping of Isps Code implementation/Cause E.

When the Cause E is analysed; centrality values of sub causes E1, E2, E3 and E4 are respectively 17, 21, 23 and 17.

E_1= Lack of curriculum

E_2= Government education

E_3= RSO expertise

E_4= Lack of security education

If we approach the analysis in itself, E3 has the biggest importance in comparison with E2, and E2 is more important rather than E1 and E4. If we approach the analysis in whole sub causes E3 has the highest rank in among the 16 sub causes.

When cognitive mapping technique results and Pareto analysis results are compared with each other related to Cause E; results are compatible with the rank 1st among 6 causes.

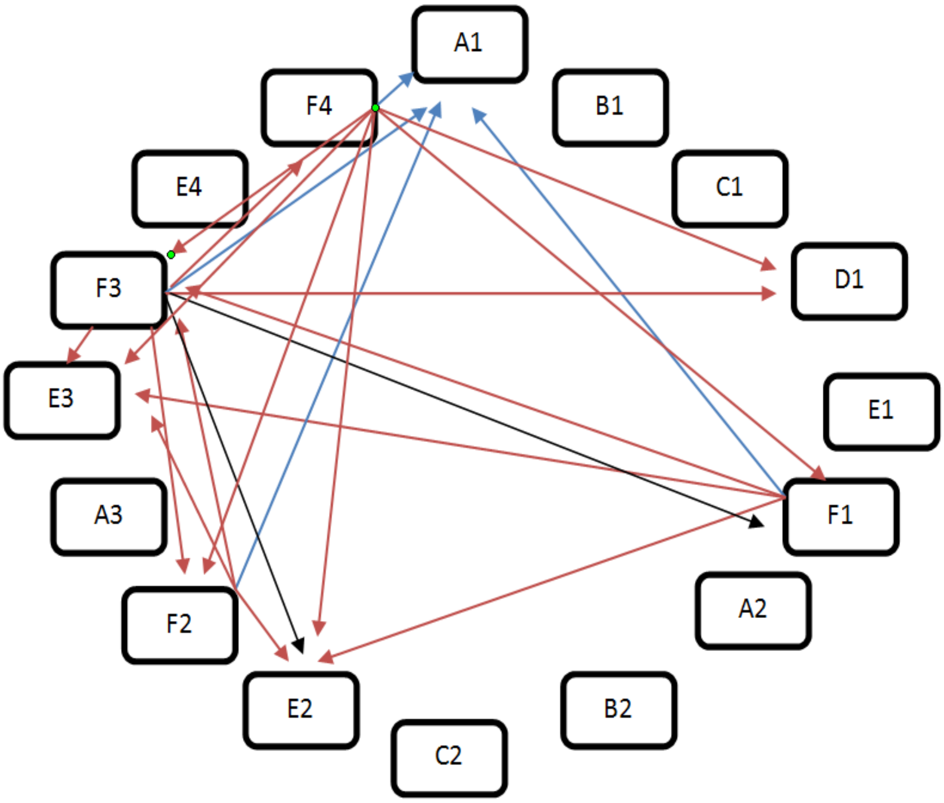


Figure 3.18 : Cognitive mapping of Isps Code implementation/Cause F.

When the Cause F is analysed; centrality values of sub causes F1, F2, F3 and F4 are respectively 14, 15, 19 and 17.

F_1= Passenger ship entrance

F_2= Container security

F_3= Access control

F_4= Sea side control

If we approach the analysis in itself, F3 has the biggest importance in comparison with F4, and F4 is more important rather than F2 and F1.

When cognitive mapping technique results and Pareto analysis results are compared with each other related to Cause F; results are not compatible. While Cause F is the 2nd rank among 6 causes in cognitive mapping technique, it is the 5th in Pareto analysis. In this case, we can say that even the monitoring and surveillance process has less importance among other causes; it stimulates other causes to generation.

Comparison of the results from the highest priority to lowest priority is given at table 3.8.

Table 3.8 : Comparison of the results.

Results via Pareto Analysis	*Results via Cognitive Mapping Technique*
1. Training	1. Training
2. Security Awareness	2. Monitoring & Surveillance Process
3. Risk Management Process	3. Risk Management Process
4. Standardization	4. Standardization
5. Monitoring & Surveillance Process	5. Security Awareness
6. Vessel Types	6. Vessel Types

4. RESULTS AND DISCUSSION

Maritime transport is the backbone of international trade and a key engine driving globalization. Around 90 per cent of global trade by volume and over 70 per cent by value is carried by sea and is handled by ports worldwide. Twenty-four hours a day and all year round, ships carry cargoes to all corners of the globe. This role will continue to grow with the anticipated increase in world trade in the years to come as millions of people are expected to be lifted out of poverty through improved access to basic materials, goods and products. World trade and maritime transport are, therefore, fundamental to sustaining economic growth and spreading prosperity throughout the world, thereby fulfilling a critical social as well as an economic function.

Maritime transportation is carried out in water environment. Ports shape the start and the end point of this transportation. Most of the world trade conducted by maritime transport system manifests the particular importance of sea ports, which are an inseparable part of this transport, in terms of presence, necessity and economic activity. In addition to their commercial effects, sea ports have also strategic and socio-economic effects on their regions. Clearly, due to their effects on maritime trade, sea ports are the doors opening to the outside world and breathing points for a country. Ports, ferry and liner terminals are usually established in crowded regions where many people live and work. Every day, billions of cargos and thousands of people go in and out of ports all around the world. Ports, which are the doors of countries opening to the outside world, can become targets for terrorist groups seeking a global impact. Because of transnational flows of goods and people; ports and maritime transport has been exposed to several types of security threats. Piracy, robbery attacks, terrorist attacks, illegal migrations, smuggling, human and drug trafficking are the most noticeable threats. In this sense, security management cannot be left aside from the installation and operating processes of ports. Since maritime transportation generates the backbone of the world trade, effective and applicable security measures are needed to ensure that the international transport system is protected from the acts of above mentioned threats.

The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The ISPS Code is implemented through chapter XI-2 Special measures to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS), 1974. Both SOLAS Chapter XI-2 and ISPS Code entered into force on the 1 July 2004.Although introduction of the ISPS Code have significantly reduced maritime attacks by terrorists since 1 July 2004, recent security breaches and incidents have shown that ISPS Code did not provide desired level of security neither for ships nor port facilities.

In this study “Security Breaches and Incidents for Ports” is determined as main problem. Fish-bone diagram is prepared to illustrate the problems effecting the ISPS Code’s implementation. Through brain-storming sessions, academic researches; and literature review; Risk Management Process, Security Awareness, Standardization, Monitoring and Surveillance Process, Training and Vessel Types are determined as the causes affecting main problem during implementation procedure of the ISPS Code in fishbone diagram technique.

After the causes that affect the ISPS Code’s implementation had been determined, Pareto analysis prepared for all the criteria to identify major causes in implementation of the ISPS Code. Questionnaire was prepared in order to identify major causes. In the questionnaire; academicians, port authorities and ship masters were asked about the evaluation of problems regarding quality of the ISPS Code such as Risk Management, Security Awareness, Standardization, Vessel Type, Training and Monitoring & Surveillance Process. According to Pareto analysis; training was found as the most significant factor compared to other causes. Security awareness, risk management and standardization have approximately same importance level when compared to the monitoring & surveillance process and vessel types. As a cause vessel types is the least important cause that affect implementation of the ISPS Code according to the Pareto analysis.

Finally, Cognitive Mapping method is used to find how the causes and their sub-causes (which have already found via fishbone diagram) affect anothers’ and to see the causal relationship between each other. Centrality values are found and ordered from highest to lowest. According to this method, training is the most important cause of the problem that affects implementation of the ISPS Code. If the causes are arranged by the importance level respectively; training, monitoring & surveillance, risk management, standardization, vessel types and security awareness follow this order.

Training is the most important cause in both Pareto analysis and Cognitive mapping technique. While security awareness is the second rank in Pareto analysis, it has least importance level in cognitive mapping technique. In such a case, we can say that even the security awareness is one of the most important reason that affect implementation of the ISPS Code, it has no stimulating effect on other causes. In the analysis of the causes of risk management, standardization and vessel types; it is seen that results found via Pareto analysis and cognitive mapping are compatible. On the other hand, in the analysis of the cause of monitoring and surveillance, which has less importance level in Pareto analysis, we see that it is in the second rank among 6 causes in cognitive mapping technique. In that case, we can say that it stimulates other causes.

In conclusion, the following suggestions were developed for the enhanced implementation of the ISPS Code to increase the effectiveness of maritime transport system from management level perspective:

1. IMO has to examine the course program and establish a generally accepted curriculum and compel contracting governments to put into force these courses.
2. Contracting governments must increase the inspections on national ISPS Code training courses.
3. Security awareness training must cover all personnel working in the port facilities. New methodologies must be developed for the training/refreshment training of the basic port security guards for the most effective management of the port security duties.
4. To detect and prevent terrorists using small vessels, non-ISPS small vessels security measures must be taken by the public, industry and government officials.

The following suggestions were developed for the enhanced implementation of the ISPS Code to increase the effectiveness of maritime transport system from operational level perspective:

1. All access points (gates) into the port should be strictly controlled and there should be a comprehensive policy and specific written procedures which define the access of persons (employees, visitors, contractors, truck drivers, ship chandlers, etc.), vehicles (employee and visitor cars, trucks, etc.), and items (cargo, containers, trailers, ship's goods, spare parts, etc.) into and out of the port.
2. The ISPS Code must obligate use of technological devices such as CCTV, fingerprint, X-ray scan, facial recognition, underwater security devices and etc and regulate respective training for the most effective employment of these devices.
3. Some best practice initiatives such as CSI (Container Security Initiative), C-TPAT (Custom-Trade Partnership against Terrorism) or contracting governments own solutions must be taken into account in developing global security solutions.
4. Seaside and under water control must be enhanced with more technological devices such as ROV's or with user divers.

Finally, in further studies; this study should be repeated at regular intervals in order to keep up with solution of the problem and follow the developments related to study. Also, this study should be specified with different ports both in different countries also different cities in same countries. Causes that constitute the problem should be detailed with more sub-causes. In addition, each cause and their subcauses should be addressed in a seperate study. Besides, different methods should be used in order to control reability of the study. These studies will enchance the effectiveness of the ISPS Code when proposed to international maritime authorities.

REFERENCES

Al-Shehab, A. J. Hughes, R. T., and Winstanley, G. (2005). “Facilitating Organizational Learning Through Causal Mapping Techniques in IS/IT Project Risk Management”, Lecture Notes in Computer Science, 145,154.

Akten, N. (1992). “Liman Planlaması: Liman Üniteleriyle Kapasitesi Arasındaki İlişki ve Elleçleme Maliyetinin Hesaplanması,” Master thesis, IU, Faculty of Business Administration, pp 20-23.

AS/NZ 4300-1990 Port & Harbour Risk Assessment and Safety Management Systems in New Zealand, Guidelines for Port & Harbour Risk Assessment and Safety Management Systems in New Zealand

Balbaa, A. (2005). - Protecting seafarer’s rights - the need to review the implementation of the Isps Code. Association of Maritime Universities (IAMU) 6th.

Bank, J. (2000). The essence of Total Quality Management. Prentice Hall.

Baran, H. (2010). “*Limanları Etki Alanı Saptanması İçin bir Yöntem önerisi (İzmir Alsancak Limanı)”*, PhD thesis, Institute of Science, Dokuz Eylul University., İzmir. Pp.9-14

Barnes, P., and Oloruntoba, R. (2005). "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management" Journal of International Management, Volume 11, Issue 4, 519-540

Besterfield, D. H. (2009). Quality Control, 8th edition, Pearson-Prentice Hall.

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 & Logistics 6(4), pp.332-348.

Bjornson, F., Wang, A., Arisholm, E. (2009). Improving effectiveness of root causes analysis in port mortem analysis: A controlled experiment. Journal of Information and Technology.

Bolat, F. (2010) “An Analysis of Marmara Region Ports’ Potentials as of Main Hub Ports Features”, PhD thesis, Institute of Science, Istanbul Technical University. Pp.3-15.

Branch, A.E. (1986). "Elements of Port Operation and Management, Chapman & Hall" London, 148.

Burmester, C. (2005). International Ship and Port Facility Security (ISPS) Code: The perceptions of shore-based and sea-going staff. In: Nielsen D (ed.) Maritime Security and MET. Ashurst: WIT Press, pp.185-194.

Carlsson, C., and Fuller, R. (1996). "Adaptive Fuzzy Cognitive Maps for Hyper knowledge Representation in Strategy Formation Process", In: Proceedings of International Panel Conference on Soft and Intelligent Computing, Technical University of Budapest, 43-50.

Chalk, P. (2008). The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States, Santa Monica, CA: RAND Corporation.

Carbonara, N. and Scozzi, B. (2006). "Cognitive Maps to Analyze New Product Development Processes: A Case Study", Technovation, 26, 1233-1243.

Chaibb Draa, B. (1994).Coordination Between Agents in Routine, Familiar and Unfamiliar Situations. Technical Report DIUL-RR-9401, Department de Informatique, Universite

Chang, J., CC, L. (2006). A study of storage tank accidents. Journal of Loss Prevention in the Process Industries; 19, 51-59.

Clarke, I. and Mackaness, W. (2001). "Management Intuition: An Interpretative Account of Structure and Content of Decision Schemas Using Cognitive Maps", Journal of Management Studies, 38 (2), 147-172.

Çelik, M. (2010). Enhancement of occupational health and safety requirements in chemical tanker operations: The case of cargo explosion, Safety Science, 48 (2), Pp. 195-203.

Celik M., and Topcu Y.I. (2010). " Assessment of ISPS Code Compliance at Ports Using Cognitive Maps." TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 4, No. 3, pp. 359-362

Çelik M., Bilgili A., Topcu I. (2011). Gemi işletmeciliğinde yönetimsel süreçlerin risk temelli analitik modellenmesi, İTÜ Dergisi - Seri D: Mühendislik, 10(1), Pp.43-54.

Çevik, G. (2013). "Gemi Emniyet Yönetimi Sisteminde Önleyici Faaliyet Planlama Yaklaşimi Önerisi", Master Thesis, İstanbul Technical University.

Dey, P.K. (2004). "Decision support system for inspection and maintenance : a case of oil pipelines". IEEE Trans. Eng. Manage., 51(1), pp.47-56.

Diffenbach, J. (1993). "Influence Diagrams for Complex Strategic Issues", Strategic Management Journal, 3, 133-146.

Dinç, A. (2001). "Tehlikeli Maddelerin Liman Operasyonu," Msc. thesis, Institute of Science, Istanbul Technical University., İstanbul, and pp.52-126.

Eden, C. (1988). Cognitive mapping: A review. European Jour-nal of Operational Research 36, pp.1-13.

Eden, C. and Ackerman, F. (1992). "The Analysis of Cause Maps", Journal of Management Studies, 29(3), 309–324.

Eden, C., Ackerman, F., Cropper, S. (1992). The analysis of cause maps, Journal of Management Studies 29, pp.309-24.

Ferriere, D., Pysareva, K., Rucinski, A. (2005). Using Technology to Bridge Maritime Security Gaps, National Infrastructure Institute center for Infrastructure Expertise.

Frankel, H. L. (2005). WB Crede, J E Topal, SA Roumanis, M W Devlin and A B Foley. Use of corporate six sigma performance improvement strategies to reduce incidence of catheter-related bloodstream infections in a surgical ICU. American College of Surgeons, 201(3).

Gedik M. (2007). "Türk Limanlarının Karşı Karşıya Olduğu Riskler", www.denizhaber.com, 02.05.2007

Gedik M. (2010). "Limanlarda Stratejiler ve Tarife Yaklaşımları", www.denizhaber.com, 14.01.2010

George, B., Whatford, N. (2007). 'Regulation of Transport Security Post 9/11' Security Journal, 20/3, pp.158-170.

Griffett, T. (2005). The impact of ISPS Compliance on Shipowners, Australian Shipowners Association, Melbourne

Goh, R. (2006). The Adequacy of the International Ship and Port Facility Security Code in Addressing Post-9/11 Maritime Security Threats from Ships and Ships' Crews, Journal of Singapore Armed Forces.

Gupta, K., Sleezer, C.M., Russ-Eft, D.F. (2007). A Practical Guide to Needs Asses sment.

Hart, J. A. (1977). "Cognitive Maps of Three Latin American Policy Makers", World Politics, 30(1), 115-140.

Haveman, D., Shatz, H. (2006). Protecting the Nation's Seaports: Balancing Security and Cost, pp.4.

Hekmatpanah, M. (2011). The application of cause and effect diagram in the oil industry in Iran : The case of four liter oil canning process of Sepahan Oil Company, African Journal of Business Management,vol 5(26),pp.10900-10907.

Ho,J. (2009). "Recovering after a maritime terrorist attack: The APEC Trade Recovery Programme" Marine Policy, Volume 33, Issue 4, 733-735

Hodgkinson, G. P., Maule, A. J., and Bown, N. J. (2004). “Causal Cognitive Mapping in the Organizational Strategy Field: A Comparison of Alternative Elicitation Procedures”, Organizational Research Methods, 7(1), 3-26.

ICS, 2013 Shipping and World Trade Available at (accessed on 25.10.2013): http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade/number-and-nationality-of-world's-seafarers

ISPS Code. (2004). The International Ship and Port Facility Security Code (ISPS Code).

Kahn. (2003). Port and Shore Security, Journal of Container Inspection and Security

Kang, I., Lee, K. C., Lee, S., and Choi, J. (2007). “Investigation of Online Community Voluntary Behavior Using Cognitive Map”, Computers in Human Behavior, 23, 111–126.

Keskin, H.A. (2006). Gemilerden Kaynaklanan Atıkların Kontrolü Kapsamında Liman Atık Kabul Tesisi ve Ambarlı Limanı Örneği, Msc. thesis, Instıtude of Science,Istanbul Technical University, İstanbul.

Klein, J. H., and Cooper, D. F. (1982). “Cognitive Maps of Decision-Makers in a Complex Game”, The Journal of the Operational Research Society, 33(1), 63-71.

Kwahk, K. Y., and Kim, Y. G. (1999). “Supporting Business Process Redesign Using Cognitive Maps”, Decision Support Systems, 25, 155–178.

Langen, P.W. (2002). “A Stylised Container Port Hierarchy: A Theorical and Empirical Exploration” Proceedings of IAME-2002, Panama.

Langfield-Smith, K. (1992). Exploring the need for a share cognitive map. J. Manage. Stud. 29, 349–367.

Lee, K. C., and Lee, S. (2003). “A Cognitive Map Simulation Approach to Adjusting the Design Factors of the Electronic Commerce Web Sites”, Expert Systems with Applications, 24(1), 1–11.

Mabrouki, C., Bentaleb, F., and Mousrij, A. (2014). "A decision support methodology for risk management within a port terminal", Safety Science,63, 124-132

Maenhout, G., Roo, F., and Janssens, W. (2010). "Contributing to shipping container security: can passive sensors bring a solution?" Journal of EnvironmentalRadioactivity, 101/2 ,95-105

Mokhtari, K., Ren, J., and Roberts, C. (2012). "Decision support framework for risk management on sea ports and terminals using fuzzy set theory and evidential reasoning approach " Expert Systems with Applications, 39/5, 5087-5103

Mokhtari, K., Ren, J., and Wang,J. (2011). "Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals" Journal of Hazardous Materials, Volume 192/2 2, 465-475

Marlow, P.B. (2000). "Port Pricing and Competitiveness in Short Sea Shipping" Journal of Transport Economics. s.315-334.

Mazaheri, A., Ekwall, D. (2009). Impacts of the ISPS Code on port activities : a case study on Swedish ports,World Review of Intermodal Transportation Research,Vol 2,No:4.

Mazur., Gleen, H., Hisoshi, T., Michiteru, O. (1998). Policy Management: Quality Approach to Strategic Planning. Integrated Quality Dynamics, Inc. ISBN 0-9664655-0-4

Meyer D. (2008) "The Role of the Metropolitan Planning Organization (MPO) In Preparing for Security Incidents and Transportation System Response" by Michael D. Meyer. 2008

Montazemi, A. R., and Conrath, D. W. (1986). "The Use of Cognitive Mapping for Information Requirement Analysis", MIS Quarterly, 45-56.

NATO Standardization Agency. (2007). Allied joint doctrine for force protection, AJP-3.14. NATO, Brussels.

Nicholas M. (2002) A Strategic Blueprint for World Class Seaport Security

Noh, J. B., Lee, K. C., Kim, J. K., Lee, J. K., and Kim, S. H. (2000). "A Case-Based Reasoning Approach to Cognitive Map-Driven Tacit Knowledge Management", Expert Systems with Applications, 19(4), 249–259.

Oakland, J. (2000). Total Quality Management. Butterworth Heinemann.

Özesmi, U., Özesmi, S.L. (2004). Ecological models based on people’s knowledge: a multi-step fuzzy cognitive mapping approach Ecological Modeling 176 (2004) 43–64.

Parfomak, P., Frittelli, J. (2007). Maritime Security: Potential Terrorist Attacks and Protection Priorities, CRS Report for Congress.

Papa, P. (2013) "US and EU strategies for maritime transport security: A comparative perspective" Transport Policy, 28, 75-85

Pedersen, P. T. (2010). Review and application of ship collision and grounding analysis procedures. 23: 241–262.

Peterson, P., Treat, J. (2008). The Post-9/11 Global Framework for Cargo Security, Journal of International Commence and Economics.

Ran, M. (2005). Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the maritime security threat, Geddes Papers.

Rodriguez-Repiso, L., Setchi, R., and Salmeron J. L. (2007). “Modeling IT Projects Success with Fuzzy Cognitive Maps”, Expert Systems with Applications, 32(2), 543-559.

Roach, J. (2004)." Initiatives to enhance maritime security at sea" Marine Policy, Volume 28, Issue1, 41-66

Ross, L. L., and Hall, R. I. (1980). “Influence Diagrams and Organizational Power”, Administration Science Quarterly, 25, 57-71.

Ruth, B. (2005). The impact of port and trade security initiatives on maritime supply-chain management, Maritime Policy & Management: The flagship journal of international shipping and port research. Volume, Issue 1.

Schellong, A. (2008). Citizen Relationship Management: A Study of CRM in Government.

Security Practices in U.S Seaports, (2010). Report of the Interagency Commission on Crime and Security in U.S. Seaport

SOLAS. (1974). The International Convention for the Safety of Life at Sea (SOLAS).

Solmaz , S. M. (2012). *“Deniz güvenliği kapsamında ISPS Code uygulamalarının liman güvenliği açısından etkinliğinin değerlendirilmesi ve Türkiye uygulamaları”* , Thesis of Doctorate, İstanbul University.

Surhone, L., Timpledon, M., Marseken, S. (2010). Pareto analysis: Statistics, decision making, Pareto principle, fault tree analysis, failure mode and effects analysis. Pareto distribution. Betascript Publishing, 2010.

Stevenson, D. (2005). The Impact of ISPS Code on Seafarers. International Conference Security of Ships, Ports and Coasts, Halifax, Canada, pp.22-23.

Stanford, V. (2003). Pervasive computing goes the last hundred feet with RFID systems, Pervasive Computing, IEEE, volume 2, issue 2.

Styblinski, M. A., and Meyer, B. D. (1988). "Fuzzy Cognitive Maps, Signal Flow Graphs, and Qualitative Circuit Analysis", Proceedings of the IEEE International Conference on Neural Networks (ICNN-87), 549-556.

Taber, W. R. (1991). "Knowledge Processing with Fuzzy Cognitive Maps", Expert Systems with Applications, 2, 83-87.

Tegarden, D. P., & Sheetz, S. D. (2003). Group cognitive mapping: a methodology and system for capturing and evaluating managerial and organizational cognition. Omega, 31(113-125).

Topaloğlu, H. (2007). "Dış Ticaret yüklerimizin Taşınmasındaki Terminal Durumları ve Liman Yeterliliklerinin Değerlendirilmesi," Msc thesis, İstanbul University, Deniz Bilimleri ve İşletmeciliği Enstitüsü, İstanbul. pp. 47-62.

Türklim. (2012). *Türk Limancılık Sektörü Raporu-2012*. Atölye Matbaası, İstanbul.

Unctad. (2009). Review of Maritime Transport, United Nations Conference on Trade and Development, Geneva.

Ulengin, F., Topcu, Y. I., and Sahin, S. O. (2001). "An Integrated Decision Aid System for Bosphorus Water crossing Problem", European Journal of Operational Research, 134(1), 179–192.

Yang, Z., Adolf, Y., and Wang, J. (2014). "A new risk quantification approach in port facility security assessment" Transportation Research Part A: Policy&Practice, 59, 72-90

Yarbrough, B., Yarbrough, R. (2006). The World Economy: Trade & Finance. Florence KY: Cengage Learning.

Yeo, G., Pak, J., and Yang, Z.(2013). "Analysis of dynamic effects on seaports adopting port security policy " Transportation Research Part A: Policy and Practice, 49, 285-301

Yilmazel, M., Asyali, E. (2005). An analysis of port state control inspections related to the ISPS Code, Proceedings of the IAMU, 6th AGA conference, WITPress, Southampton, 2005.

Yüksel, Y., Çevik, E., Çelikoğlu, Y. (1998). *Kıyı ve Liman Mühendisliği,* TMMOB, Ankara.

Zec, D., Frančić, V., Hlača, M. (2010). Ports Security Organization and Functionality – Implementation of the ISPS Code in Medium and Small Countries, NATO Science for Peace and Security Series - D: Information and Communication Security,vol 28, pages 41-49.

Zhang, W. R., Wang, W., and King, R. S. (1994). "A-Pool: An Agent-oriented Open System Shell for Distributed Decision Process Modeling", Journal of Organizational Computing and Electronic Commerce, 4(2), 127–154.

Zhang, W. R., Chen, S. S., and Bezdek, J. C. (1989). "Pool2: A generic System for Cognitive Map Development and Decision Analysis", IEEE Transactions on Systems, Man and Cybernetics, 19(1), 31–39.

Watson, G. (2004) The Legacy of Ishikawa. Qual. Prog., 37(4), pp.54-57.

Wenning, R.J., et. al. (2007). Understanding environmental security at ports and harbors. In: Linkov I, Kiker GA, and Wenning RJ (eds) Managing Critical Infrastructure Risks: NATO Security through Science Series. Dordrecht: Springer, pp.3-15.

Wood, D.F., Barone, A., Murphy, P., Wardlow, P.L. (2002) International Logistics, Amacom Books, New York.

Url-1: Catch Me If You Can Man Poses As Pilot: Breaches Airport Security: <http://www.cgiprotects.com/security-tips-blog/tag/Port_Security/> data retrieved 25.02.2013

Url-2: <http://www.imo.org/OurWork/Security/Instruments/Pages/ISPSCode.aspx> Data retrieved 15.03.2013

Url-3: Total quality management. <http://www.wiley.com/college/sc/reid/chap5.pdf > data retrieved 26.06.2013

Url-4: Pareto Analysis, <https://depts.washington.edu/oei/resources/toolsTemplates/ pareto_ principle.pdf data retrieved: 15.02.2013

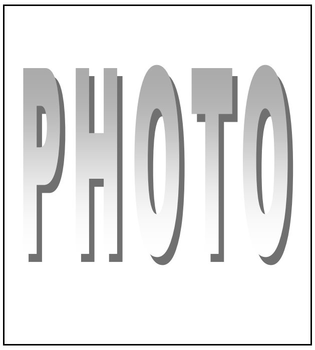
Url-5: Maritime security: Implementation of the ISPS Code <http://www. porttechnolog .org /images / uploads/technical_ papers /PT28-05.pdf> data retrieved: 10.03.2013

Url-6: Small Vessel Security Strategy, Department of Homeland Security. <http://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy. pdf> Data retrieved 25.11.2013

Url-7: Final Guides for Port & Harbour Risk Assessment and Safety Management Systems in NewZeland.<http://www.maritimenz.govt.nz/Publications-and-forms/Commercial-operations/Ports-and-harbours/Port-harbour-risk-assessment.pdf> data retrieved : 05.04.2013

Url-8: Delegation of the European Commission to the USA. Securing Trade: The EU's Approach to Port and Maritime Container Security. EU Insight, Issue 21, July 2008. Pub: Delegation of the European Commission to the United States. http://www.eurunion.org/News/eunewsletters /EUInsight/2008/EUInsightContainerJuly2008.pdf data retrieved 11.04.2013

Url-9: Supply Chain Security Solutions. <http://www.supplychainsecurity.com /gov _ctpat.html> data retrieved 25.11.2013



CURRICULUM VITAE

Name Surname: Burcu ÖZTÜRK

Place and Date of Birth: ISTANBUL/ 11.10.1985

Address: USKUDAR/ISTANBUL

E-Mail: burcuozt1985@gmail.com

B.Sc.: Maritime Transportation and Management Engineering / Istanbul Technical University (2010)

Professional Experience and Rewards:

ARKAS Shipping- Oceangoing watch keeping officer (Agu 2010- Nov 2010)

Wanhai Lines Turkey – Sales and marketing assistant (May 2011- Jan 2012)

ITU Ecotoxıcology Research and Education Laboratory- Tubitak project assistant (Jan 2012- Oct 2012)

Piri Reis University – Research Assistant (Oct 2012-)

List of Publications and Patents:

PUBLICATIONS/PRESENTATIONS ON THE THESIS

1. “Stratejik Güvenlik Yaklaşımları Kapsamında Liman Güvenlik Yönetimi” , 5th International Symposium on Terrorism and Transnational Crime, Antalya ,December 2013
2. “Limanların Konumlandırılması Süresince Risk Yönetimi”, 1. Ulusal Liman Kongresi,Dokuz Eylül Üniversitesi,İzmir,Kasım 2013