

AYBARS ORUÇ

CYBERSECURITY RISK ASSESSMENT FOR
TANKERS AND DEFENCE METHODS

M.Sc. THESIS

AYBARS ORUÇ

2020

PİRİ REİS UNIVERSITY

JANUARY 2020

CYBERSECURITY RISK ASSESSMENT FOR TANKERS
AND
DEFENCE METHODS

by

Aybars ORUÇ

B. S., Marine Engineering, Near East University, 2015

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Maritime Transportation Management Engineering

Piri Reis University

2020

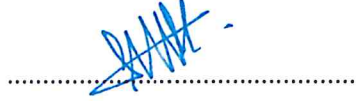
Aybars ORUÇ, M.Sc. student of Piri Reis University Maritime Transportation Management Engineering student ID: 168013004, successfully defended the thesis entitled “CYBERSECURITY RISK ASSESSMENT FOR TANKERS AND DEFENCE METHODS” which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

APPROVED BY

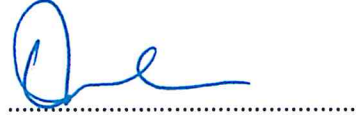
Prof. Dr. Funda YERCAN



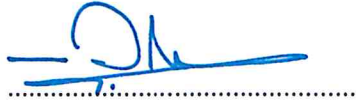
Assist. Prof. Dr. Elif BAL BEŞİKÇİ



Assist. Prof. Dr. Emre ÇAKMAK
(Thesis Supervisor)



Assist. Prof. Dr. Murat Selçuk SOLMAZ
(Thesis Co-Supervisor)



Assist. Prof. Dr. Tuba KEÇECİ



Date of Approval: 13th January 2020

ACKNOWLEDGMENTS

Foremost, I would like to express my gratitude towards my dear mother and father who supported me by providing me with all the opportunities for a qualified education. Certainly, they are my greatest chance in life. Even though I neglect to say that I love them very much, I hope they know this very well.

I am highly indebted to my advisers Assist. Prof. Dr. Emre Cakmak and Assist. Prof. Dr. Murat Selcuk Solmaz in the Graduate School of Science and Engineering who I am proud to be the player of the same team during the preparation of this thesis. I could never have reached this current level of success in this thesis without if they had not shared their experience with me.

My thanks and appreciation also go to my colleagues at Armona Shipping who have willingly helped me. They do not only support me during my master's degree, but also contribute to the emergence of this academic study with response to the questions I asked.

Last of all, I must say that I gained a significant part of my knowledge that I have today thanks to my valuable teachers who have influenced a period of my life. I realize that what I have today is their legacy. I thank each one of them with all my heart.

ABSTRACT

CYBERSECURITY RISK ASSESSMENT FOR TANKERS AND DEFENCE METHODS

Ships take significant place in the maritime transport, and technological developments are rapidly reflected on ships. A wide range of equipments, such as GPS ECDIS, AIS and ARPA-Radar is utilized in this field in order to ensure safe navigation on a ship. However, several studies have also been published that show cyber vulnerabilities in navigational equipments. Moreover, cyber attacks in the maritime industry also have led to gain importance of cybersecurity at sea. When compared to other vessel types, such as dry cargo vessels and RO-ROs, tankers are more likely to pollute the environment, to cause more people to be injured or died and more economic loss after an arising accident due to the cargo they carry. Due to this known fact, inspections on cybersecurity have been started firstly on tankers through vetting programmes of TMSA, SIRE and CDI. IMO requires all maritime companies to carry out a cyber risk assessment by 2021. In this study, the potential cyber risks of equipments in the bridge, engine room and cargo control room on a tanker underway were assessed. As a result of the assessment, a total of 31 risks are identified in nine categories, and 37 procedural and technical measures that could be taken against these risks are examined. The risks either before taking measure or after taking measures are evaluated by using the Fuzzy Fine-Kinney method. Thus, effectiveness of the suggested measures is approached.

Keywords: Cybersecurity, Maritime cybersecurity, Tankers, Defence methods

ÖZET

TANKERLERDE SİBER GÜVENLİK RİSK DEĞERKLENDİRMESİ VE SAVUNMA METODLARI

Deniz taşımacılığının olmazsa olmazı gemilerdir ve teknolojik gelişmeler gemilere hızla yansır. Bir gemi üzerinde emniyetli seyri sağlamak amacıyla GPS, ECDIS, AIS, ARPA-Radar gibi pek çok ekipman bulunur. Ancak üzücüdür ki seyir ekipmanlarındaki siber zaafiyetleri gösteren çeşitli araştırmalar da yayınlanmıştır. Ayrıca denizcilik sektöründe yaşanan siber saldırılar da denizde siber güvenlik konusunun ön plana çıkmasına sebep olmuştur. Kuruyük, RO-RO gibi diğer gemi tipleri ile karşılaştırıldıklarında tankerlerin, taşıdıkları yükler sebebi ile meydana gelecek bir kaza sonrasında çevreyi daha fazla kirletmesi, daha fazla sayıda insanın yaralanmasına ya da ölmesine sebebiyet vermesi ve daha çok ekonomik kayba uğratması olasıdır. Bu bilinen gerçek sebebi ile siber güvenlik ile ilgili denetlemeler öncelikle tankerlerde TMSA, SIRE ve CDI gibi denet programları aracılığıyla başlatılmıştır. IMO ise 2021 senesi itibari ile tüm denizcilik şirketlerinden bir siber risk değerlendirmesi yapılmasını beklemektedir. Bu çalışmada seyir halinde bulunan bir tankerin köprüüstü, makine dairesi ve kargo kontrol dairesine ait ekipmanların sahip olabileceği olası siber riskler değerlendirilmiştir. Değerlendirme sonucunda dokuz kategoride, toplam 31 adet risk belirlenmiş olup belirlenen bu risklerine karşı alınabilecek toplam 37 adet prosedürel ve teknik önlem incelenmiştir. Riskler Bulanık Fine-Kinney metodu kullanılarak gerek önlemler alınmadan önce gerek ise önlemler alındıktan sonra değerlendirilmiştir. Böylelikle önerilen tedbirlerin etkinliği gözlemlenmiştir.

Anahtar kelimeler: Siber güvenlik, Denizde siber güvenlik, Tankerler, Savunma metodları

TABLE OF CONTENTS

ACKNOWLEDGMENTS	ii
ÖZET	iv
LIST OF FIGURES	viii
LIST OF TABLES.....	ix
LIST OF SYMBOLS	x
LIST OF ABBREVIATIONS.....	xi
1. INTRODUCTION	1
2. MARITIME TRADE AND TANKER INDUSTRY	5
2.1. The Situation of Tanker Fleet in the World	6
2.2. Types of Tankers.....	9
2.2.1. Oil Tanker	9
2.2.2. Chemical Tanker.....	10
2.2.3. Gas Carrier	10
3. MARITIME CYBERSECURITY	12
3.1. Maritime Safety, Maritime Security and Maritime Cybersecurity	12
3.2. Cybersecurity in General Terms	14
3.2.1. The Definition of Risk.....	14
3.2.2. Definition of Cyber Attack.....	15
3.2.3. Common Cyber Attack Methods.....	15
3.2.4. Stages of a Cyber Attack	19
3.2.5. Typical Characteristics of Cyber Threats	20
3.3. Cyber Attacks in the Maritime Industry.....	21
3.3.1. Ports of Belgium and Netherlands (2011).....	21
3.3.2. IRISL (Islamic Republic of Iran Shipping Lines) (2011)	22
3.3.3. Australian Customs and Border Protection Service Agency (2012).....	22
3.3.4. Danish Maritime Authority (2012)	23
3.3.5. Oil Rig Platform (2013)	24
3.3.6. South Korea (2016)	24
3.3.7. Hacking Broker's e-Mail Account (2016)	25
3.3.8. Maersk (2017)	25
3.3.9. Russia (2017)	26
3.3.10. Clarksons (2017)	27

3.3.11. German-Owned Container Ship (2017)	27
3.3.12. BW Group (2017)	28
3.3.13. Svitzer Australia (2018)	28
3.3.14. COSCO Shipping (2018)	28
3.3.15. Austal (2018).....	29
3.3.16. Analysis of the Maritime Cyber Incidents	29
3.4. Legislations and Vetting Programmes	31
3.4.1. Mandatory Regulations	31
3.4.2. Non-Mandatory Vetting Programmes.....	32
3.4.3. Analysis of Legislations and Vetting Programmes	42
3.5. Vulnerable Systems to Cyber Attacks onboard Ships.....	42
3.5.1. Bridge Systems.....	43
3.5.2. Access Control Systems	45
3.5.3. Cargo Handling and Management Systems	46
3.5.4. Propulsion and Machinery Management and Power Control Systems	46
3.5.5. Communication Systems.....	47
3.5.6. Passenger Servicing and Management Systems	47
3.5.7. Passenger Facing Public Networks	48
3.5.8. Administrative and Crew Welfare Systems	48
3.6. The Cyber Attacks Methods towards GPS, AIS, ECDIS and ARPA-RADAR....	49
3.6.1. Attack Methods to Global Positioning System (GPS)	49
3.6.2. Attack Methods to AIS.....	52
3.6.3. Attack Methods to ECDIS	55
3.6.4. Attack Methods to ARPA – RADAR	56
3.7. Protection Cybersecurity Measures towards Tankers	56
3.7.1. Technical Protection Cybersecurity Measures towards Tankers.....	56
3.7.2. Procedural Protection Cybersecurity Measures towards Tankers	61
3.8. Literature Review	71
4. MATERIALS AND METHODS	75
4.1. The Method of Fuzzy Logic.....	75
4.1.1. Advantages of Fuzzy Logic	76
4.1.2. Disadvantages of Fuzzy Logic	76
4.1.3. Fuzzy Set Theory	76
4.1.4. Membership Function	77

4.1.5. Membership Value Assignment.....	78
4.1.6. Sections of Membership Function.....	78
4.1.7. Types of Membership Function.....	80
4.1.8. Fuzzy Set Operations.....	82
4.1.9. Linguistic Variables.....	83
4.1.10. Fuzzification.....	83
4.1.11. Defuzzification.....	83
4.2. Fine-Kinney Risk Assessment Method.....	86
4.3. Implementation of Fuzzy Fine-Kinney Method.....	88
4.3.1. Application of the Model in Matlab.....	94
4.3.2. Defining of Membership Functions.....	96
4.3.3. Preparation of Fuzzy Rules.....	99
5. FINDINGS.....	101
6. CONCLUSION.....	112
REFERENCES.....	114
APPENDIXES.....	121
A. Questionnaire and Options for Fine-Kinney Method.....	121
B. Resolution MSC.428(98).....	124
C. MSC-FAL.1/Circ.3.....	125
CURRICULUM VITAE.....	130

LIST OF FIGURES

Figure 2.1. Total number of tankers	6
Figure 2.2. Rate of tankers in whole feet	7
Figure 2.3. Dead-weight tons change in tanker fleet	8
Figure 3.1. An example code number of a KPI in TMSA	37
Figure 3.2. Required equipments for GPS spoofing attack	50
Figure 3.3. Illustration of a spoofing attack via portable receiver-spoofers	51
Figure 3.4. Sketch of the spoofer setup on the White Rose of Drachs	52
Figure 4.1. Core, support and boundaries of a fuzzy set	80
Figure 4.2. Command window of Matlab	94
Figure 4.3. Matlab fuzzy inference system	95
Figure 4.4. FIS variables	95
Figure 4.5. Defining of membership function	96
Figure 4.6. Fuzzy diagram for likelihood input	98
Figure 4.7. Fuzzy diagram for frequency input	98
Figure 4.8. Fuzzy diagram for consequence input	99
Figure 4.9. Fuzzy diagram for risk score output	99
Figure 4.10. Rule editor of fuzzy logic designer	100

LIST OF TABLES

Table 2.1. Ownership of world fleet ranked by dead-weight tonnage.....	5
Table 2.2. Ratio of crude oil, petroleum products and gas in total cargo	8
Table 2.3. Oil tankers as per deadweight.....	9
Table 3.1. Words of “safety” and “security” in different languages	12
Table 3.2. Typical characteristics of cyber threats	20
Table 3.3. Cyber attacks in the maritime industry	30
Table 3.4. Chapters in VIQ 7.....	33
Table 3.5. Elements in TMSA 3	36
Table 3.6. Chapters in CDI Ship Inspection Report	39
Table 3.7. Sections in Rightship questionnaire.....	41
Table 3.8. The data can be recorded by VDR.....	43
Table 3.9. Featured researches towards the purposes of the thesis.....	73
Table 4.1. Types of membership functions.....	81
Table 4.2. Types of defuzzification methods.....	84
Table 4.3. Risk scores and action plan as per Fine-Kinney	86
Table 4.4. The table of likelihood.....	87
Table 4.5. The table of frequency	87
Table 4.6. The table of consequence.....	87
Table 4.7. The table of cyber risk areas on a tanker	89
Table 4.8. Cyber risks with attack methods on a tanker	90
Table 4.9. The technical protection cybersecurity measures towards defined risks.....	92
Table 4.10. The procedural protection cybersecurity measures towards defined risks	92
Table 4.11. The protection measures against defined cyber risks	93
Table 4.12. The name and params for likelihood (L)	97
Table 4.13. The name and params for frequency (F).....	97
Table 4.14. The name and params for consequence (C).....	97
Table 4.15. The name and params for risk score (R).....	97
Table 5.1. Risk evaluation before taking protection as per Fine-Kinney method	103
Table 5.2. Risk scores after taking protection as per Fine-Kinney method.....	104
Table 5.3. Risk evaluation before taking protection as per Fuzzy Fine-Kinney method	105
Table 5.4. Risk scores after taking protection as per Fuzzy Fine-Kinney method.....	106
Table 5.5. The comparison table for Fine-Kinney and Fuzzy Fine-Kinney risk scores ..	107
Table 5.6. Risks in same level in despite of protection measures	108
Table 5.7. Mitigated risk level difference after protection measures	108
Table 5.8. Sort of risks as per Fuzzy Fine-Kinney method after protection measures	110

LIST OF SYMBOLS

Symbol	Description
m^3	cubic meter
$^{\circ}C$	degree celcius
σ	function width
μ	fuzzy set
\int	integral
\cap	intersection of two sets
\in	is an element of
Σ	summation
\cup	union of two sets

LIST OF ABBREVIATIONS

Abbreviation	Description
ABS	American Bureau of Shipping
AIS	automatic identification system
ARPA	automatic radar plotting aid
AtoN	aids-to-navigation
BNWAS	bridge navigation watch alarm system
BP	British Petroleum
C	consequence
C-DAC	Center for Development of Advanced Computing
C4ADS	Center for Advanced Defense Studies
CCNR	Central Commission for Navigation on the Rhine
CCR	cargo control room
CCTV	closed circuit television
CD	compact disc
CDI	Chemical Distribution Institute
CESG	Communications-Electronics Security Group
CISO	chief information security officer
CoA	contract of affreightment
COSCO	China Ocean Shipping Company
CPA	closest point of approach
CSP	cybersecurity plan
CV	curriculum vitae
CySO	cybersecurity officer
DNV-GL	Det Norske Veritas - Germanischer Lloyd
DoC	document of compliance
DPA	designated person ashore
DoS	denial of service
DVD	digital versatile disc
EC3	European Cybercrime Centre
ECDIS	electronic chart display and information system

ECR	engine control room
ETA	estimated time arrival
EU	European Union
F	frequency
FAL	facilitation committee
FIS	fuzzy inference system
GCSOS	guidelines on cybersecurity onboard ships
GHz	gigahertz
GLONASS	global orbiting navigation satellite system
GNSS	global navigation satellite systems
GPS	global positioning system
GT	gross tonnage
HFO	heavy fuel oil
HSEQ	health, safety, environment, quality
IBC Code	International Bulk Chemical Code
IMarEST	Institute of Marine Engineering, Science & Technology
IMO	International Maritime Organization
INTERTANKO	International Association of Independent Tanker Owners
IRISL	Islamic Republic of Iran Shipping Lines
IRM	Institute of Risk Management
IRP	incident response plan
ISM Code	International Safety Management Code
ISO	International Standard Organization
ISPS Code	International Ship and Port Facility Security Code
IT	information technology
KPI	key performance indicator
L	likelihood
LAN	local area network
LOA	length overall
LNG	liquefied natural gas
LPG	liquefied petroleum gas
MARPOL Convention	Convention for the Prevention of Pollution from Ships
MGO	marine gas oil

MITM	man in the middle
MMSI	maritime mobile service identity
MOC	major oil company
MoC	management of change
MSC	maritime safety committee
NLS	noxious liquid substances
NM	nautical mile
OCIMF	Oil Companies International Marine Forum
OOW	officer of the watch
OPEX	operational expenses
OT	operational technology
P&I	protection & indemnity
P/V Valve	pressure/vacuum valve
PMS	planned maintenance system
PC	personal computer
PSC	port state control
R	risk score
RF	radio-frequency
RJ-45	registered jack-45
RX	receive
SAR	search and rescue
SART	search and rescue transponders
SENC	system electronic navigation chart
SIRE	Ship Inspection Report Programme
SMS	safety management system
SOLAS Convention	International Convention for the Safety of Life at Sea
SSA	ship security assessment
SSAS	ship security alarm system
SSL	secure sockets layer
STCW	Standards of Training, Certification and Watchkeeping
T/C	time charter
TEU	twenty-foot equivalent unit
TMSA	Tanker Management Self Assessment

TX	transmit
UK	United Kingdom
ULCC	ultra-large crude carrier
UNCTAD	United Nations Conference on Trade and Development
URL	uniform resource locator
US	United States
USB	universal serial bus
UTI	ullage temperature interface
V/C	voyage charter
V-SAT	very small aperture terminal
VDR	voyage data recorder
VIQ	Vessel Inspection Questionnaire
VLCC	very large crude carrier (VLCC)
VPN	virtual private network
WMN	World Maritime News
WPA 2	wi-fi protected access 2

1. INTRODUCTION

World maritime trade grew by 2.7% in 2018, and in 2019, is expected to grow by 2.6% (UNCTAD, 2019). Over the next five years including the years 2019-2024, the annual growth rate is expected to be 3.4% (UNCTAD, 2019). Approximately 90% of the world trade is executed by maritime transportation (Allianz, 2019). Due to the fact that the cargo can be transported at low cost and safety, maritime transportation has become prominent. Besides, transportation to the islands requires maritime transportation. Because establishing substructure for transportation of the airway, the highway or the railroad may bring bureaucratic problems as well as being overcosting economically.

The maritime industry always wants to make the most of technological opportunities. Through technological opportunities, the number of crew is reduced. Reducing the number of crew also reduces crew costs, and it means the reduction of operating costs. Under the skin of autonomous ship and remote control ship project, there is an effort to decrease the operation cost. One of the most important matters discussed for these projects is, without doubt, cyber threats. The cyber attacks are heard more and more in the maritime industry, and cause risk for the future of autonomous projects.

Even though the ships are not totally autonomous at the present time, by means of developing automatization technology, the number of crew is decreasing rapidly. However, this automatization technology brings cyber attack risks along. Because of this reason, IMO (International Maritime Organization) took an action, and imposed the obligation of companies to make a cyber risk assessment by 2021 (IMO, 2017c). The vetting organizations that inspect the tankers had reacted earlier, and obligated tanker operators take precautions by adding questions about cybersecurity to vetting programmes they developed. Regarding these advanced vetting programmes, it can be stated that in particular tanker operators are more aware and ready for cyber threats.

Due to developing technology, tankers also have cybersecurity risks. Because of flammable or explosive cargo they carry. The level of these risks must be defined and then risks must be reduced to acceptable level or eliminated. This study may be response to evaluation of cybersecurity risks in tankers and measures to reduce these or eliminate risks.

This study has two main purposes. One of these purposes is to determine and assess cyber risk for tankers underway, and the other purpose is to identify the procedural and technical precautions against cybersecurity risks of these tankers.

This study considers cybersecurity threat arising in tankers underway due to developments in technology. Cargo handling systems are different based on ship types. Each cargo handling system has unique cyber risks. Additionally, the effect of these cyber attacks on the environment, human life and cargo vary based on ship type. Therefore, the scope of this study is limited to tankers rather than all ship types. During risk assessment, possible cyber attacks against bridge equipment, machinery systems and cargo management systems are analysed.

The literature review showed that there is a limited number of studies on maritime cybersecurity. The studies are generally attempted to determining the vulnerability of navigation equipment and do not include any risk assessment. Furthermore, qualitative research methods are generally used in the studies, and there are almost no quantitative studies. Furthermore, it has been seen that qualitative research methods are generally used in the studies, and there is almost no quantitative study. The studies are generally carried out by individuals who has computer science background and rarely by professionals with sea experience. This has led a gap in the research of the impact of cyber risks on operations on the ship. Furthermore, based on international rules, by 01st January 2021, maritime companies should have a cyber risk assessment for the ships they manage (IMO, 2017c). Nevertheless, no attempt has been found to meet this need. This study aims to address an important gap in the literature.

Although risk assessment methods are divided into two main groups, qualitative and quantitative, they are similar in terms of implementation steps. In both, principally risks must be identified and assessed. There is not enough data on cyber incidents in the maritime sector. Therefore, expert opinion should be utilized. Since expert opinions may differ from each other, fuzzy logic approach makes risk assessment more accurate. The Fine-Kinney method is a quantitative risk assessment, and is simple to use. The quantitative method also makes it easier to analyze the results. It can also be combined with fuzzy logic. For this reason, Fuzzy Fine-Kinney risk method was preferred in this study.

During the literature review, papers, dissertations, guidelines, books and news in English and Turkish language related to this topic are reviewed. Then, these resources are analysed in detail, and resources in line with this study's purposes are examined. Possible cyber threats are determined and depending on the place of attack of the tankers, these threats are classified. A questionnaire compatible with Fine-Kinney risk assessment method including these risks is prepared, and focus group's opinions are taken by this questionnaire. Risk assessments as a result of group member discussions are analysed with Fuzzy Fine-Kinney risk assessment method.

Therefore this study has six main sections. These are:

- Introduction
- Maritime Trade and Tanker Industry
- Maritime Cybersecurity
- Materials and Methods
- Findings
- Conclusion

The first section of the study is introduction section which provides general information about the topic, scope, importance and research method of the study. In maritime trade and tanker industry section, information about today's maritime activities, tanker industry and tanker types are presented. In the section of maritime cybersecurity, cybersecurity topic is explained. Cyber attack types, stages and methods are presented. The topic of cybersecurity at sea is included in this section. International rules, incidents, vulnerable systems, technical and procedural protection measures are investigated in this section in detail. The materials and methods section describes Fuzzy Logic and Fine-Kinney risk assessment method. In this section, a risk assessment is made by using Fuzzy Fine-Kinney risks assessment method. In the findings section, the results of risk assessment with Fuzzy Fine-Kinney method are presented. A risk score comparison was made before and after the measures in order to understand the effectiveness of the measures taken. In conclusion section, the obtained results are presented with a general perspective in line with the purpose of this study is presented to the researcher as a summary. Besides that, a variety of recommendations have been made for further research.

2. MARITIME TRADE AND TANKER INDUSTRY

More than 90% of the world trade is carried out by maritime transportation (Allianz, 2019). Due to this fact, maritime transport has a great importance for the world trade. Setbacks in maritime transport or changes in transport fees directly affect the trade. World maritime trade grew by 2.7% in 2018, and is expected to grow by 2.6% in 2019. The annual average growth predicted between 2019 and 2024 is 3.4%. The leaders of world maritime transportation as per ownership of world fleet ranked by dead-weight tonnage are Greece, Japan, China, Singapore and Hong Kong accounting for nearly 51% of the world's dead-weight tonnage. Total dead-weight carriage capacity of the first ten countries is nearly 69% of world's tonnage. In the Table 2.1, the ownership of world fleet ranked by dead-weight tonnage and their rates in the world are shown as per UNCTAD (United Nations Conference on Trade and Development). (UNCTAD, 2019)

Table 2.1. Ownership of world fleet ranked by dead-weight tonnage (UNCTAD, 2019)

No	Country	Dead-weight tonnage	Rate
01	Greece	349,195,189	17.79%
02	Japan	225,121,215	11.47%
03	China	206,301,032	10.51%
04	Singapore	121,485,648	6.19%
05	Hong Kong	98,128,318	5.00%
06	Germany	96,532,360	4.92%
07	Republic of Korea	76,701,517	3.91%
08	Norway	61,115,099	3.11%
09	United States	58,377,706	2.97%
10	Bermuda	58,232,207	2.97%
Subtotal of top 10 shipowners		1,351,190,291	68.85%
Rest of world		611,391,749	31.15%
World total		1,962,582,040	100%

2.1. The Situation of Tanker Fleet in the World

Equasis is web service which provides transparency for the professionals in the maritime industry. Its aim is to increase quality and safety performance in the maritime industry. Everybody can register free of charge, and then can access the data of any ships, such as detention status, deficiencies in PSC (Port State Control) inspections, main data like IMO number, call sign and registered owner etc. Equasis has various data providers, such as classification societies, PSC regimes, IHS Markit, P&I (Protection & Indemnity) clubs and insurance companies, intergovernmental organisations, private companies and associations from the maritime industry. Today, Equasis takes data from 58 different data providers (Equasis, 2019a). Equasis was launched by European Commission and the UK (United Kingdom) Government in November 1997 (Equasis, 2019b). The IMO currently has observer status in Equasis. Based on Equasis statistics published in 2019, total number of vessels around the world was 116857 as of 2018. 16858 of these vessels were tankers. When 2014 – 2018 years are analysed, it can be seen that the number of vessels in world maritime merchant fleet in Figure 2.1 (Equasis, 2015, 2016, 2017, 2018, 2019c).

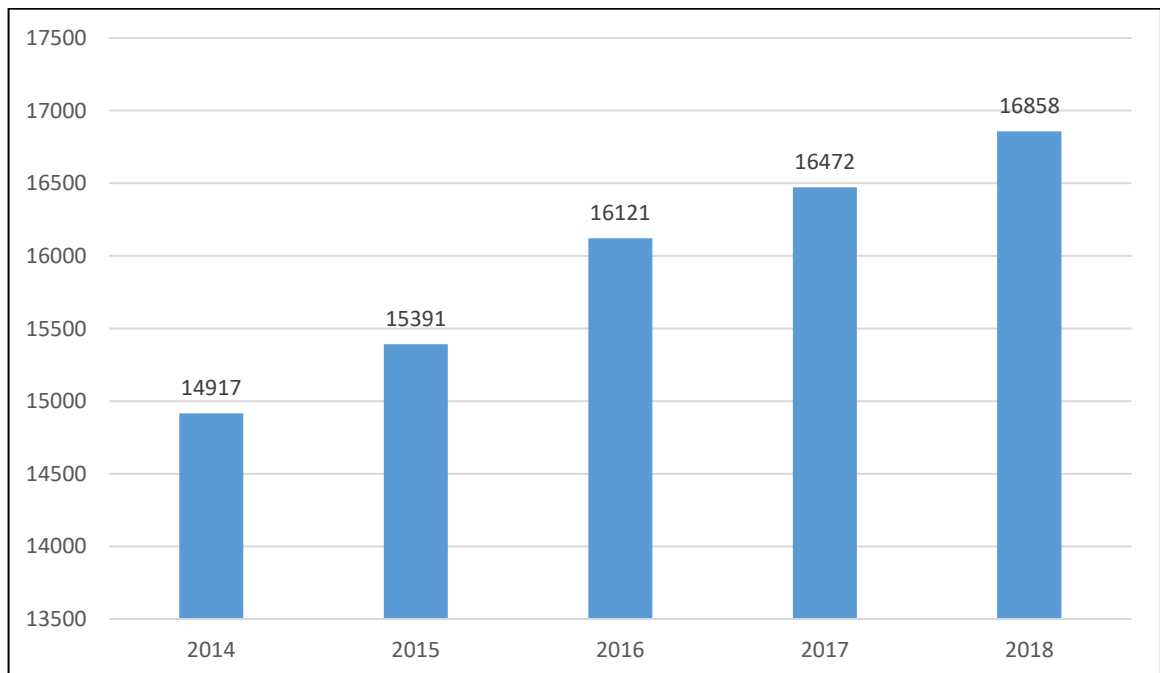


Figure 2.1. Total number of tankers (Equasis, 2015, 2016, 2017, 2018, 2019c)

It is seen that we see that the rate of tankers in whole fleet in 2018 reduced from 18.2% to 14.4% (Equasis, 2019c). The reason of this decline is that Equasis includes fishing vessels in its new statistics unlike previous years. This situation has caused the number of ships in the world to increase by more than 25000 within a year. In order to make an accurate comparison of the tanker rate with previous years, it is necessary to redetermine the total number of vessels by subtracting the fishing vessels from the total number of ships in 2018. When the fishing vessels are subtracted, the total number of vessels in the world is 92251. According to the data of 2018, the number of oil/chemical tankers, gas carriers and other tankers is 16858. When estimated, the rate of tankers in whole fleet in 2018 will be calculated as 18.3%. In Figure 2.2, rate of tankers in the last five years is shown, and it shows that there is an increase by per year (Equasis, 2015, 2016, 2017, 2018, 2019c).

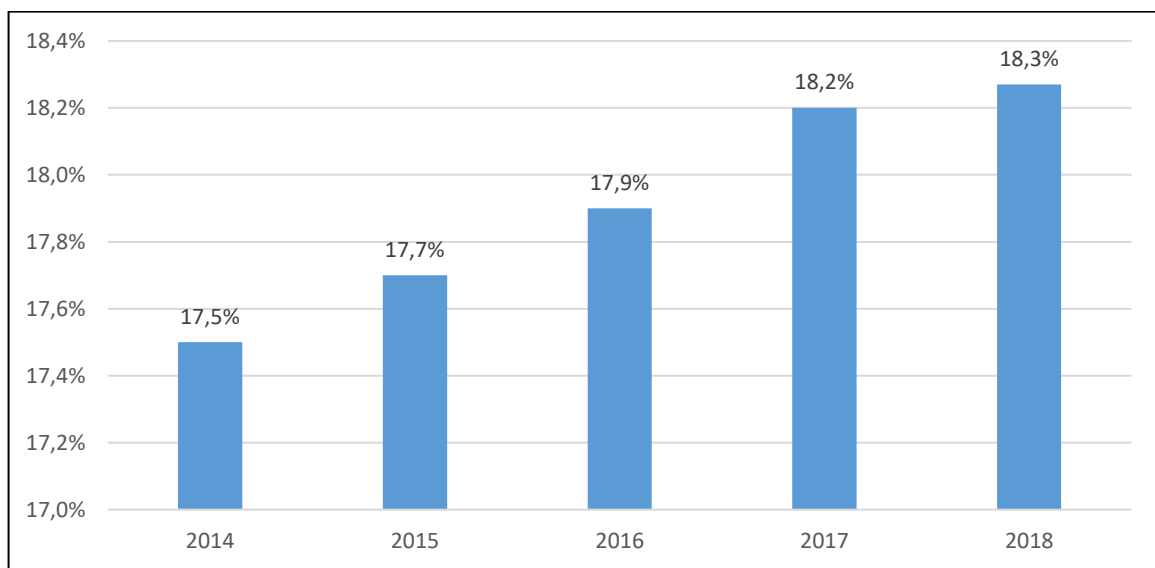


Figure 2.2. Rate of tankers in whole feet (Equasis, 2015, 2016, 2017, 2018, 2019c)

When Equasis reports are analysed, it can be seen that number of tankers increased. However, this numerical increase raises the question to analyse this growth in dead-weight tonnes. This is because although number of vessels can increase, vessels' capacities in terms of dead-weight tonnes may be decreased. To better understand the position of tanker fleet in world maritime trade, it is important to consider dead-weight tonnes. Because dead-weight tonne is a vital indicator of seaborne trade and cargo carrying capacity.

UNCTAD annually publishes a comprehensive report called “Review of Maritime Transport”. When past data of these reports are analysed, it can be seen that over the last five years, dead-weight tonnes of global tanker fleet has grown. Especially when gas carriers are compared to oil tankers and chemical tankers, it can be seen that gas carriers had shown higher growth. In Figure 2.3, the growth rates of oil tankers, chemical tankers and gas carriers are seen (UNCTAD, 2015, 2016, 2017, 2018, 2019).

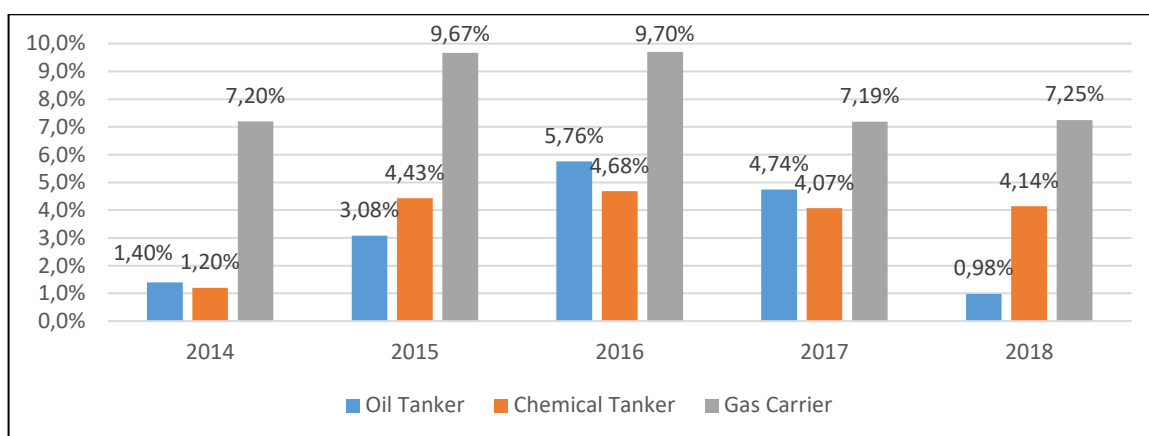


Figure 2.3. Dead-weight tons change in tanker fleet
(UNCTAD, 2015, 2016, 2017, 2018, 2019)

Table 2.2 below shows development in international seaborne trade between 2014-2018 and crude oil, petroleum products and gas ratios are presented (Millions of tons loaded) (UNCTAD, 2015, 2016, 2017, 2018, 2019). Based on data provided in the Table 2.2 below, cargo transported by sea has increased annually for the last five years. Crude oil, petroleum products and gas amount that can be carried with tankers is almost the same among total transported cargo.

Table 2.2. Ratio of crude oil, petroleum products and gas in total cargo
(UNCTAD, 2015, 2016, 2017, 2018, 2019)

Year	Total Cargo	Crude Oil, Petroleum Products and Gas	Ratio
2014	9842	2825	28.70%
2015	10023	2932	29.25%
2016	10295	3058	29.70%
2017	10716	3146	29.36%
2018	11005	3194	29.02%

2.2. Types of Tankers

The tankers are divided into three main categories called “Oil Tanker”, “Chemical Tanker” and “Gas Carrier” as per SOLAS (International Convention for the Safety of Life at Sea) Convention (IMO, 2014b).

2.2.1. Oil Tanker

As per the International Convention for the Prevention of Pollution from Ships (MARPOL Convention), oil tanker means a ship constructed or adapted primarily to carry oil in bulk in its cargo spaces and includes combination carriers, any “NLS (Noxious Liquid Substances) tanker” as defined in Annex II of the present Convention and any gas carrier as defined in regulation 3.20 of chapter II-1 of SOLAS 74 (as amended), when carrying a cargo or part cargo of oil in bulk. (IMO, 2017b)

Deadweight is the weight of cargo plus weights of fuel, stores, water ballast, fresh water, crew, passengers and baggage. As per the Table 2.3, oil tankers are divided into six groups as deadweight. (Bruce & Eyres, 2012)

Table 2.3. Oil tankers as per deadweight (Bruce & Eyres, 2012)

Name	Size interval (deadweight)
ULCC (Ultra-Large Crude Carrier)	300,000 – 550,000
VLCC (Very Large Crude Carrier)	200,000 – 300,000
Suezmax crude tanker	App. 150,000 (can transit the Suez Canal)
Aframax crude tanker	80,000 – 115,000
Panamax crude tanker	55,000 – 70,000 (can transit the Panama Canal)
Handysize / Handymax	35,000 – 45,000

2.2.2. Chemical Tanker

Chemical tanker means a cargo ship constructed or adapted and used for the carriage in bulk of any liquid product listed in chapter 17 of the IBC Code (International Bulk Chemical Code) (IMO, 2014b). Chemical tankers are divided into three types under IBC Code. These tankers are designed and constructed as per the requirements of selected type. The cargo that can be carried by each type chemical tanker are determined within IBC Code. While Type 1 chemical tankers can carry the most dangerous cargo, Type 2 and Type 3 chemical tankers can carry less dangerous products. (Bruce & Eyres, 2012)

2.2.3. Gas Carrier

Gas carrier means a cargo ship constructed or adapted and used for the carriage in bulk of any liquefied gas or other product listed in chapter 19 of the International Gas Carrier Code. (IMO, 2014b)

As per OCIMF (Oil Companies International Marine Forum) and CCNR (Central Commission for Navigation on the Rhine), gas carriers are divided into two categories as LPG (Liquefied Petroleum Gas) ships and LNG (Liquefied Natural Gas) ships. LPG ships are used in the transportation of propane, butane and chemical gases. These products can be carried by three types of LPG ships called “Fully Pressurised Tankers”, “Semi-Pressurised Tankers” and “Fully Refrigerated Tankers”. (OCIMF & CCNR, 2010)

- Fully Pressurised Tankers: These are low cost vessels and generally constructed up to 2000m³ capacity. These vessels are often used between small gas terminals. (Bruce & Eyres, 2012)

- Semi-Pressurised Tankers: These are generally built up to 5000m³ capacity. These tankers has reliquefaction plant (OCIMF & CCNR, 2010). Temperature of carried cargo is approximately -5°C. (Bruce & Eyres, 2012)

- Fully Refrigerated Tankers: These tankers generally have 10,000 – 100,000m³ capacity. Cargo is carried in fully refrigerated storage tanks. Temperature of carried cargo is approximately -48°C. (Bruce & Eyres, 2012)

LNG ships carry LNG which is carried at its boiling point, being -162°C. LNG containment systems have developed considerably. LNG ships are fitted with independent cargo tanks or with membrane tanks. (Bruce & Eyres, 2012)

3. MARITIME CYBERSECURITY

As many sectors, maritime sector has been affected by developing technology. Autonomous systems have allowed to reduce the number of crew members. However, since these systems are equipped with computers, ships have become vulnerable to cyber attacks. In autonomous ship projects, which are today frequently becoming a current issue and attracting the attention of many professionals from the maritime sector, one of the crucial question marks is undoubtedly potential cyber attacks. As a result of the analysis of the attacks that the maritime sector is exposed, it is seen that some of these attacks are targeted attacks, and other part is untargeted attacks. Nevertheless, maritime sector is under the risk of potential cyber attacks by a teenager sitting in front of a computer at home, or by the specialized groups supported by governments. Such attacks may endanger vessel and crew safety, cause marine pollution or economic losses.

3.1. Maritime Safety, Maritime Security and Maritime Cybersecurity

The meanings of “safety” and “security” are synonymous basically (Mejia, 2002). Turkish language has two separate words for “safety” and “security” as “emniyet” and “güvenlik” respectively. On the other hand, only one word is used for “safety” and “security” in Chinese, French and Spanish languages (Li, 2003). In the Table 3.1, the words of “safety” and “security” in different languages are shown.

Table 3.1. Words of “safety” and “security” in different languages (Li, 2003)

English	safety	security
Turkish	emniyet	güvenlik
Chinese	安全 (anquan)	
French	securite	
Spanish	seguridad	

Although “safety” and “security” have similar meanings, there are differences between these terms. Although “safety” is a protection term against “hazards”, “security” term is precaution against “criminal activities”. “Security” is related with “threat” (Eirik, 2003). Whereas the source of “security” concept is a form that threatens the security, the source of “safety” is measures that must be taken so that a false or deficient behavior or negative conditions don’t cause undesired result (Solmaz, 2012).

“Maritime Safety” concept is the vital study field of IMO, and is being developed by the SOLAS Convention. The slogan of “Safety at Sea” which is written on the accommodation, in general draws the attention immediately when viewed from the ship’s deck. “Safety at Sea” slogan, generally draws the attention readily when viewed from the ship’s deck. This implementation aims to increase the safety awareness of seafarers. Since, a seafarer can jeopardize human life, ship, environment and transported cargo as a result of an unintentional mistake. The consequences of potential accidents may be even more severe due to the offshore voyages of the ships.

The concept of “Maritime Security” means illegal and planned attacks against ships and crew. It is started to be discussed, and improved after the attacks organized against The World Trading Center on 11th September 2001. In order to prevent the terror rampages against ships, ports and facilities after the attack, ISPS (International Ship and Port Facility Security) code was developed. (Solmaz, 2012)

“Maritime Cybersecurity” is investigated by IMO under Maritime Security category. MSC (Maritime Safety Committee) and FAL (Facilitation Committee) publishes regulations and guidance, and then these are circulated to maritime sector. Maritime cybersecurity is the subject under the maritime security. It is a known fact that cyber attacks in maritime sector are not only caused by criminal reasons, such as drug-smuggling or data theft, but also attacks are organized to determine target vessels for pirate activities. Capturing a vessel and using the vessel as a physical platform for further attacks by using cyber attack is also one of the developed scenarios. (Sen, 2016)

3.2. Cybersecurity in General Terms

Today that the digital transition continues, the attacks as well started to come through computer systems. Due to recent cyber attacks that affected large masses, cybersecurity occupies the agenda constantly. Also, due to the fact that usage of internet and especially social media has increased rapidly in all age groups, the concept of cybersecurity is within everyone's area of interest. The cybersecurity is not only about computer, it is a concept that contains all devices with signal exchange.

3.2.1. The Definition of Risk

Many people give a negative meaning to it when they hear the word of risk. However, this is just a mistake. As opposed to popular belief, risk does not only have a negative meaning, but also a positive meaning. While some sources refer risk as a negative effect, other interpret risk as an opportunity (Raz & Hillson, 2005). In this study, negative effect of risk is emphasised rather than positive effect. Therefore, negative definition of risk will be considered under cyber risk framework. Cyber risk as per IRM (Institute of Risk Management) is that any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems (IRM, 2014).

There is a legendary narrative about the question and answer of the "What is risk?" in internet. According to this narrative, the professor asks, "What is risk?" in an exam. One of the students only gives the blank exam paper that he wrote "This is the risk." and gets the full score from the exam. The professor asks again the same question in the next exam, and this time all students without exception, answer the question by writing "This is the risk". This time, however, everyone gets the full score from the exam, except the student who gets the full score from the first exam. The professor explains the situation as "under the same conditions, the person who takes the same risk twice is stupid". This story tells us that the word of "risk" can be encountered in life, both as an opportunity and as a threat.

3.2.2. Definition of Cyber Attack

Cyber attack is explained as an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (International Organization for Standardization & International Electrotechnical Commission, 2018). Cyber attacks may be carried out against companies and governments as well as individuals. Such attacks can be launched by computers, smartphones, tablets or electronic equipment developed for cyber attacks. Types of cyber attacks are divided into two categories as “Targeted Attacks” and “Untargeted Attacks”.

- Targeted Attacks: Targeted attacks where a company or a ship’s systems and data are the intended target. For a successful targeted attack, ship-specific attack method might be required. (BIMCO, 2018)
- Untargeted Attacks: Untargeted attacks where a company or a ship’s systems and data are one of many potential targets. Necessary information and tolls for untargeted attacks can be found on internet. (BIMCO, 2018)

3.2.3. Common Cyber Attack Methods

The current technological era brings along cyber threats as well. Cyber attacks are carried out in many different methods by malicious individuals, groups or state-sponsored organizations. Some of these methods can be easy to perform even by a teenager sitting at home, while others are very sophisticated and require experience and extensive knowledge. In this chapter, the most common cyber attack methods are specified.

3.2.3.1. Malware

Harmful softwares, such as viruses, worms, trojans and spywares are called malware. Malware is a generic name. Malware is used to damage infected devices or files and to steal personal data, photo and video (Sophos, 2013). Malware usually sets off users through warez software. It can set off easily through files downloaded via torrent, USB (Universal Serial Bus) memory sticks or any visited websites. Connecting a mobile phone to ship's computer to charge up can cause the virus to set off the ship's network. It may cause to collapse some systems, such as ECDIS (Electronic Chart Display and Information System). There are more than 1 million malwares in 22 categories worldwide (Paganini, 2019; UpGuard, 2019). However, especially the petya virus used for ransomware attacks between them should be specifically examined. Since, the petya virus has made its name in the maritime sector with the damage it has caused to Maersk. With the malware which is a type of ransomware, all files on the victim's computer become inaccessible, and these files cannot be accessed unless ransom is paid to the Bitcoin account issued by the attacker (Trend Micro, 2017). The Danish maritime company Maersk was also affected by the petya virus, which was developed to attack ransomware, and suffered about \$300 million from the attack (Sead, 2017).

3.2.3.2. MITM (Man in the Middle)

This is an attack type monitoring connection between two computer systems. This attack tries to steal information transferred from user to client computer (UpGuard, 2017). Even though this kind of attack can be made through different methods, it doesn't usually require significant information. Visits made to websites that has SSL (Secure Sockets Layer) certificate are safer against MITM (Man in the Middle) attacks. Because it provides an encrypted connection between the web server that broadcasts the website and the computer of the visitor.

3.2.3.3. Water Holing (Watering Hole)

As per the explanation of CESG (Communications Electronics Security Group) a new website is launched, or a live website is hacked. Purpose of this attack is to install a malware to a visitor's computer via this website (CESG, 2015). Popular websites that has security gap are tried to be find by the hackers. The malicious codes are injected to the website through this gap. And then, visitor of this website who usually doesn't have an installed firewall or anti-virus software, is affected by this attack.

3.2.3.4. Denial of Service (DoS)

This attack type is denial of service rather than data theft. This attack sends multiple requests to a server or a network. Server or network infrastructure cannot meet this demand, so that it is out of service. This attack aims for financial damage as service cannot be used. (Sophos, 2013)

3.2.3.5. Social Engineering

It is a non-technical attack method. As per the "Cybersecurity Handbook" published by C-DAC (Center for Development of Advanced Computing), victim is persuaded to share sensitive information like user ID, password via phone call, interview or e-mail. Obtaining information by listening to dialogues that contains business or personal information is considered under this attack. An Attacker can even go through the garbage to learn more about the victim, and to persuade the victim. (C-DAC, 2015)

3.2.3.6. Phishing

Attacker sends an e-mail to different accounts. This e-mail seems to be sent from reliable institutions, such as bank, e-mail provider or university, and this e-mail often request to click a link. Purpose of this attack is personal data theft by entering desired information to pop-up page. This information might include passwords, personal information and credit card numbers. (Sophos, 2013)

3.2.3.7. Spear Phishing

Application of this method is the same as phishing. The difference between these attack is while phishing is random, spear phishing is more targeted. Target can be an individual, department or a company. Additionally, more customised e-mail is sent. E-mail might contain name, logo or personal details of the victim. (Sophos, 2013)

3.2.3.8. Brute Force Attack

In this attack type, attacker has a database that contains various password combinations. To identify password to access the system, attacker automatically tries these passwords on the database by using a special software (Sophos, 2013). The high number of password combinations in the attacker's database increases the likelihood of the attack being successful.

3.2.4. Stages of a Cyber Attack

A successful cyber attack consists of four stages called survey, delivery, breach and affect. (CESG, 2015)

- **Survey:** This is the process where attacker searches for physical, procedural or technical vulnerability. Attacker searches internet services and social media or conducts technical analysis to gain as much as information s/he can. Attacker tries to gain information about employees, policies and procedures via social media and websites. As for technical analysis, attacker tries to uncover open ports, services, operating system and vulnerable applications. During technical analysis, attacker might use various softwares.
- **Delivery:** At this stage, attackers starts with attack initiative. Attack points are vulnerabilities detected during survey stage or predicted possible vulnerabilities. In order to benefit from the gaps determined, an attacker may give an infected USB stick, send an e-mail that includes a harmful attachment or create a fake website, and hope the victim to visit.
- **Breach:** After test attacks, attacker can now intervene in computer systems and network. At this stage, ship's computer or mobile devices can be interfered. Some data can be deleted or changed.
- **Affect:** Attackers that can successfully infiltrate to system aims to collect more information about the system to expand the effect of the attack. They might install various software and try to find new vulnerabilities. Attackers try to reach their ultimate target. These targets might include incorrect onboard IT and OT system operation, whole or partial control or altering recorded data. As a result of these attacks, economic loss may occur. It may cause crew to injure or die, or sea pollution.

3.2.5. Typical Characteristics of Cyber Threats

As attack levels increase from level 1 to level 5, they become more sophisticated. Level advancement not only improves attack methods, but also increases the qualification of aggressive groups. A level 1 attack can be carried out by a teenager sitting in front of a computer at home, even for entertainment purposes, while at level 5, the attackers appear to be more knowledgeable and experienced, as well as supported by countries for political or military purposes. In other words, these attacks are state-sponsored. Table 3.2 shows that there are five levels of cyber threats, and actors are divided into five categories (Bodeau, Graubart, & Fabius-Greene, 2010).

Table 3.2. Typical characteristics of cyber threats (Bodeau et al., 2010)

Level	Typical Threat Actors	Typical Intents of Threat Actors
1 Cyber Vandalism	Hackers, Taggers, and “Script Kiddies;” small disaffected groups of the above	Disruption and/or embarrassment of the victimized organization or type of organization (e.g., a specific Department or Federal government as a whole).
2 Cyber Theft / Crime	Individuals or small, loosely affiliated groups; political or ideological activists; terrorists; domestic insiders; industrial espionage; spammers.	Obtain critical information and/or usurp or disrupt the organization’s business or mission functions for profit or ideological cause.
3 Cyber Incursion / Surveillance	Nation-state government entity; patriotic hacker group; sophisticated terrorist group; professional organized criminal enterprise.	Increase knowledge of general infrastructure; plant seeds for future attacks. Obtain or modify specific information and/or disrupt cyber resources, specifically resources associated with missions or even information types.
4 Cyber Sabotage / Espionage	Professional intelligence organization or military service operative.	Obtain specific, high value information, undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future.
5 Cyber Conflict / Warfare	Nation-state military possibly supported by their intelligence service; very sophisticated and capable insurgent or terrorist group.	Severely undermine or destroy an organization’s use of its mission, information and/or infrastructure.

3.3. Cyber Attacks in the Maritime Industry

Especially in recent years, cyber attacks in the maritime industry are more frequently on the agenda. The attacks target maritime offices, ports and even ships. Attacks, in particular on ships attract more attention as they may lead to injury people and marine pollution. Further, cyber incidents should be investigated carefully, since one of the most significant question marks in autonomous ship projects is the possibility of cyber attacks. The major cyber attacks that have occurred in the maritime industry, are stated below.

3.3.1. Ports of Belgium and Netherlands (2011)

As per the report of EC3 (European Cybercrime Centre), since June 2011, attackers were intervening two container terminals, and one harbour company computer system. These cyber attacks lasted until 2013. Traffickers wanted to intervene location and movement of containers in ports. Attackers made an agreement with hackers. Hackers could intervene to cargo tracking and release system of the port with an infected e-mail sent to port staff. After a while, containers in the port which go missing without a cause, attracted attention, and police were involved. Trafficking group was in Holland. Hackers were in Belgium. Holland and Belgium police force arrested total of 15 people after busts in Belgium and Holland. After these busts, 1.3 million Euro cash, six firearms including machine gun and silencer, bullet-proof vests, 1044 kg cocaine and 1099 kg heroin were confiscated. (EC3, 2013)

Investigations showed that hackers informed traffickers about containers with valuable cargo. Lorry drivers that worked for trafficking group, stole the containers before harbour staff arrived. Hackers were then deleting containers from port system. Additionally, there was drug and weapons smuggling hidden in various legitimate cargoes, such as banana and timber. These smuggling containers were again tracked by hackers. (Bateman, 2013)

The attack is denominated as a phishing attack. Harbors and terminals are classified as spear-phishing, since they are targeted by attackers, and a planned attack. In such attacks, it is a significant protection method for employees to have information about cybersecurity and cyber attacks. If the port staff were aware of phishing attacks, these attackers might not have achieved their goals.

3.3.2. IRISL (Islamic Republic of Iran Shipping Lines) (2011)

In August 2011, IRISL (Islamic Republic of Iran Shipping Lines) was under a cyber attack. This attack damaged data regarding date, location, cargo number and rates. Various information was stolen. These data were not private, and was recovered later on. Additionally, internal communication network of the company was impacted and disabled due to this attack. (Jonathan & Torbati, 2012)

Company's operational activities were affected from this attack. Containers' locations were unknown. Cargo were shipped to incorrect destinations. Serious amount of cargo completely disappeared. Therefore, company faced serious financial loss. (Cyber Keel, 2014)

3.3.3. Australian Customs and Border Protection Service Agency (2012)

In 2012, hackers working for traffickers hacked cargo control system of Australian Customs and Border Protection Service Agency. Hackers had been learning containers that were identified as suspicious by the police and customs authorities. This way, during smuggling, containers with high capturing risk had been being selected by traffickers. (Kochetkova, 2015)

3.3.4. Danish Maritime Authority (2012)

In April 2012, it was seen that Danish Maritime Authority was subjected to a vital cyber attack. This cyber attack was announced to public in September 2014 (Cyber Keel, 2014).

This cybersecurity breach was uncovered after a notification by American IT expert in 2014. Investigations showed that when an employee in Danish Maritime Authority opened a PDF file that containing virus that was sent as an e-mail attachment, this virus infected an employee's computer and network respectively. It was seen that attackers want to obtain sensitive data about Danish shipping companies and merchant fleet. Whole network system for several days was shut down, and new anti-virus programmes were installed. It was announced that this attack was highly sophisticated, it was state-sponsored, and it is believed that this attack was organised by China. Chinese Embassy in Copenhagen refused all accusations, and announced that they had no knowledge about this attack. (The Local, 2014)

The same method was used in 2011, in the attack on the ports of Belgium and the Netherlands. This method is spear-phishing. Since it is a targeted attack. In this type of attack, it is crucial that the staff is aware. When checking emails that received from unrecognized people, more care should be taken. In this case, if the Danish Maritime Authority had not been warned by the American IT expert, more critical information would have been stolen by the attackers for at least for a while unfortunately.

3.3.5. Oil Rig Platform (2013)

In Gulf of Mexico, an oil rig platform off Houston experienced cyber attack in 2013. Cyber attack started when a malware infected oil worker's laptop who was working on the platform. It was seen that oil worker's laptop was infected from porn and pirated music downloaded. Investigations showed that these materials were still on the laptop (Sin, 2013). It was determined that this malware infected oil rig network by using USB stick. The computer system locked up because of the malware (Zain, 2013).

Controlling USB sockets is one of the main measures to be taken on board ships. In many guidelines on maritime cybersecurity draws attention to this issue. Accordingly, only authorized devices must be able to be connected to the USB sockets of computerized systems. Moreover, in the success of these untargeted attacks, the lack of the knowledge with the maritime cybersecurity risks of the seafarer occupies an important place.

3.3.6. South Korea (2016)

In April 2016, South Korea announced that around 280 vessels were under GPS (Global Positioning System) jamming attack. By reason of this attack, affected vessels were forced to go back to port (Graham, 2017). It was claimed that this attack was organised by North Korea. However, this claim was refused by North Korea (Saul, 2017).

Even if it is not confirmed with certainty that North Korea has carried out this attack, it is seen that quite sophisticated when the scope of the attack is examined. Further, GPS jamming attacks can not be performed with the help of a computer only, they also require technical equipment. For this reason, it is more likely to be a state-sponsored attack.

3.3.7. Hacking Broker's e-Mail Account (2016)

In 2016, a broker's e-mail account was hacked. The attacker who captured e-mail address, sent e-mail to a maritime firm, and demanded payment to be transferred to another bank account. The maritime firm completed approximately \$500,000 worth payment to declared bank account without verification. Due to this incorrect payment, the shipping company was forced to re-pay the broker, so that companies loss was \$500,000. (Belmont, 2016)

Although still the maritime company lost \$500,000 as a result of a cyber attack, also the financial department had a mistake here. If there is a critical information change, such as a bank account change, especially before making high-budget payments, the accounting department should investigate the matter. In this case, if the accounting department employees had called the broker before making the payment, the company would not have lost \$500,000.

3.3.8. Maersk (2017)

On 27th June 2017, Maersk announced on official website that they were under cyber attack by a virus called Petya (Maersk, 2017). All began when an employee in Ukraine opened to an email which featuring the Petya malware (Safety4Sea, 2018). Due to activated virus, various IT systems of Maersk were down. 4,000 new servers, 45,000 new PCs (Personal Computers) and 2,500 applications were reinstalled in 10 days to regain reliable operations. The economic cost of this attack was estimated at \$250-300 million. (Tung, 2018)

Maersk is one of the world's most important maritime companies, and has a wide range of employees. Even though the company had taken many cybersecurity measures prior to the attack, as an employee's lack of awareness of cyber risks, has affected from an untargeted attack, resulting in a loss of about \$300 million. It also suffered a loss of prestige. However, they managed the post-attack process well. Instead of trying to hide the attack, they made the necessary statements directly through their top management.

3.3.9. Russia (2017)

On 22nd June 2017, a ship off Novorossiysk-Russia shore notified U.S. Coast Guard Navigation Centre about GPS. According to this notification, the ship with more than 20 ships around showed wrong location on GPS. GPS gave a position inland (near Gelendzhik Airport), but vessel was actually drifting more than 25 NM (nautical mile) from it. After various investigation, it was found that this was a GPS spoofing cyber attack. Experts claimed that this attack was organised by Russia to test defence system against American missiles. (Goward, 2017; T. Humphreys, 2017)

GPS attacks, by their nature, cannot be carried out only with computers and require additional technical equipment. Although the attack was not admitted by the Russian government, it could be inferred that the attack was state-sponsored, given the scope of the attack and the number of ships affected.

3.3.10. Clarksons (2017)

British shipping services firm Clarksons announced on 30th July 2018 with a press statement that they were under cyber attack. Company announced that this cyber attack was between 31st May 2017 and 04th November 2017, and various personal data, such as seafarers' personal information, CVs (curriculum vitae), and financial data might be captured by hackers. This attack has been reported to police and regulators. Additionally, an investigation was started by receiving support from external experts. (Esage, 2018; John, 2018)

3.3.11. German-Owned Container Ship (2017)

In February 2017, en route from Cyprus to Djibouti, 8250 TEU (Twenty-foot Equivalent Unit) capacity German-owned container ship's navigation systems were controlled by hackers for 10 hours. Hackers planned to navigate this ship to a certain location, go aboard the ship, and take over the control. These plans were ceased by intervention of IT specialists. (Blake, 2017)

Although there is less information about the attack, it is very important as the command of ship have been passed to the attackers for 10 hours. It was the only incident where the navigation capability of the ship was completely lost during this literature survey. During the literature review, this was the only event in which ship navigation capability was completely lost. Therefore, it should be stated that this example has an important place in order to better understand the risks that ships may face.

3.3.12. BW Group (2017)

In July 2017, computer systems of BW Group which is an important leader in the global maritime sector, in Singapore was under cyber attack. During this attack, the computer systems were accessed in unauthorised manner by attackers (Ngai, 2017). During the cyber attack, business systems were inaccessible outside Singapore. Although company had officially verified this attack, there was no announcement on financial or data loss (Sameer, 2017).

3.3.13. Svitzer Australia (2018)

As per the news of WMN (World Maritime News), personal data of more than 400 employees of Australian-based Svitzer Australia that offers towage service under Maersk has been stolen. Reasons for this data theft were e-mail forwarding to e-mail addresses of three employees from two different e-mail addresses. This incident was detected on 01st March 2018, and investigation revealed that data theft was on-going since 27th May 2017. (WMN, 2018b)

3.3.14. COSCO Shipping (2018)

On 24th July 2018, COSCO (China Ocean Shipping Company) Shipping experienced a ransomware attack. This attack included U.S. offices of COSCO Shipping and Pier J Terminal in Port of Long Beach. COSCO's U.S. website, e-mail, phone and network infrastructure were affected from this attack, and systems were recovered after five days. (WMN, 2018a)

3.3.15. Austal (2018)

Australian ferry and defence shipbuilder Austal announced on 01st November 2018 that they experienced cyber attack. The company announced that their internal data were captured by attackers after this attack. The company stated that attackers contacted the company for ransom, but their demands were refused due to company policies. Australian Cybersecurity Centre and Australian Federal Police started an investigation to investigate this attack. (Maritime Executive, 2017)

3.3.16. Analysis of the Maritime Cyber Incidents

In the maritime sector, both targeted attacks and untargeted attacks can be seen. In particular, the ransomware attack which caused Maersk company to lose \$300 million is an important example of untargeted attacks in the maritime industry. For information theft, attacks can be carried out against the offices of maritime companies, and ransom can be demanded by attackers. Further, there are attacks allegedly supported by the state for both political and military purposes. It is claimed that especially the attacks on GPS systems of ships are supported by governments. Ports are another area has been attacked in the maritime industry. Attacks on ports are generally organized for carrying out smuggling activities. In addition to the GPS attacks, the case in which attackers has gained the full control of a large container vessel in 2017 also attracted quite attention. In Table 3.3, it is seen that the cyber attacks reflected in the press have increased especially in recent years. Due to these incidents in the press, the financial losses that could be caused by cyber attacks in the maritime sector became more understandable. For attacks that do not have an attack method and economic losses, N/A is written. There are 15 cyber incidents that took place in the media or academic studies in the maritime sector between 2011-2018. Only four of these are cyber attacks against direct ships. The other attacks were organized to ports and offices of maritime companies.

Table 3.3. Cyber attacks in the maritime industry

Year	Impact Area	Organization / Location	Affected System	Method	Impact	Economic Loss
2011	Shore	IRISL	Cargo tracking system	N/A	Operational interruption	N/A
2011	Shore	Ports of Belgium and Netherlands	Container tracking system	Spear phishing	Smuggling	N/A
2012	Shore	Australian Customs and Border Protection Service Agency	Container tracking system	N/A	Smuggling	N/A
2012	Shore	Danish Maritime Authority	Network	Spear phishing	Data theft	N/A
2013	Vessel	Gulf of Mexico	Network	Malware	Operational interruption	N/A
2016	Vessel	Coast off South Korea	GPS	GPS jamming	Blocking GPS signal	N/A
2016	Shore	A Broker's e-mail account	E-mail	N/A	Financial loss	\$500,000
2017	Shore	Clarksons	Network	N/A	Data theft	N/A
2017	Shore	Maerks	Network	Ransomware (Petya)	Operational interruption	\$250-300 million
2017	Vessel	En route from Cyprus to Djibouti	Navigation system	N/A	Full control by attackers	N/A
2017	Vessel	Coast off Russia	GPS	GPS spoofing	Wrong GPS location	N/A
2017	Shore	BW Group	Network	N/A	Operational interruption	N/A
2018	Shore	Svitzer Australia	E-mail	E-Mail forwarding	Data theft	N/A
2018	Shore	COSCO Shipping	E-mail, phone, website, network	Ransomware	Operational interruption	N/A
2018	Shore	Austal	Network	N/A	Data theft	N/A

3.4. Legislations and Vetting Programmes

Maritime transport is subject to international laws. However, for both ships and offices, inspections are taken with commercial concerns, and aim to succeed in these inspections. Cybersecurity rules as a precaution against cyber incidents in the sector have been included in both mandatory regulations and non-mandatory vetting programmes.

3.4.1. Mandatory Regulations

Maritime is a global profession, so the industry has globally valid rules. Ships engaged on international voyages, and the operators governing these ships must comply with these international rules. There are two codes that can be associated with cybersecurity at sea, namely ISM Code and ISPS Code. The ISPS Code indicates that the ship's computer systems should also be evaluated, during a security assessment on the ship. ISM is an only mandatory code, is issued by IMO, regarding directly maritime cybersecurity.

3.4.1.1. ISPS Code

After 9/11 attacks, maritime security studies have accelerated. As a result of these studies, ISPS Code was entered into force on 01st July 2004 under SOLAS Convention. This code includes necessary security practices in ports and vessels. It is applicable to all vessels over 500 grt operating on international trades, as well as the ports that service them. There are two sections as Part A and B. Part A includes mandatory requirements, and Part B includes recommendations. In accordance with the requirements of ISPS Code, each vessel covered by ISPS Code must specifically have an SSA (Ship Security Assessment). As per ISPS Code Part B, 8.3, SSA should cover radio and telecommunication systems, including computer systems and networks of the ship.

3.4.1.2. ISM Code

Under ISM Code, all shipping companies are mandatory to add “Guidelines on Maritime Cyber Risk Management” manual to their SMS (Safety Management System) manuals until 01st January 2021 (IMO, 2017c). In compliance with ISM Code, for firms which have DoC (Document of Compliance), cybersecurity risk assessment will be mandatory as of 01st January 2021, and this assessment will be inspected in the first DoC inspection following this date. DoC means a document issued to a company which complies with the requirements of ISM Code (IMO, 2014a).

3.4.2. Non-Mandatory Vetting Programmes

There are numerous accidents in the history of tanker transportation (Havold, 2010). There are two well-recognized and non-profit organizations to decrease accidents, and increase the service quality in the maritime industry for tanker transportation. These are OCIMF (Oil Companies International Marine Forum) and CDI (Chemical Distribution Institute). SIRE (Ship Inspection Report Programme) and TMSA (Tanker Management and Self-Assessment) programmes were developed by OCIMF that has important place in the maritime industry. Because “Consultative Status” was given to OCIMF by IMO. CDI that is another organization, provides vetting service for chemical tankers and gas carriers. These programmes also cause a competition among tanker operators. They play a critical role in commercial life of tanker firms. On the other hand, RightShip provides significant vetting service for dry cargo ships. Questions and efficiency of RightShip that offers vetting service for dry cargo ships, were assessed to maritime cybersecurity, because although OCIMF and CDI are non-profit organisations, RightShip’s private company status leads to questions about efficiency. However, it is seen that there are challenging vetting questions posed by RightShip. Noted observations during vettings may negatively impact both commercial life and reputation.

3.4.2.1. SIRE

An essential vetting program developed by OCIMF is SIRE and this program was launched in 1993. The aim of this program was to increase safety and quality standards on tankers. After vetting, inspection reports can be accessed by OCIMF members such as bulk oil terminal operators, port authorities, canal authorities, oil, power, industrial or oil trader companies which charter tankers/barges as a normal part of their business. (OCIMF, 2019)

SIRE inspections are conducted by SIRE experts on vessels. SIRE inspections have various questionnaires. Oil tankers, combination carriers, shuttle tankers, chemical tankers and gas tanker audits are conducted on VIQ (Vessel Inspection Questionnaire). There are total of 12 chapters. These are shown at the Table 3.4 below.

Table 3.4. Chapters in VIQ 7 (OCIMF, 2018)

Chapter No	Topic
Chapter 1	General information
Chapter 2	Certification and documentation
Chapter 3	Crew management
Chapter 4	Navigation and communications
Chapter 5	Safety management
Chapter 6	Pollution prevention
Chapter 7	Maritime security
Chapter 8	Cargo and ballast systems – petroleum
	Cargo and ballast systems – chemicals
	Cargo and ballast systems – LPG
	Cargo and ballast systems – LNG
Chapter 9	Mooring
Chapter 10	Engine and steering compartments
Chapter 11	General appearance and condition
Chapter 12	Ice operations

The last edition called VIQ 7 entered into force on 17th September 2018. It can be seen that in this edition, cybersecurity related questions are included in “Chapter 7: Maritime Security”.

The questions regarding maritime cybersecurity in the VIQ 7 and comments are explained as following.

Question 7.14: *Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard?* (OCIMF, 2018)

This question requires risk assessment related to cybersecurity, providing information about cyber threats, identifying key contacts, password management and mitigation measures. In current inspections, inspectors first want to see if there is a plan. Risk assessment criteria do not challenge ship operators under current conditions. However, it is possible that inspectors will emphasise this topic over time. Some inspectors examine prepared plans in detail to make sure that these plans are created as ship specific.

Question 7.15: *Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems?* (OCIMF, 2018)

This criterion requires USB and RJ-45 (Registered Jack-45) port control on shipboard IT/OT systems. Thus, the main objective is to prevent virus infection on navigation equipment, such as ECDIS. This item is commonly interrogated during inspections. SIRE inspectors examine if USB ports and RJ-45 connections are under control. Precautions of companies are physically locking USB or RJ-45 portals or only permitting authorised devices and memory sticks to these ports by using cybersecurity software. There are numerous hardwares with RJ-45 and USB ports from the bridge to the engine room in a ship. Although the secured status of all hardwares is not controlled by the inspectors yet, the secured status of USBs in equipment, such as ECDIS, GPS and VDR (Voyage Data Recorder) are examined carefully.

Question 7.16: *Does the company have a policy or guidance on the use of personal devices onboard?* (OCIMF, 2018)

This question examines if there is a procedure that prevents visitors on the ship (For example 3rd party contractors) to connect to ship network by using their personal devices, such as crew's smartphone, tablet and memory stick. It is accepted that there are various visitors, such as custom, agent, surveyor on ships. These individuals might be given with ship memory stick for special printouts. These memory sticks might contain virus, and this virus might infect the ship network and prevent IT/OT system to work in a reliable way. Declining printing on the ship side might lead to disruption in the operation. Therefore, this topic leads to discussions. To meet these criteria, ship operators can provide an independent computer and printer from ship network, and allocate these devices only to 3rd parties. Ships without this system might want sending an e-mail to the ship and printing that e-mail. Company procedures prohibit charging mobile devices, such as crew and visitor's tablets and smartphones on USB ports.

Question 7.17: *Is Cyber Security awareness actively promoted by the company and onboard?* (OCIMF, 2018)

This question examines raising awareness of the crew against cyber threats. Inspectors observe existence of cybersecurity related posters on IT terminals. Posters known as "Social Media Guidance for Seafarers" or "Golden Rules" published by INTERTANKO (International Association of Independent Tanker Owners) are especially recommended. Additionally, it is recommended for the crew to watch cybersecurity related training videos, and keep these training records as evidence.

3.4.2.2. TMSA 3

TMSA programme is developed by OCIMF. Purpose of this program is to contribute tanker management firms to develop their SMS (OCIMF, 2019). While SIRE is based tankers, TMSA is based on auditing offices of tanker management firms. Companies give their answers to published questions. These answers are examined by TMSA experts via office audits. Office audits are not conducted periodically. Major oil companies, such as Chevron, Shell and BP (British Petroleum) may demand for TMSA office audit, and conduct this audit. These audits approximately take between two and three days. TMSA has 13 sections. These sections are called “elements”. The elements of TMSA are shown in the Table 3.5 below.

Table 3.5. Elements in TMSA 3 (OCIMF, 2017)

Element No	Topic
Element 1	Leadership and the safety management system
Element 2	Recruitment and management of shore-based personnel
Element 3	Recruitment, management and wellbeing of vessel personnel
Element 4	Vessel reliability and maintenance including critical equipment
Element 5	Navigational safety
Element 6	Cargo, ballast, tank cleaning, bunkering, mooring and anchoring operations
Element 7	Management of change
Element 8	Incident reporting, investigation and analysis
Element 9	Safety management
Element 10	Environmental and energy management
Element 11	Emergency preparedness and contingency planning
Element 12	Measurement, analysis and improvement
Element 13	Maritime security

Questions are called as KPI (Key Performance Indicator). In TMSA, KPIs are divided into four levels. First level is basic, and fourth level is the most advanced stage. Firms that try to pass TMSA audit successfully, must meet the whole requirements of level 1 at least. Some charterers might require from tanker management companies to get a higher TMSA stage. That's why tanker firms try to meet the highest stage of requirements possible. In this way, the firms will have the opportunity to offer carrying service to a wider range in the maritime sector.

Before charter party agreements with MOCs (Major Oil Company), TMSA performance of tanker manager is reviewed. Depending on the type of charter party agreement, whole or partial KPIs in a certain stage of TMSA can be required for tanker management company by MOC. Although it is not officially declared, according to charter party agreements of various MOCs, TMSA stages demanded from tanker management companies are listed below (Karti, 2017).

Level 1 → Tanker manager is satisfactory for V/C (Voyage Charter)

Level 2 → Tanker manager is satisfactory for CoA (Contract of Affreightment)

Level 3 → Tanker manager is satisfactory for T/C (Time Charter)

Level 4 → Tanker manager is satisfactory for a joint venture with a MOC

Element and stage of a KPI can be easily understood from the code number. An example code number is shown in the Figure 3.1. below. The first part of the code number gives the element number, the middle part shows the KPI level, and also the last part consists of the KPI number.

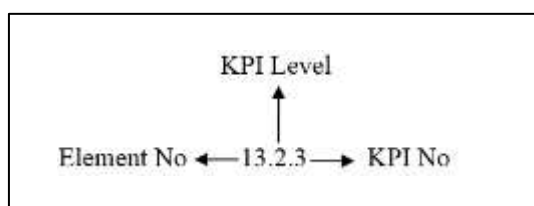


Figure 3.1. An example code number of a KPI in TMSA

TMSA has been introduced to maritime sector in 2004. In 2008, scope and content were expanded with TMSA 2. On 10th April 2017, OCIMF published a guide for TMSA 3 which entered into force on 01st January 2018. One of the most striking revisions in TMSA 3 is “Element 13: Maritime Security” which is new. This element has cybersecurity related KPIs at 2nd level, so that tanker firms were forced to take action regarding cybersecurity. The KPIs regarding maritime cybersecurity in the TMSA 3 and the comments are explained as following.

KPI 13.2.3: Policy and procedures include cybersecurity and provide appropriate guidance and mitigation measures. (OCIMF, 2017)

This KPI expects risk assessment towards IT systems and technical and procedural precautions for these risks from ship operators. Inspectors desire to analyse cybersecurity related company policies and procedures. Within policies and procedures, precautions for social media use is also analysed. Currently, there is no detailed analysis of risk assessment.

KPI 13.2.4: The company actively promotes cybersecurity awareness. (OCIMF, 2017)

This KPI questions awareness of both crew and shore staff about cybersecurity. Social media use, secure password selection and controlled use of portable storage devices are inspected. Inspectors might want to investigate training related recordings. Additionally, familiarity of the office personnel can be tested and inspected with different methods. For example, according to the senior manager of a tanker operator firm, after an inspector in the office to inspect TMSA completed the inspected, the inspector asks to give a memory stick to an office staff to print the report. Office staff declines the request of the inspector by stating that USB drive cannot be connected to office computers due to technical precautions. Later, the inspector says that this was a trick to assess staff’s awareness about cybersecurity.

3.4.2.3. CDI Ship Inspection

CDI is a non-profit organization. Inspections are conducted in marine transport to increase safety, security and quality performance. These inspections are conducted based on published CDI Ship Inspection Report. (CDI, 2019a)

For both chemical tankers and liquified gas carriers, it can be seen that two questions related with cybersecurity have been added to version 9.8.1 of CDI Ship Inspection Report that will enter into force on 02nd September 2019. CDI Ship Inspection Report has 14 sections. These sections are listed in the Table 3.6 below.

Table 3.6. Chapters in CDI Ship Inspection Report (CDI, 2019b)

Section No	Topic
Section 1	Certification, manning etc.
Section 2	Management and personnel
Section 3	Bridge
Section 4	Mooring
Section 5	Cargo operations
Section 6	Engine department
Section 7	Operational safety
Section 8	Health, safety and personnel protection
Section 9	Firefighting
Section 10	Lifesaving
Section 11	Environmental protection
Section 12	Security
Section 13	Hull and superstructure
Section 14	Accommodation

Cybersecurity related questions are included under “Section 12: Security”. When these questions in the guideline are analysed, it is seen that “Recommended” category was designated for these questions. This means “Referenced to industry Codes of Practices”. Additionally, these questions are included in the group “I”. Group “I” means “Inspections questions” are for full inspection by the inspector”.

In CDI SIR, it is shown 2nd version of GCSOS (The Guidelines on Cyber Security Onboard Ships) as a reference created with the support of important marine authorities, such as IMO, BIMCO, INTERTANKO and OCIMF. In fact, there is a striking point. Although GCSOS version 2 was referenced for criteria in SIR 9.8.1, 3rd version which is the latest version of GCSOS, was published at the end of 2018. Thus, an older version is referenced within CDI SIR.

Currently, how challenging is cybersecurity related conditions in CDI inspections are unknown. Application of CDI SIR 9.8.1. version and observations noted by inspectors will give a general idea. The cybersecurity related questions and comments are explained below.

Question 12.11: *The company provides guidance on cybersecurity (CDI, 2019b)*

This criterion examines risk assessment. Additionally, preventive precautions for cyber threats and vulnerabilities are recommended. Also, contingency plan to be applied in case of cybersecurity is questioned.

Question 12.12: *The crew has been trained in company guidelines, policies or procedures on cybersecurity. (CDI, 2019b)*

It is expected from the crew to complete cybersecurity related training and to keep records of these training as evidence. Crew must be familiar with possible cyber threats and vulnerabilities.

3.4.2.4. Rightship

Rightship is an Australia based vetting firm. This firm provides vetting service for tankers and dry cargo vessels. In vetting inspections for tankers, SIRE questionnaires are used by Rightship. However, for dry cargo vessels, RightShip has own questionnaire. This questionnaire for usage in inspection of dry cargo ships, has 10 sections shown below Table 3.7.

Table 3.7. Sections in Rightship questionnaire (Rightship, 2017)

Section No	Topic
Section 1	Vessel particulars
Section 2	Documentation
Section 3	Effectiveness of ISM system
Section 4	Safety, security & environmental management
Section 5	Structural condition
Section 6	Machinery management
Section 7	Bridge management
Section 8	Holds – ventilation, lighting securing
Section 9	Condition of cranes
Section 10	Inspection summary

One of the inspected topics is “cybersecurity” which is under “Section 4: Safety, Security & Environmental” title. Rightship’s questions related with cybersecurity and comments are given following.

Question 4.7.1: *Does the vessel and/or company have documented software/firmware and hardware maintenance procedures?* (Rightship, 2017)

Maintenance reports of IT/OT systems are desired to be examined. Additionally, existence of a procedure that needs to be applied prior to any software or firmware update is questioned.

Question 4.7.2: *Does the vessel and/or company have any cybersecurity procedures?*
(Rightship, 2017)

This question examines conducting risk assessment against cyber attacks. Additionally, it is possible to control existence of response in case of a cyber attack.

Question 4.7.3: *Does the vessel and/or company provide any cybersecurity training?*
(Rightship, 2017)

This question examines the awareness of crew regarding cybersecurity. The inspector would like to see training records as an evidence.

3.4.3. Analysis of Legislations and Vetting Programmes

Even though it is desirable to assess the computer system and ship network in the scope of the ISPS Code via the SSA, this is not sufficient and needs to be improved. ISM Code is the only mandatory regulation that emphasize on cybersecurity directly. Requirements related to cybersecurity are included in the vetting questionnaires developed by CDI, OCIMF and RightShip. These requirements consist mostly of procedural measures. Particularly emphasis is placed on the crew's cybersecurity awareness.

3.5. Vulnerable Systems to Cyber Attacks onboard Ships

There are a variety of computerized systems in order to ensure safe operation on ships. These systems may contain some vulnerabilities. An example list which covers vulnerable systems onboard ships is given by IMO (IMO, 2017a).

3.5.1. Bridge Systems

The bridge has various navigation systems and navigation aids. With advancements in technology, these systems are vulnerable to cyber attacks. Some of these systems are listed below.

3.5.1.1. Voyage Data Recorder (VDR)

Voyage data recorder (VDR) means a complete system, including any items required to interface with the sources of input data, for processing and encoding the data, the final recording medium in its capsule, the power supply and dedicated reserve power source (IMO, 1997). VDR can store data in three categories as static, dynamic and voyage related. The data recorded in the VDR may include some or all of the following data at the Table 3.8 (Shao, Teng-da Sun, Jia-cai Pan, & Xian-biao, 2007).

Table 3.8. The data can be recorded by VDR (Shao et al., 2007)

Static	Dynamic	Voyage Related
MMSI (Maritime Mobile Service Identity)	Ship's position	Draft
Call sign and ship name	Position time	Dangerous cargo (type)
IMO number	Course over ground	Destination and ETA (Estimated Time Arrival)
Length and breadth	Speed over ground	Route plan (Waypoint)
Vessel's type	Navigational status	
Position of antenna	Rate of turn	

3.5.1.2. ECDIS

ECDIS means a navigation information system which with adequate back-up arrangements can be accepted as complying with the up-to-date chart required by regulations V/19 and V/27 of the SOLAS Convention, as amended, by displaying selected information from a system electronic navigational chart (SENC) with positional information from navigation sensors to assist the mariner in route planning and route monitoring, and if required display additional navigation-related information (IMO, 2006). While ECDIS is an equipment that enhances safety of navigation, it also makes it easier for OOW's (Officer of the Watch) to prepare a passage plan. ECDIS, which also allows electronic logging, may be examined for accident investigation after a possible accident.

3.5.1.3. GNSS (Global Navigation Satellite Systems)

Although GPS is a popular location service around the world, Russian alternative GLONASS (Global Orbiting Navigation Satellite System) and GPS are parts of GNSS system. GNSS is a satellite group for sending signals from space and used in global positioning. (Kaplan & Hegarty, 2017)

US-based GPS and Russian alternative GLONASS (Global Orbiting Navigation Satellite System) services are two most popular location services. However, a new service will be added to these in the near future. EU (European Union) started operations for its own independent GNSS service "Galileo", and it is planned that this system will have reached full operational capability by 2020. (Kaplan & Hegarty, 2017)

3.5.1.4. AIS

AIS provides automatically to appropriately equipped shore stations, other ships and aircraft information, including the ship's identity, type, position, course, speed, navigational status and other safety-related information (IMO, 2014b). AIS is divided into two groups as Class A and Class B. Class A of AIS is used on all vessels which sailed on international voyages of 300 GT (Gross Tonnage) and above. On the other hand, Class B is for use on vessels, such as pleasure crafts that are not subject to SOLAS. AIS onboard must be continuously active. It may only be turned off by the Master for security reasons.

3.5.1.5. ARPA / Radar

Automatic Radar Plotting Aid (ARPA) is a radar function, and used by ship's officers as an important barrier against collision. This could operate independent of GNSS. This system warns OOWs with automatic tracking, and plotting of contact identified by radar, and contacts that might create dangers based on predetermined criteria. (Bhatti & Humphreys, 2014)

3.5.2. Access Control Systems

While growing digitalisation decreases physical security concerns, questions are raised on cybersecurity risks. CCTV (Closed Circuit Television), SSAS (Ship Security Alarm System), and BNWAS (Bridge Navigational Watch Alarm System) are main systems that has cybersecurity risk. CCTV that enables interior and exterior vessel monitoring for possible security problems. SSAS that notify flag state and company when the vessel is in danger. BNWAS that ensures navigation safety on bridge.

3.5.3. Cargo Handling and Management Systems

Cargo management system usually take place on bridge or in a designated area called CCR (Cargo Control Room) in the accommodation space. With cargo management systems in CCR, loading and discharging operations can be carried out. Additionally, these systems can store cargo related data, and enables cargo monitoring during voyage. The temperatures, levels and tank pressures of the cargo being transported are controlled from this center. Positions of the valves can be controlled through panels in the CCR. These areas are rigged with computerized systems. Structuring computerized systems independent of the ship's network, in other words in an isolated way, has a critical importance to protect against cyber attacks.

3.5.4. Propulsion and Machinery Management and Power Control Systems

Developing technology has brought together the machines and computerized systems, and it has brought out the automation technology. Automation systems that are used in vessels to decrease operational expenses, and increase efficiency, but also increase cybersecurity risks. The propulsion system, auxiliary engines, steering gear and monitoring softwares supported with digital technologies have vulnerabilities. Controlling area of the engine room is called ECR (Engine Control Room). Lots of data, such as working performance of the machinery systems, levels of the tankers, the pump pressures, the ship's electrical measures can be examined by responsible engineers. At the present time, ship machinery management systems can be monitored even remotely at shore. This makes these systems more defenseless against cyber attacks.

3.5.5. Communication Systems

Developing technology made ability of ship-to-ship or ship-to-shore communication possible. Vessel might have various satellite connections for data and audio transmission. Security of these connections should be ensured by communicating with service providers. Satellite connection should not be damaged when on-board network connection safety is ensured.

VHF/UHF is used for meeting Ship-to-Ship and Ship-to-Shore communication needs through the frequency band. S-Band of 2.4 GHz (Gigahertz) and 5 GHz frequency connections are used in Bluetooth and Wi-Fi applications. GSM based internet connections, such as 3G, 4G and 5G to meet the internet needs of passengers and ship's crew. (BIMCO, 2018; Boyes & Isbell, 2017)

3.5.6. Passenger Servicing and Management Systems

Developing technology affected the passenger servicing and the management systems. Whereas passengers' information used to be kept as hardcopy in the past, with the effect of digitalism, now this information is kept in computers and followed up. The security controls are provided with the card pass systems. Card pass system used by passengers, visitors and ship's crew, financial related systems, electronic health records are systems that are open to cyber attack. (BIMCO, 2018)

3.5.7. Passenger Facing Public Networks

The technology of V-SAT (Very Small Aperture Terminal) made broadband internet connection possible through satellites even in offshores. So, the internet connection can be provided to the passengers in order to spend time, and make their daily work. Wi-Fi and LAN (Local Area Network) connections used by passengers create a suitable circumstance for cyber risks. These systems must definitely be isolated of ship's safety critical systems. Because of the access of the passengers to network, the network traffic can be kept under control only limited.

3.5.8. Administrative and Crew Welfare Systems

Nowadays, internet connection can be provided in cargo vessel just like passenger ships for crew's utilization for a price or free. Whereas some of these services allow only e-mail communication, some systems offer broadband internet connection. Due to the decrease of the fee of internet connection, the number of maritime companies that provide internet access for crew's daily utilization increases.

In addition to the daily use of crew, the internet connection for healthcare is now available on boards. Besides that, a video consultation with a doctor can be made, as well as electronic medical records of seafarers can be kept. Moreover, remote refresher medical training can be given on board, under the supervision of a doctor. (Sharples, 2018)

This situation increases the risk of being affected of a possible cyber attack. The network used by the crew must definitely isolated from the ship's critical systems. Also training the crew against cyber risks, decreases the possibility of being harmed from a possible attack.

3.6. The Cyber Attacks Methods towards GPS, AIS, ECDIS and ARPA-RADAR

GPS, ECDIS, AIS and ARPA-Radar are critical navigation equipment. Any errors that will occur in these equipments, risk the safe navigation of the ship. Moreover, given both published academic research and cyber incidents reflected in the press, attacks, in particular against these systems, have been successful. Therefore, it is necessary to investigate specifically the attacks against the subject systems.

3.6.1. Attack Methods to Global Positioning System (GPS)

Today, ships use computer based navigation systems (Su, He, Cheng, & Chen, 2016). GPS as a part of GNSS system is extremely important for this computer-aided navigation systems. GPS signals travel at light speed which is approximately 300,000 km/sec (Joseph, Drumhiller, & Roberts, 2017). When GPS signals are measured from Earth's surface, these signals are weak. This makes these signals vulnerable against attacks (Grant, Williams, Ward, & Basker, 2014).

3.6.1.1. GPS Jamming

C4ADS (Center for Advanced Defense Studies) is stated that GPS jamming is also called brute force jamming (C4ADS, 2019). GPS jamming where radio noise is broadcast on the GPS frequency. This noise blocks the use of GPS, and could disable the vessel's ability to navigate safely (Vistiaho, 2017). However, due to the GPS failure alert, OOW may realize the problem. Further, there are anti-jamming devices against GPS jamming attack. Although the applications of these devices to land vehicles are currently available, no such application exists for ships. There are many GPS jamming attacks that affect a large area, as in an attack affecting about 280 ships on the Coast of South Korean.

3.6.1.2. GPS Spoofing

GPS spoofing attack causes that targeted GPS shows wrong location by receiving false GPS signal (Lund, Hareide, & Jøsok, 2018). GPS spoofing attack is more dangerous than GPS jamming attack (T. E. Humphreys, Ledvina, Psiaki, Hanlon, & Kintner, 2009). Because in case of GPS spoofing attack, this attack might not be detected by OOW. This endangers safe navigation of the ship. For GPS spoofing attack, three methods listed below may be used. The equipments for subject attack methods are shown in the Figure 3.3 (T. E. Humphreys et al., 2009).

- GPS Signal Simulator (Simplistic Attack)
- Portable Receiver-Spoofers (Intermediate Attack)
- Multiple Phase-Locked Portable Receiver-Spoofers (Sophisticated Attack)

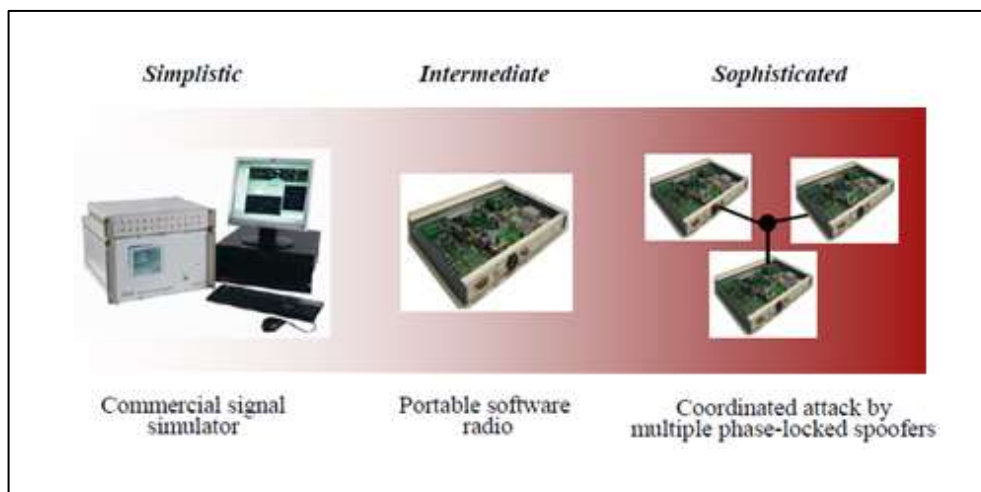


Figure 3.2. Required equipments for GPS spoofing attack (T. E. Humphreys et al., 2009)

- GPS Signal Simulator (Simplistic Attack):
This is less dangerous compared to other GPS spoofing methods. Because it generally looks like GPS jamming and therefore, when there is an abnormal situation on GPS, OOW can detect GPS to be unreliable.

This is because of the difficulty of synchronizing a simulator's output with the actual GPS signals in its vicinity. An unsynchronized attack effectively acts like signal jamming. (T. E. Humphreys et al., 2009)

- Portable Receiver-Spoofers (Intermediate Attack)

For a GPS spoofing attack to be successful, the target receiver antenna's location and velocity must be known. This knowledge is required to precisely position the counterfeit signals relative to the genuine signals at the target antenna. It is easy to detect GPS spoofing attacks without an exact location. (T. E. Humphreys et al., 2009)

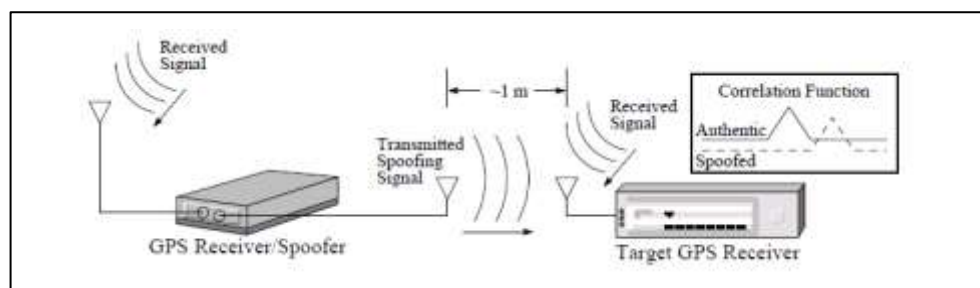


Figure 3.3. Illustration of a spoofing attack via portable receiver-spoofers

(T. E. Humphreys et al., 2009)

In this method, the receiver component receives real GPS signals to detect its own position, speed and time information. Spoofers component transmits false GPS signals via an antenna which is placed to targeted GPS receiver near. The targeted GPS receiver is affected from false GPS signals which causes to show incorrect location to user. It might be extremely hard to detect attacks with portable receiver-spoofers. Because the devices can be manufactured at small size. (T. E. Humphreys et al., 2009)

It is a nice experiment that in 2013, researchers from University of Texas applied GPS spoofing attack to superyacht (LOA (Length Overall): 65m) called “White Rose of Drachs” and sheered this yacht from actual course. Fore of the yacht had GPS antenna. Stern part has spoofers RX (Receive) antenna. Spoofers device processed signals from RX antenna and transmitted to TX (transmit) antenna. GPS antenna of yacht confused these fake signals with real signals and deviated from course. (Bhatti & Humphreys, 2014)

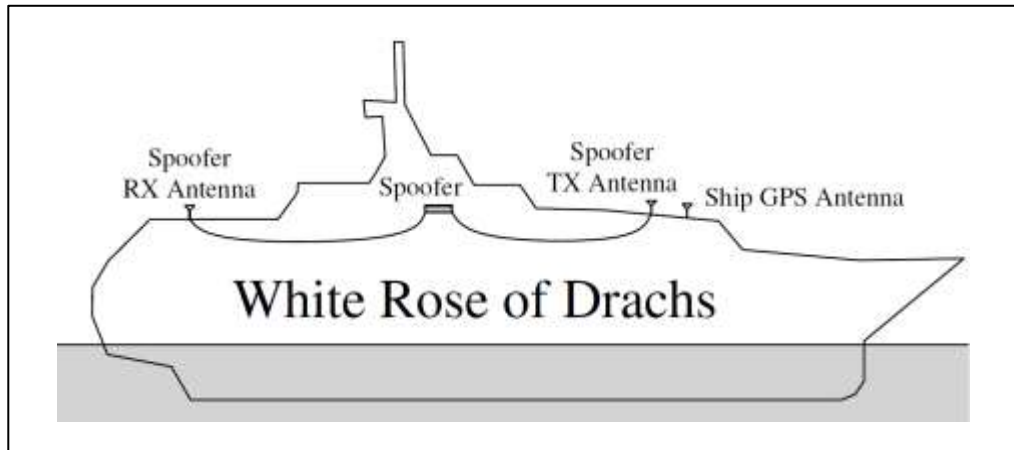


Figure 3.4. Sketch of the spoofer setup on the White Rose of Drachs
(Bhatti & Humphreys, 2014)

- Multiple Phase-Locked Portable Receiver-Spoofers (Sophisticated Attack)

The angle-of-arrival defense against a portable receiver-spoofers may be blocked by a coordinated attack with as many receiver-spoofers as antennas on the target GPS receiver. Receiver-spoofers the size of a pack of cards small enough to mount directly atop a target antenna. The receiver-spoofers receiving and transmitting antennas are placed respectively on the upper and lower faces of the device and are shielded to avoid self-spoofing. Now imagine several such devices sharing a common reference oscillator and communication link, with each device mounted to one of the target receiver's antennas. The angle-of-arrival defense fails under this attack scenario. An attack via multiple phase-locked portable receiver-spoofers is somewhat less likely than an attack via single portable receiver-spoofers, but may be impossible to detect with user-equipment-based spoofing defenses. (T. E. Humphreys et al., 2009)

3.6.2. Attack Methods to AIS

Academic research has shown that AIS has several vulnerabilities. It is possible that there will be a marine accident due to these vulnerabilities, which could result in damage to the vessel, cargo, crew and marine. Attacks against AIS can be carried out both through the software and RF (Radio-Frequency).

3.6.2.1. Ship Spoofing

This attack type enables creating a fake ship. This fake ship can have flag, speed, position, course, destination, cargo, ship type, dimension, call sign and MMSI information like a real vessel. Additionally, underway, moored and anchored states of the vessel can be provided. With this attack, it is possible to create different scenarios. For instance, a fake ship that carries nuclear cargo in territorial waters of a country that doesn't allow nuclear cargo in its territorial waters. (Balduzzi, Pasta, & Wilhoit, 2014)

3.6.2.2. Collision Spoofing

One of the reasons to install AIS is to reduce collision risk between vessels. CPA (Closest Point of Approach) property of AIS enables this risk to be reduced. A distance is set to use this feature. When any vessel enters inside this distance, the system alerts the OOW. With Collision Spoofing attack, fake data can be created to force the OOW to change course of the vessel. (Balduzzi et al., 2014)

3.6.2.3. AtoN (Aids-to-Navigation) Spoofing

By the help of AtoN (Aids-to-Navigation), the OOW is warned about dangers in the vicinity of vessel, such as low tides, rocky outcroppings and shoals (Balduzzi et al., 2014). With AtoN spoofing attack, fake data can be created to force the OOW to change course of the vessel. (Balduzzi et al., 2014)

3.6.2.4. Weather Forecasting

AIS provides information about environmental factors, such as sea current and climate condition (Balduzzi et al., 2014). If the master does not receive confirmation from another source, it may alter the course of the ship due to incorrect weather data. The master may even decide to anchor in a safe area. However, such a situation will lead to financial loss of the tanker operator.

3.6.2.5. AIS Hijacking

The method of AIS Hijacking has two variations. In one of the variations, attacker listens and changed AIS signals broadcasted from ship. In the other version, stronger fake signals are transmitted to suppress real AIS signals. In both variations, receiver station receives modified messages by attacker rather than original AIS messages. (Balduzzi et al., 2014)

3.6.2.6. Disruption Threats

There are a variety of interruption threats in AIS. These threats are categorized under three main headings as follows.

- Slot Starvation

Attacker acts like maritime authority to absorb AIS address space. This attack affects all vessels and AIS gateways, and prevents AIS system usage at wide range. (Balduzzi et al., 2014)

- Frequency Hopping

The attacker seems as maritime authority, and forces AIS transponder to change operation frequency. Due to operating logic, AIS is adapted to this frequency. In this way, AIS can no longer be used. (Balduzzi et al., 2014)

- Timing Attack

The attacker forces AIS transponder to delay transmission time. The attacker repeatedly sends commands to do this. This prevents AIS transponder to send signals. (Balduzzi et al., 2014)

3.6.2.7. AIS-SART Spoofing

AIS can be used for SAR (Search and Rescue) operations. Vessels have a device called SART (Search and Rescue Transponders). This device is used in case of abandon ship, and enables casualty to be visible on the radar screen in the vicinity of vessels and planes. AIS detects this signal and alerts. Because of this attack, AIS is forced to give SART alarm, and ship crew might be involved in unnecessary SAR operation. (Balduzzi et al., 2014)

3.6.3. **Attack Methods to ECDIS**

When installed a malware, the attack can perform three kinds of actions: It can manipulate GPS coordinates via the network, and the malware can crash the operator station by provoking a bluescreen (Lund et al., 2018). Additionally, electronic maps used by ECDIS can be accessed and modified. In 2014, a research was conducted on Windows 7 (x32) installed computer without anti-virus software and firewall. Test results showed certain vulnerabilities. ECDIS software can run with outdated Apache Web Server, and this version of Apache has certain vulnerabilities. Due to these vulnerabilities, attackers can access and modify electronic maps used by ECDIS. (Dyryavyy, 2014)

3.6.4. Attack Methods to ARPA – RADAR

In 2017, after receiving required permissions, Israel based Naval Dome firm, a series of cyber penetration test was conducted on various tankers, container ships, super yachts and cruise ships. As a result of these tests, radar was manipulated by using local Ethernet Switch Interface. Radar targets were eliminated, simply by deleting them from the screen. During this attack, radar did not give any alert or warning to attract attention of OOW. (Shefi, 2017)

3.7. Protection Cybersecurity Measures towards Tankers

Computerized systems on tankers must be protected against cyber threats. Not only technical measures, but also procedural measures are required for protection. The implementation of these measures should be monitored carefully and ensured that they are effective. Inadequacies in implementation cause the measures taken to be ineffective. Procedural measures can usually be accomplished with resources that company owned, nevertheless third party support may be required for technical protection measures.

3.7.1. Technical Protection Cybersecurity Measures towards Tankers

Technical measures include both software and hardware measures, and may also require a budget. Although these measures increase tanker opex (Operational Expenses), it is necessary to ignore the expenses to be incurred, considering the financial loss and reputational losses of the tanker operator in a successful cyber attack. When taking technical measures, IT professionals who are experts and experienced in their fields should be consulted.

3.7.1.1. Anti-Virus Softwares

Anti-virus software are automated tools, and these tools can protect computerized systems against harmful effects of malware. It may be combined with a firewall to analysis internet traffic against harmful malwares. It is important to make sure that anti-virus software is always up-to-date. Because new viruses are served to the internet everyday by the attackers, so that it is beneficial to activate automatic update option if it is available. Internet access on ships may be expensive. For this reason, managers of marine companies can disable automatic update option. This situation risks computer systems in the ship.

3.7.1.2. VPN (Virtual Private Network)

Company servers should be accessed over dedicated VPN (Virtual Private Network) for secure access (Sophos, 2013). In marine companies, there may be servers in order to carry out some functions, such as accounting, PMS (Planned Maintenance System) and file storing. Accessing this serves out of office, in other words, though directly internet is not secure. Because the internet used outside may be monitored. On account of VPN technology, internet connections made out of the office is made secure by encrypting. The attacker sees only encrypted data which can not be retrieved.

3.7.1.3. Encryption

Important folders and files should be encrypted by using encryption software. This way, anyone who does not has the password, can not open your folders, and can not access the data inside the files (Sophos, 2013). While making up the code to open the file or the folder, attention should be paid. Making up the code with the combination of letter, number and symbols reduces the possibility of being broken by the attacker.

3.7.1.4. Back-Up

The files should be backed-up periodically. This way, it is possible to avoid data loss if files are inaccessible or files are corrupt. Having back-ups in different location is a precaution against scenarios like sinking or fire. Back-up file and restoration procedure should be regularly tested. (Branch & January, 2019; Joint Hull Committee, 2015)

3.7.1.5. Up-to-Date Software and Operating Systems

Always, current version of software must be installed as per the guideline of ABS (American Bureau of Shipping). Installation and updates should only be applied by experts and authorised personnels, such as service engineers and IT specialists. These updates must be tested before installation, and reliable operation must be verified. If there is, automatic update option must definitely be activated. (ABS, 2016a)

3.7.1.6. Wireless Encryption

Due to the decrease of the price of internet in the ship, now the companies can provide internet access for crew as paid or free. This internet is usually provided through one modem, and is extended to accommodation wirelessly. If there is a wireless network on board, this network must be encrypted with a method like WPA 2 (Wi-Fi Protected Access 2) (Sophos, 2013). Unencrypted wireless networks can be easily accessed by the attackers.

3.7.1.7. Isolated Navigation Systems

The researches made and the cyber incidents experienced showed that there were various weaknesses in navigation equipment in the ships, such as ECDIS, GPS and ARPA radar. Also, a cyber attack against navigation equipment risks safe navigation directly. Navigation systems on bridge must be isolated from vessel network. This way, if network of vessel is under cyber attack, navigation systems will not affect from this attack. (Transas, 2017)

3.7.1.8. Secured Remote Connection

Because of advanced technology, it is possible to remotely connect with vessels. With these connections, vessel's performance can be monitored in real-time, alarm records can be analysed, physical intervention, such as valve control can be applied, and real-time video stream is possible over cameras (Ulstein, 2019). However, these opportunities have cyber attack risk, as well. Therefore, when there is no need for remote access, hardware (e.g. switch) or software based access should be stopped. In case of remote connection, data transmission between vessel-shore must be encrypted.

3.7.1.9. Protection Interfaces such as USB, RJ-45 and Card Reader

Interfaces, such as USB, card reader, RJ-45 and optical drives should be kept down. Usage of these interfaces should be limited or disabled. Various visitors including customs, port authorities and agencies visit vessels in ports. These individuals might ask for prints by providing their memory sticks. In this case, they might be asked to send this document as an e-mail to vessel. Another precaution is to have a dedicated computer independent of vessel network. A printer can be defined for this computer to prevent virus infection on vessel network after third party visits. (BIMCO, 2018)

3.7.1.10. Administrative Privileges

Computers onboard must not have administrative privileges. Restricted user account without authorisation for software installation or uninstallation should be created for the ship crew. The possibility to authorize flexibly the users via various computer security software must be publicized to system admin. Utilization of these softwares will prevent the crew to set up risky software.

3.7.1.11. Penetration Test

Penetration test enables identification of effectiveness of protective systems. In case of vulnerabilities, action lists can be created to close these vulnerabilities. Penetration tests are classified into two main groups as internal and external. Both must be applied periodically, so that it is possible to be prepared against cyber attacks from the inside and the outside.

3.7.1.12. Dedicated USB for License and Chart Data

A dedicated USB should be determined to update licence and charts of ECDIS, and these USBs should have warning notice. This dedicated USB should only be used for communication PC and ECDIS. This way, virus infection risk to ECDIS will be decreased. Bridge can have two ECDISes. In this case, two dedicated USBs should be determined. (Transas, 2017)

3.7.1.13. Combined GPS and GLONASS

Location accuracy that provided by GPS or GLONASS may not be satisfied either due to cyber attacks or low signal quality. Dual frequency receivers are available in which GPS and GLONASS are combined, and can be purchased easily from the market (Moaiied & Mosavi, 2016). In case of a GPS spoofing attack, receivers in which are GPS and GLONASS combined can also be used on ships. Thus, if GPS or GLONASS is exposed to spoofing attack, the OOW may be warned by the equipment and additional measures may be taken to ensure safe cruising without accident.

3.7.2. Procedural Protection Cybersecurity Measures towards Tankers

Taking only technical measures is insufficient for a successful cyber defense, procedural measures must also be taken. When taking procedural measures, not only the IT professionals, but also should be benefited from experienced masters, officers and engineers, since some of the procedural measures require operational experience on the ship.

3.7.2.1. Ensure Cargo Tank Pressure/Vacuum

With tank monitoring system, pressure/vacuum status of cargo tanks can be monitored from CCR. It is important to monitor tank pressure/vacuum, and keep these within certain limits. Being off-limits might damage physical structure of the vessel. As a result of cyber attack, pressure/vacuum system can be manipulated. To prevent possible losses due to this event, P/V (Pressure/Vacuum) valve maintenance should be completed on-time, problem-free operation of valves should be ensured, tank pressure should be regularly controlled over mechanical gauge on the tank.

3.7.2.2. Train the Trainer

Ship crew must be trained based on certain plan. These trainings can be in-house, as well. At this point, knowledge of trainer is an important topic. Also trainers should have required training and awareness on this topic. (Transas, 2017)

3.7.2.3. Ensure Cargo Line Pressure

With tank monitoring system, pressure of cargo line can be monitored from CCR. Pressure of cargo line should not exceed permitted limits. Otherwise, line could be damaged. Therefore, tank monitoring systems have an alarm. This alarm can be manipulated after a possible cyber attack. Therefore, pressure gauge of line in manifold area should be regularly controlled as a precaution.

3.7.2.4. Check Sounding / Ullage

Level indication systems are extremely important for both officers and engineers. With this system, volume of liquids, such as cargo, ballast, fresh water, HFO (Heavy Fuel Oil) and MGO (Marine Gas Oil) in tanks can be instantaneously measured. These systems can affect from a possible cyber attack. Therefore, sounding should be taken periodically. Sounding tape can be used for this control. For cargo tanks, portable ex-proof UTI (Ullage Temperature Interface) detector must be preferred.

3.7.2.5. AIS - ARPA (Radar) Association

ARPA (Radar) and AIS targets should be integrated in ECDIS. By association, the position, course and speed of the target vessel can be compared against the received AIS information from this vessel. This allows assessing data quality provided by AIS. Ensure AIS targets and ARPA targets are available on the ECDIS or radar. It is beneficial to issue a procedure to check both information for one target against each other. (Transas, 2017)

3.7.2.6. Classify Data

Lots of data is kept in the computers of the ships. Nowadays, almost each operation is made through computers. Various records such as the crew list, the cargo storage plan, the passage plan and the risk assessment may be kept in the computers. Current data in the computers should be classified, and crew should understand which data is important.

3.7.2.7. Manual Position Fix in ECDIS

GPS spoofing attack is frequently encountered. Procedures are necessary for manual position fix (Transas, 2017). This is a crucial precaution against GPS spoofing attack, which is a type of attack that affected around 20 ships in the coast of Russia in 2017.

3.7.2.8. The Procedure of Management of Change (MoC)

The objective of this procedure is to ensure a planned approach to all proposals for changes which may impact health, safety, security, environment, or quality of fleet vessels, the company, and its systems. Therefore, all proposals for changes are to be investigated,

evaluated, approved, reviewed, verified, and documented to ensure safe and proper management. MoC (Management of Change) procedure should be created and execution of MoC procedure when there is an application or modification that affects IT and OT system can decrease risks and enable fast reaction against such problems. (ABS, 2016b)

3.7.2.9. Create Company Policy

Company must issue a cybersecurity policy. This policy must meet regulatory and reporting requirements. Additionally, this policy must meet technology usage targets of the company (ABS, 2016c). Also, presence of a company policy about cybersecurity in TMSA, CDI and SIRE inspections are questioned.

3.7.2.10. Equipment Disposal

Hard disc, CD (Compact Disc), DVD (Digital Versatile Disc) and USB stick are for data storage. These equipments might have confidential information belongs to company. That's why a procedure is necessary for disposal and destruction. In the procedure, the one responsible for demolishing the equipment and method of demolishment must be stated.

3.7.2.11. Develop a Plan

Creating a plan for cybersecurity will be beneficial. This plan is also known as Cyber Security Plan (CSP) or Incident Response Plan (IRP) in different resources. Content of this plan might change based on organisation recommendations and requirements. Therefore, needs of the company should be identified and plans should be created to meet these needs. This plan may consist of risk assessment, contact details, training plan, drills, incident reports, circulars, resources, inventory list, response and recovery plans.

3.7.2.12. Awareness

As per the guideline of DNV-GL (Det Norske Veritas - Germanischer Lloyd) trainings organised by qualified trainers should be provided. These trainings should include company policies, procedures and previous incidents related to cybersecurity. Trainings of individuals should be recorded. (DNV-GL, 2016)

Ship crew must understand the importance of cybersecurity. Regular drills should be organised. Cybersecurity related posters should be hanged to visible areas inside the vessel (ABS, 2016c). Circulars published by maritime authorities should be shared with crew. Starting with flag states and class societies, various reputable organisations or institutions around the world are organising training programs and publishing circulars regarding cyber attack to raise awareness in the maritime industry. If there is not qualified trainer, maritime cybersecurity related training can be purchased from third parties such as;

- DNV-GL
- Lloyd's Maritime Academy
- KVH Videotel
- Maritime Training Services

3.7.2.13. Password Security

None of the equipments should be operated with default password. Passwords should not be kept in easily accessible areas. Password should be as long as possible. If possible, passwords should include combination of upper case letter, lower case letter, number and character. A strong password is the best precaution against brute force attack. Additionally, organization implements login failure time-out periods to prevent password guessing. (ABS, 2016c; Sophos, 2013)

Also, if all passwords in the office and on vessel should be kept in a secure place, and individuals with access permissions for these passwords should be identified (ABS, 2016a). Individuals with access permission can be designated officers or engineers on board.

3.7.2.14. Physical Security of Critical Hardware

Critical equipment and cable runs should be physically protected from interference by concealment or physical security, i.e. locked compartments subject to strict access controls. These areas should be identified within Ship Security Plan. (Joint Hull Committee, 2015)

Ship Security Plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident. (IMO, 2012)

3.7.2.15. Assign a Responsible Person

It is recommended to assign at least one person to ensure cybersecurity. Senior management should decide whether this person should be on-board or in office. When this decision is made, it is important to consider certain criterias, such as vessel type, tonnage, number of crew and voyage area. Having a qualified person onboard will enable faster reaction against cyber attacks. (BIMCO, 2018; Boyes & Isbell, 2017)

Designated person might have responsibilities, such as following local and international regulations, conducting periodic assessments, creating and developing a plan related to cybersecurity, investigating cybersecurity incidents, evaluate risks, identify policy and training needs and provide these trainings. (ABS, 2016a; BIMCO, 2018; Boyes & Isbell, 2017)

As per reputable resources, the person with these responsibilities may be entitled as CISO (Chief Information Security Officer) or CySO (Cyber Security Officer) (ABS, 2016a; Boyes & Isbell, 2017). Designated person should be a person related with maritime operations rather than IT. IT experts are required to meet business needs. Cybersecurity begins at senior management level of the company. Because a possible cyber attack will impact operations and business process of a company. Additionally, implementations of vetting requirements, such as TMSA and Rightship, communication with customers or reporting to maritime authorities are outside the scope of IT specialist responsibilities. (BIMCO, 2018; JWC International, 2017)

3.7.2.16. Social Engineering

E-mails that ask for the passwords or personal information shouldn't be replied. While logging into an account in a computer or a mobile device, people around should be look out, and be sure that no one is watching. While posting on social media, the next port the ship arrives must not be shared.

3.7.2.17. Remote Access

Remote access must be limited. Individuals with permission of remote access should be designated. Permission should be taken from the company if third parties, such as service engineers require to connect. Log in and log out time of connected individuals, connected individual or organization, and connected system should be recorded. (ABS, 2016a)

3.7.2.18. Key Performance Indicator (KPI)

Key Performance Indicator (KPI) is used for evaluating a situation in qualitative or quantitative way. KPI can be kept for cybersecurity. Possible KPIs are listed under three groups (Rishikesh Sahay & Daniel Sepúlveda Estay, 2018).

- Behavioral indicators: impact time, detection time, time to recovery etc.
- Financial indicators: Cost of recovery, implementation costs for preventive / recovery, cost of mitigation, cost of disruption etc.
- Structural indicators: Number of Unsafe Control Actions, Proportion of Unsafe Control Actions per Accident etc.

3.7.2.19. Phishing and Spear Phishing

An important protection method is not clicking on links inside e-mails or downloading attachment files. This is an effective precautions against phishing and spear phishing attacks. Additionally, anti-virus software with phishing detection property are beneficial. (Sophos, 2013)

3.7.2.20. Develop a Risk Assessment

In compliance with ISM Code, for firms which have DoC, cybersecurity risk assessment will be mandatory as of 01st January 2021, and this assessment will be inspected in the first DoC inspection following this date (IMO, 2017c). Risk assessment preparation is already a requirement of TMSA 3 and Rightship (OCIMF, 2017; Rightship, 2017).

A suitable risk assessment method for business structure and cybersecurity risks should be preferred. Due to technological developments and changeable nature of business structure, risk assessment should be regularly reviewed. Risks, preventive actions, possible losses should be re-evaluated. Not only risks should not be considered as possible attacks and natural disasters, but also equipment malfunctions and human errors should be considered. Based on risk assessment, various vulnerabilities can be detected. These vulnerabilities should be classified based on priority, and then these vulnerabilities should be eliminated by taking their priorities into consideration. (ABS, 2016c)

3.7.2.21. URL or Web Content Filtering

Various malware and phishing attack can happen through websites. That's why it is possible to prevent access of websites in certain categories or with certain URLs (Uniform Resource Locators) to reduce infection risks. Websites containing warez content, torrent websites, pornographic websites and hacking websites are the ones to which access must be denied.

3.7.2.22. Prepare an Inventory List

Critical systems of the ship that may be affected of cyber attacks should be determined. Version numbers and last update date for softwares of these critical systems should be listed, and this list should always be up-to-date by a responsible person (Boyes & Isbell, 2017).

3.7.2.23. Participate the Vetting Programmes

Tanker operators should participate in SIRE, CDI and TMSA which are defined as vetting programmes and also the criteria related to cybersecurity taking place in questionnaires in those programmes should be regarded. So, both cybersecurity related issues are developed on the ship, and these issues are externally inspected. From commercial perspectives, the performance of the tanker operator in vetting programmes is increased, thus expanding the cargo option available to transport.

3.7.2.24. Keep a Proper Lookout

Due to cyber attacks in the maritime sector, proper a lookout has become even more important. Advancing technology causes officers to build excessive confidence in navigation equipment used on ships. Because of this extreme confident on electronic devices, the lookout is not effectively carried out by every officer. It should be well understood by the officers that the fact that these devices are equipped on board to improve navigational safety does not remove the need of effective lookout.

3.8. Literature Review

The aim of the literature review is to outline the issue of maritime cyber security, to identify the cyber risks at sea and the measures that can be taken against these risks. Further, a literature review is required to choose the accurate risk assessment method as well.

During the literature review, academic papers, dissertations, guidelines and books related to maritime cyber security were identified. Moreover, in order to identify the cyber incidents occurred especially in the maritime sector, research was also carried out on the internet. Research has also been conducted on the subject through the National Thesis Center of the Turkish Higher Education Institution, the IMarEST (Institute of Marine Engineering, Science & Technology) databank and the online library of the World Maritime University founded by IMO. Then, the resources obtained were categorized in accordance with the objectives of the thesis and examined in detail.

During the literature review, academic studies published in recent years were particularly regarded. The reason for this is that as a result of the development of computer technology in the past years, some risks have disappeared, and some risks have become more prominent. In addition, the studies that have been cited more than others regarding the research subject and the objectives of the thesis have been given priority. It is seen that basic studies on maritime cyber security are based on these articles.

During the literature review, both the cyber incidents in the maritime sector and various navigation equipments that have proven their vulnerability through academic studies such as GPS, ECDIS, AIS, ARPA-Radar were found. There was not found any research for cargo management systems, which is the main factor that determines the types of ships. This situation ensures that this study complements a significant deficiency in the literature.

Risk assessment is one of the objectives of the thesis, and identifying the accurate risk assessment method plays a crucial role. Hence, the literature has been reviewed not only in relation to maritime cyber security, but also in risk assessment methods. During the literature review, it was seen that risk assessment methods were divided into two groups as quantitative and qualitative. In order to better evaluate the results obtained, it is necessary to choose among the quantitative risk assessment methods. Different quantitative risk methods such as Fault Tree Analysis, Event Tree Analysis, Attack Tree, Failure Mode and Effect Analysis have been widely used in academic studies. During the review to the literature, it was seen that there is not enough data and statistical studies with regard to cyber incidents occurring in the maritime industry. For this reason, undertaking the risk assessment by a focus group that consist of people who are knowledgeable about the subject is important for increasing the accuracy of the results of the thesis. Also, the inclusion of expert opinions in the risk assessment led to the use of the fuzzy logic approach. Fuzzy logic is an important method that is recommended to be used in cases where there is not enough data and expert opinions are required. Since it is a quantitative risk assessment method and there are successful studies of this method combined with fuzzy logic in the literature, it was decided to use the Fine-Kinney risk assessment method in this study.

Table 3.9 shows frequently used resources in line with the purposes of this study. These sources consist of articles, thesis and books. This table contains academic studies on cyber vulnerability of various equipment on board, fuzzy logic approach, Fine-Kinney risk assessment method, vetting programs in autonomous ships and tankers. In sum, it is seen that academic studies on cyber security at sea have been carried out particularly for the last 10 years. For this reason, it may be stated that maritime cyber security is a new research area.

Table 3.9. Featured researches towards the purposes of the thesis

No	Surname, Name	Type	Year	Title	Scope
01	Bodeau, Deborah J Graubart, Richard Fabius-greene, Jennifer	Article	2010	Improving Cyber Security and Mission Assurance via Cyber Preparedness	AIS
02	Shao, Zhe-ping Teng-da Sun Jia-cai Pan Xian-biao, Ji	Article	2007	Vessel Information Service System based on ECDIS and AIS	ECDIS AIS
03	Bhatti, Jahshan Humphreys, Todd E.	Article	2014	Covert control of surface vessels via counterfeit civil GPS signals	GPS
04	Su, Jie He, Jianping Cheng, Peng Chen, Jiming	Article	2016	A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle	GPS
05	Grant, Alan Williams, Paul Ward, Nick Basker, Sally	Article	2014	GPS Jamming and the Impact on Maritime Navigation	GPS
06	Vistiaho, Petteri	Thesis (MSc)	2017	Maritime Cyber Security Incident Data Reporting for Autonomous Ships	Autonomous ships
07	Lund, Mass Soldal Hareide, Odd Sveinung Jøsok, Øyvind	Article	2018	An Attack on an Integrated Navigation System	INS
08	Joseph, Drenzo Drumhiller, Nicole K Roberts, Fred S	Book	2017	Issues in Maritime Cyber Security	Maritime cyber security

No	Surname, Name	Type	Year	Title	Scope
09	Humphreys, Todd E Ledvina, Brent M Psiaki, Mark L Hanlon, Brady W O Kintner, Paul M	Article	2009	Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer	GPS
10	Kaplan, Elliott D. Hegarty, Christopher J.	Book	2017	Understanding GPS/GNSS	GPS GNSS
11	Balduzzi, Marco Pasta, Alessandro Wilhoit, Kyle	Article	2014	Security Evaluation of AIS Automated Identification System	AIS
12	Balduzzi, Marco Pasta, Alessandro Wilhoit, Kyle	Article	2014	A Security Evaluation of AIS Automated Identification System	AIS
13	Karti, Efstathia N	Thesis (MSc)	2017	Vetting and TMSA: Role and Requirements in the Shipping Industry	Vetting
14	Ross, Timothy J.	Book	2010	Fuzzy Logic with Engineering Applications	Fuzzy Logic
15	Kinney, G. F. Wiruth, A. D.	Article	1976	Practical Risk Analysis for Safety Management	Fine-Kinney Risk Assessment
16	Sivanandam, S. N. Sumathi, S. Deepa, S. N.	Book	2007	Introduction to Fuzzy Logic Using MATLAB	Fuzzy Logic MATLAB
17	Birgoren, Burak	Article	2017	Calculation Challenges and Solution Suggestions for Risk Factors in the Risk Analysis Method in the Fine Kinney Risk Analysis Method	Fine-Kinney Risk Assessment

4. MATERIALS AND METHODS

In this study, the risks of cyber attack that may occur in the bridge, engine room and cargo control room of the tankers that are underway, have been evaluated. During the study, it was seen that experts could evaluate an existing cyber threat differently. In order to avoid misclassification of the threat, these differences were re-evaluated with the fuzzy logic approach. During the literature review, it is found that there are many academic studies where fuzzy logic is combined with risk analysis methods. Fine-Kinney is also a quantitative risk assessment method that can be combined with fuzzy logic. It is also possible to take advantage of the Matlab during the calculations.

4.1. The Method of Fuzzy Logic

Fuzzy logic concept was first proposed in 1965 by an Azerbaijani scientist Prof. Lotfi A. Zadeh in Berkeley University, California, and fuzzy logic system was first used in 1975 in steam engine control (Ross, 2010). The fuzzy logic carries out the math in the real life. It lets an expert's opinions to turn into numerical value and its evaluation in computer environment. It provides to make logical inference by giving numerical value to verbal expression of the expert such as "low", "lot", "some". The fuzzy logic brings option of making operation despite deficient or not known well information to the researcher. In classic logic the value is 0 or 1. In fuzzy logic the values are in between 0 and 1. Whereas there are only two levels in classic logic, there are multiplexed levels in the fuzzy logic. Fuzzy logic is divided into four main bases, and these are listed below.

- Fuzzy sets
- Linguistic variables
- Probability distribution
- Fuzzy "if-then"

4.1.1. Advantages of Fuzzy Logic

Several important advantages of fuzzy logic are given below.

- Fuzzy logic is not complex, and it is easy to understand (Manoj & Shah, 2014).
- Expert views can be used in fuzzy logic systems.
- Fuzzy logic is highly flexible. It can be combined with various control methods. Thus, more accurate results could be obtained (Chugh, Chaudhary, & Rizwan, 2015).
- Fuzzy logic is based on daily language.

4.1.2. Disadvantages of Fuzzy Logic

In addition to its advantages, fuzzy logic has several disadvantages, which are mentioned below.

- Expert views are important when rules are formed. Incorrect assessments by experts can lead to incorrect determination of risk levels.
- There is no method for membership function selection. The function selection decision is made only after trials.

4.1.3. Fuzzy Set Theory

While classical set logic has sharp limits, fuzzy set logic does not have these sharp limits. Fuzzy set is a mathematical concept developed to define uncertainties. Elements of a fuzzy set are between the numbers of 0 and 1 and with different membership degrees. Main rules of the set theory developed by Aristoteles are listed below.

- X, is either an element of a set or not.
- Intersection of the elements of a set and others is an empty set.
- If X is not an element of a set, it does not belong to that set.
- Union of the elements of a set and others is a universal set.

4.1.4. Membership Function

Membership function is the most important element of fuzzy set theory. Fuzziness in fuzzy sets is determined by membership functions. A membership function is a figure assigns membership values or membership degree that corresponds to each member and defines fuzzy set properties. Each point in input area is defined with a membership value between 0 and 1 values.

Fuzzy Logic Membership Function:

$$\mu_A(x) = E [0,1] \quad (4.1)$$

Classical Logic Membership Function:

$$\mu_A(x) = \begin{cases} 1; & x \in A \\ 0; & x \notin A \end{cases} \quad (4.2)$$

Membership functions enable tangibly represent fuzziness state regardless of continuous or discrete status of the elements in the set and show membership degree of these elements in the set. Transitions between membership degrees are smoother with these functions.

4.1.5. Membership Value Assignment

Membership value assignment may be intuitive or based on logic. The assignment methods are divided into five main types, however it is doable to say more methods. These are listed below. (Ross, 2010)

- Intuition: This method requires no or little information. In this method, membership functions depend on humane intuitions and it can vary from person to person.
- Inference: This method requires precise information.
- Rank order: This method depends on survey. Assessment is carried out either by one individual or by a group.
- Neural networks: These are applied with software programmed in line with human thinking.
- Genetic algorithms: This method depends on selecting the most suitable option.

4.1.6. Sections of Membership Function

All parts of a fuzzy set that contain information generate its membership function. Using its own terminology to better identify the membership function makes it easier to understand. Regarding the terminology, the emphasis was put on the simplicity. A membership function consists total of four sections, such as core, support, boundary and height. Subject terms are valid not only to discrete but also to continuous fuzzy set. The details for these sections are provided below. (Ross, 2010)

- Core: The membership function is equal to 1. This represents the set elements with a full-membership degree. It is defined by the equation 4.3.

$$\mu_A(x) = 1 \quad (4.3)$$

- Support: This section of the membership function is larger than 0. It is defined by the equation 4.4.

$$\mu_A(x) > 0 \quad (4.4)$$

- Boundary: Elements with a partial degree that do not have 0 or 1 value in a fuzzy set are included in this section. It is defined by equation 4.5.

$$0 < \mu_A(x) < 1 \quad (4.5)$$

- Height: The highest membership degree of the fuzzy set represents the height of that set. It is defined by equation 4.6.

$$\max [\mu_A(x)] \quad (4.6)$$

In the Figure 4.1, the sections as boundary, core, and support of the membership function are shown.

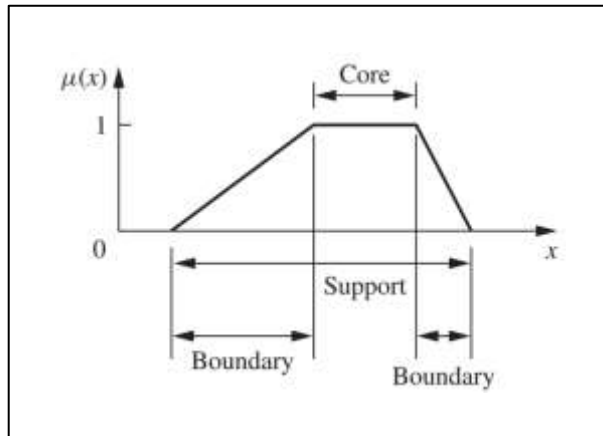


Figure 4.1. Core, support and boundaries of a fuzzy set (Ross, 2010)




4.1.7. Types of Membership Function

Membership functions provide a concrete expression of the current fuzzy situation, regardless of the continuity or disjointed of the members of the set. Moreover, these functions are used to demonstrate the degree to which these elements belong to the set. The transition between membership degrees takes place in a calm structure without any interruption and sharpness through functions. (Kaya, 2018)

- Triangular membership function
- Trapezoidal membership function
- Gaussian membership function
- Sigmoidal membership function
- S-Shape membership function

Types of membership functions are shown in the Table 4.1 below with the functional equation and graphic. (Falah, 2018)

Table 4.1. Types of membership functions (Falah, 2018)

Types of Function	Function Equation	Function Graphic
Triangular Membership Function	$\text{Triangular}(x;a,b,c) = \begin{cases} 0 & x < a \\ \frac{x-a}{b-a} & a \leq x \leq b \\ 1 & b \leq x \leq c \\ \frac{c-x}{c-b} & b \leq x \leq c \\ 0 & c \leq x \end{cases}$ <p>a, b, c: x coordinate for capital triangle x: the real value from the private variable fuzzy universe of discourse.</p>	
Trapezoidal Membership Function	$\text{Trapezoidal}(x; a, b, c, d) = \begin{cases} 0 & x < a \\ \frac{x-a}{b-a} & a \leq x \leq b \\ 1 & b \leq x \leq c \\ \frac{d-x}{d-c} & c \leq x \leq d \\ 0 & d \leq x \end{cases}$ <p>a, b, c, d: x- coordinates of the four heads of the trapezoidal</p>	
Gaussian Membership Function	$\text{Gaussian}(x;c,\sigma) = e^{-\frac{1}{2}\left(\frac{x-c}{\sigma}\right)^2}$ <p>c: function center σ: the function width</p>	

Types of Function	Function Equation	Function Graphic
Sigmoidal Membership Function	$sig(x, a, c) = \frac{1}{1 + \exp[-a(x - c)]}$	
	<p>c: The point at which the curved change its direction and this point has a degree of membership 0.5 ($\mu(c) = 0.5$).</p> <p>a: controls the slope at the intersection point $x = c$.</p>	
S-Shape Membership Function	$S\text{-Shape}(x; a, b, c, d) = \begin{cases} 0 & x \leq a \\ 2 \left(\frac{x-a}{a-b} \right)^2 & a \leq x \leq \left(\frac{a+b}{2} \right) \\ 1 - 2 \left(\frac{x-b}{b-a} \right)^2 & \left(\frac{a+b}{2} \right) \leq x \leq b \end{cases}$	
	<p>a, b: x- coordinates</p>	

4.1.8. Fuzzy Set Operations

Fuzzy sets have three fundamental operations similar to classical sets. These are listed with their equations below. Fuzzy set A is μ_A and fuzzy set B is μ_B .

- “Union” of the fuzzy set is defined by equation 4.7.

$$\mu_{A \cup B} = \max(\mu_A, \mu_B) \quad (4.7)$$

- “Intersections” of the fuzzy set is defined by equation 4.8.

$$\mu_{A \cap B} = \min(\mu_A, \mu_B) \quad (4.8)$$

- “Complement” of the fuzzy set is defined by equation 4.9.

$$\mu_{\bar{B}} = 1 - \mu_B \quad (4.9)$$

4.1.9. Linguistic Variables

Variables often have numerical value but these could be named as a linguistic variable if the variable has an oral statement. At this point, the difference in fuzzy set theory is visible. Classical set logic has numerical variables. But fuzzy set logic permits oral variables as well. These oral variables are in every area of daily life. Linguistic variables can be words, phrases or sentences.

4.1.10. Fuzzification

Fuzzification is the process of determining the membership degree of input data by using membership functions. Converting numerical variables to linguistic variables is called fuzzification. Fuzzy information is transformed into a linguistic variable by using membership functions.

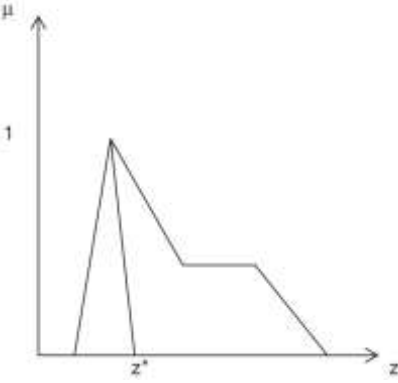
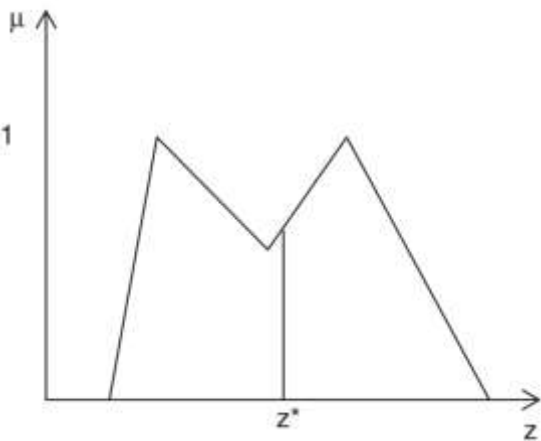
4.1.11. Defuzzification

Operations with fuzzy data sets will give fuzzy result sets and these results must be defuzzified. Certain methods can be used for defuzzification. Some of these methods are given below. (Ross, 2010)

- Max-membership principle
- Centroid method
- Weighted average method
- Mean–max membership
- Centre of sums
- Centre of largest area
- First of maxima or last of maxima

In the Table 4.2, types of defuzzifications methods are shown as expression and graphics. (Ross, 2010)

Table 4.2. Types of defuzzification methods (Ross, 2010)

Defuzzification Methods	Expression	Graphic
Max-membership principle	$\mu_{\tilde{C}}(z^*) \geq \mu_{\tilde{C}}(z) \text{ for all } z \in \mathfrak{Z}.$	
Centroid method	$z^* = \int \frac{\mu_{\tilde{C}}(z) z dz}{\int \mu_{\tilde{C}}(z) dz},$	

<p>Weighted average method</p>	$z^* = \frac{\sum \mu_{C_i}(\bar{z}) \bar{z}}{\sum \mu_{C_i}(\bar{z})}$	
<p>Mean-max membership</p>	$z^* = \frac{a + b}{2}$	
<p>Centre of sums</p>	$z^* = \frac{\int_2 z \sum_{k=1}^n \mu_{C_k}(z) dz}{\int_2 \sum_{k=1}^n \mu_{C_k}(z) dz}$	
<p>Center of largest area</p>	$z^* = \frac{\int \mu_{C_m}(\bar{z}) \bar{z} dz}{\int \mu_{C_m}(\bar{z}) dz}$	
<p>First of maxima or last of maxima</p>	<p>First of Maxima</p> $z^* = \inf_{z \in \bar{z}} \left\{ z \in \bar{z} / \mu_{C_k}(z) = \text{hgt}(C_k) \right\}$ <p>Last of Maxima</p> $z^* = \sup_{z \in \bar{z}} \left\{ z \in \bar{z} / \mu_{C_k}(z) = \text{hgt}(C_k) \right\}$	

4.2. Fine-Kinney Risk Assessment Method

Kinney or also known as Fine-Kinney method is a risk assessment method developed in 1976 by G.F. Kinney and A.D. Wiruth in their “Practical Risk Analysis for Safety Management” paper (Kinney & Wiruth, 1976). It is easy to use. Title of the published paper referred to ease-of-use. Fine-Kinney method enables quantitative risk assessment. Three parameters are used in this method. These are:

- L (Likelihood): Injury possibility when exposed to a dangerous event
- F (Frequency): Frequency to exposure to a dangerous event
- C (Consequence): Measurement of arising damage

R (Risk Score) in Fine-Kinney method is obtained by multiplying values of L, F and C. It is defined by equation 4.10 below.

$$R = L \times F \times C \tag{4.10}$$

The calculated R value should be targeted to be as low as possible. Because the decrease in risk score, also means that the risk of cyber attack decreases. Obtained score is assessed based in the Table 4.3. Furthermore, the reader is given a color code consisting of green, blue, yellow, orange and red so that they can immediately detect these risks visually.

Table 4.3. Risk scores and action plan as per Fine-Kinney

(Birgören, 2017; Kinney & Wiruth, 1976)

Risk Score	Risk Level	Action for Risk	Colour Code
$R < 20$	Risk	Perhaps acceptable	
$20 \leq R < 70$	Possible risk	Attention indicated	
$70 \leq R < 200$	Substantial risk	Correction needed	
$200 \leq R \leq 400$	High risk	Immediate correction required	
$R > 400$	Very high risk	Consider discontinuing operation	

While scoring in risk assessment with Fine-Kinney method, it is important to correctly understand and assess likelihood and frequency concepts. Otherwise, the risk assessment result would be misleading. While getting expert opinion, Table 4.4 used for likelihood, Table 4.5 for frequency, and Table 4.6 for consequence. When calculating the risk score, the value corresponding to the selection of the expert is used. The values given are fixed and specific to the Fine-Kinney method.

Table 4.4. The table of likelihood (Kinney & Wiruth, 1976)

Likelihood (L)	Value
Might well be expected	10
Quite possible	6
Unusual but possible	3
Only remotely possible	1
Conceivable but very unlikely	0.5
Practically impossible	0.2
Virtually impossible	0.1

Table 4.5. The table of frequency (Kinney & Wiruth, 1976)

Frequency (F)	Value
Continuous (daily)	10
Frequently (weekly)	6
Occasional (monthly)	3
Unusual (yearly)	2
Rare (1 time per year)	1
Very rare (1 time every 10 years)	0.5

Table 4.6. The table of consequence (Kinney & Wiruth, 1976)

Consequence (C)	Value
Catastrophic (many fatalities, or $> \$10^7$ damage)	100
Disaster (few fatality, or $> \$10^6$ damage)	40
Very serious (fatality, or $> \$10^5$ damage)	15
Serious (serious injury, or $> \$10^4$ damage)	7
Important (disability, or $> \$10^3$ damage)	3
Noticeable (minor first aid accident, or $> \$10^2$ damage)	1

4.3. Implementation of Fuzzy Fine-Kinney Method

During the literature review, papers, theses, guidelines, books and news in English and Turkish language related to cybersecurity were identified. Then, these resources were analysed in detail, and resources in line with the thesis purposes were determined. Cyber incidents which were occurred on vessels, and methods of attack were examined regardless of the type of vessels. The analysis of these cyber incidents revealed that they could also be happened in tankers. Afterwards, the equipment located in the bridge, engine room and CCR which was proven to be cyber vulnerability as research, was identified. As a scenario, various cyber risks that may be encountered on tankers were added to the list obtained. At the end of this research, a risk table was created for the equipments found on the bridge, engine room and CCR on tankers. Subsequently, the table was categorized based on location and equipment, and Table 4.7 was prepared containing a total of 31 risks in nine equipment related categories.

Given this table, some issues are worth noting. GPS, ECDIS, AIS and ARPA-Radar, which are among the bridge navigation equipments, have been researched, and as a result of this research, many cybersecurity vulnerabilities have been identified in these devices. Among them, attacks on GPS were encountered in also real life and were reflected in the press. These attacks on GPS have been claimed to be state-sponsored, nevertheless, these claims have not been confirmed. Although the attack method was not elucidated, the steering gear of a container vessel was seized, and the ship was directed to the location designated by the attackers. Also, as a consequence of a research conducted by a private company, steering gear control manipulated. When research and news were examined, there was no cyber vulnerability affecting the engine room, except the steering gear. Since all computerized systems related to cargo management are located here, CCRs for tankers are crucial. Still, there is no research or case yet to show that they have a cyber vulnerability. However, due to the nature of computers, the systems here always carry a certain risk.

Table 4.7. The table of cyber risk areas on a tanker

No	Area	Equipment	Decription	Research	News	Scenario	
01	Bridge	GPS	Spoofing	(Bhatti & Humphreys, 2017)	(Goward, 2017)		
02			Jamming		(Saul, 2017)		
03		ECDIS	ECDIS is out of order because of blue screen.		(Lund et al., 2018)		
04			Modification of the map		(Dyryavyy, 2014)		
05			Seems wrong location on ECDIS		(Lund et al., 2018)		
06		AIS	Ship spoofing		(Balduzzi et al., 2014)		
07			AtoN spoofing		(Balduzzi et al., 2014)		
08			Collision spoofing		(Balduzzi et al., 2014)		
09			AIS-SART spoofing		(Balduzzi et al., 2014)		
10			Weather forecasting		(Balduzzi et al., 2014)		
11			Slot starvation		(Balduzzi et al., 2014)		
12			Frequency hopping		(Balduzzi et al., 2014)		
13			Timing attack		(Balduzzi et al., 2014)		
14			AIS hijacking		(Balduzzi et al., 2014)		
15		ARPA Radar	Eliminating radar targets		(Shefi, 2017)		
16	Engine Room	Alarm Console	Being out of order of alarm monitoring system			✓	
17			Seems wrong level in bunker level indication system				✓
18			Blocking of valve control system in bunker lines				✓
19			Blocking of valve control system in steam lines				✓
20			Seems wrong position of the valves on bunker system				✓
21			Seems wrong position of the valves on steam system				✓
22		Steering	Remote control of steering gear by the attackers				✓
23			Being out of control of the steering gear		(Shefi, 2017)	(Blake, 2017)	
24		Main Engine	Increase the load				✓
25			Reduce the load				✓
26	Shut-Down				✓		
27	Auxiliary Engine	Black-Out				✓	
28	Cargo Control Room	Cargo Management System	Being out of order of cargo alarm monitoring system			✓	
29			Seems wrong level in cargo level indication system			✓	
30			Blocking of cargo valve control system			✓	
31			Seems wrong position of the valves of steam lines on cargo lines.			✓	

Possible 31 risks with attack methods were identified in order to ask to the focus group which would be formed. There has not been expressed any methods for risks that are scenarios or have unknown attack method, are written as N/A. As shown in Table 4.8, a table was drawn containing the risks and attack methods categorized to be given to the focus group.

Table 4.8. Cyber risks with attack methods on a tanker

Risk No	Risk Definition	Method
Risks regarding GPS		
01	GPS spoofing	Spoofing via antenna
02	GPS jamming	Jamming via antenna
Risks regarding ECDIS		
03	ECDIS is out of order because of blue screen.	Malware infection
04	Modification of ECDIS map.	HTTP Attack
05	Seems wrong location on ECDIS	Malware infection
Risk regarding AIS		
06	Ship spoofing	Spoofing via antenna
07	AtoN spoofing	Spoofing via antenna
08	Collision spoofing	Spoofing via antenna
09	AIS-SART spoofing	Spoofing via antenna
10	Weather forecasting	Spoofing via antenna
11	Slot starvation	Spoofing via antenna
12	Frequency hopping	Spoofing via antenna
13	Timing attack	Spoofing via antenna
14	AIS hijacking	Spoofing via antenna
Risk regarding ARPA-Radar		
15	Elimination of a target and deleting from the screen.	Through RJ-45
Risks regarding Alarm Console in Engine Room		
16	Being out of order of alarm monitoring system	N/A
17	Seems wrong level in bunker level indication system	N/A
18	Blocking of valve remote control system in bunker lines.	N/A
19	Blocking of valve remote control system in steam lines.	N/A
20	Seems wrong position of the valves on bunker system.	N/A
Risks regarding Steering Gear		
21	Remote control of steering gear by the attackers	N/A
22	Being out of control of the steering gear	N/A
Risks regarding Main Engine		
23	Reducing the load	N/A
24	Increasing the load	N/A
25	Shut-Down of the main engine	N/A
Risks Regarding Auxiliary Engine		
26	Black-out	N/A
Risks regarding Cargo Management Systems		
27	Being out of order of cargo alarm monitoring system	N/A
28	Seems wrong level in cargo level indication system	N/A
29	Blocking of cargo valve remote control system	N/A
30	Seems wrong position of the valves on cargo lines.	N/A
31	Seems wrong position of the valves of steam lines on cargo lines.	N/A

A questionnaire consisting of these categorized vulnerabilities according to the Fine-Kinney risk assessment method was created. The likelihood, the frequency and the consequence of cyber risks in this questionnaire were asked to focus group before taking precaution. Focus group members were consisted of the following people.

- 1 DPA (Designated Person Ashore)
- 3 Fleet managers
- 1 Training superintendent
- 1 HSEQ (Health, Safety, Environment, Quality) coordinator
- 1 IT manager

DPA is a graduate of maritime faculty, and has an oceangoing master competency. He worked on tankers and passenger ships. After working six years in a tanker operator as a fleet manager, he was promoted to the DPA in the same company. All fleet managers are graduates of maritime faculty, all have an oceangoing master competency, and all have worked as master in tankers. They have shore experience ranging from five - seven years. Training superintendent graduated from maritime vocational high school, also has oceangoing master competency. He worked on tankers as master. He has been working as training superintendent in a tanker operator for three years. HSEQ coordinator graduated from maritime faculty, and has oceangoing chief officer competency. He also worked on tankers as officer. He has four years of shore experience as well. The IT manager is a graduate of the vocational high school, and has been providing service to a tanker operator for both ships and the office for nine years. The questions were presented to the focus group for discussion, and they were asked to identify the likelihood, frequency and consequence of each defined risk. Results of the discussions presented to the group for final decision. As a result of the likelihood, frequency and consequence values of the focus group, the risk scores of the risks were identified in accordance with the Fine-Kinney risk assessment method. Furthermore, in line with the responses given, risk scores were re-identified through using Matlab software of Fuzzy Logic Designer. Then, the same questionnaire was asked to focus group again. However, this time they had to response the questions, assuming that technical protective measures in Table 4.9, and procedural protective measures in Table 4.10 were taken. Table 4.11 demonstrates which measures are used to reduce which risk. Focus group members re-identified likelihood, frequency and consequence values by assuming that the subject measures were taken. After that, these values were calculated based on both Fine-Kinney and Fuzzy Fine-Kinney method and risk scores were obtained.

Table 4.9. The technical protection cybersecurity measures towards defined risks

No	Description
1	Anti-virus software
2	VPN
3	Encryption
4	Back-up
5	Up-to-date softwares and operating systems
6	Wireless encryption
7	Isolated navigation system
8	Secured remote connection
9	Protection of interfaces, such as USB, RJ-45 and card reader etc.
10	Administrative privileges
11	Penetration test
12	Dedicated USB for license and chart data
13	Combined GPS and GLONASS

Table 4.10. The procedural protection cybersecurity measures towards defined risks

No	Description
1	Ensure cargo tank pressure/vacuum
2	Train the trainer
3	Ensure cargo line pressure
4	Check sounding / ullage
5	AIS-ARPA (Radar) association
6	Classify data
7	Manual position fix in ECDIS
8	Procedure of management of change
9	Create company policy
10	Equipment disposal
11	Develop a plan
12	Awareness
13	Password security
14	Physical security of critical hardware
15	Assign a responsible person
16	Social engineering
17	Remote access
18	Key performance indicator
19	Phishing and spear phishing
20	Develop a risk assessment
21	URL or web content filtering
22	Prepare an inventory list
23	Participate the vetting programmes
24	Keep a proper lookout

Table 4.11. The protection measures against defined cyber risks

Risk No	Risk Definition	Technical Protection Measures	Procedural Protection Measures
Risks regarding GPS			
01	GPS spoofing	7, 13	2, 11, 12, 15, 18, 20, 23, 24
02	GPS jamming	7	2, 11, 12, 15, 18, 20, 23
Risks regarding ECDIS			
03	ECDIS is out of order because of blue screen.	1, 4, 5, 7, 8, 9, 10, 11, 12	2, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23
04	Modification of ECDIS map	5, 4, 7, 8, 9, 10, 11, 12	2, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23, 24
05	Seems wrong location on ECDIS	5, 4, 7, 8, 9, 10, 11, 12	2, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23, 24
Risk regarding AIS			
06	Ship spoofing	7	2, 11, 12, 15, 18, 20, 23, 24
07	AtoN spoofing	7	2, 11, 12, 15, 18, 20, 23, 24
08	Collision spoofing	7	2, 11, 12, 15, 18, 20, 23, 24
09	AIS-SART spoofing	7	2, 11, 12, 15, 18, 20, 23
10	Weather forecasting	7	2, 11, 12, 15, 18, 20, 23
11	Slot starvation	7	2, 11, 12, 15, 18, 20, 23
12	Frequency hopping	7	2, 11, 12, 15, 18, 20, 23
13	Timing attack	7	2, 11, 12, 15, 18, 20, 23
14	AIS hijacking	7	2, 11, 12, 15, 18, 20, 23
Risk regarding ARPA-Radar			
15	Elimination of a target and deleting from the screen	1, 7, 11	2, 5, 9, 11, 12, 14, 15, 18, 20, 23, 24
Risks regarding Alarm Console in Engine Room			
16	Being out of order of alarm monitoring system	1, 2, 4, 5, 8, 9, 10, 11	2, 4, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23
17	Seems wrong level in bunker level indication system	1, 2, 4, 5, 8, 9, 10, 11	2, 4, 9, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23
18	Blocking of valve remote control system in bunker lines	1, 2, 4, 5, 8, 9, 10, 11	2, 4, 9, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23
19	Blocking of valve remote control system in steam lines	1, 2, 4, 5, 8, 9, 10, 11	2, 4, 9, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23
20	Seems wrong position of the valves on bunker system	1, 2, 4, 5, 8, 9, 10, 11	2, 4, 9, 11, 12, 13, 14, 15, 17, 18, 20, 22, 23
Risks regarding Steering Gear			
21	Remote control of steering gear by the attackers	1, 2, 9, 11	2, 11, 12, 14, 15, 17, 18, 20, 23
22	Being out of control of the steering gear	1, 2, 9, 11	2, 11, 12, 14, 15, 17, 18, 20, 23
Risks regarding Main Engine			
23	Reducing the load	1, 4, 9, 11	2, 8, 11, 12, 13, 14, 15, 16, 17, 18, 20, 23
24	Increasing the load	1, 4, 9, 11	2, 8, 11, 12, 13, 14, 15, 16, 17, 18, 20, 23
25	Shut-down of the main engine	1, 4, 9, 11	2, 8, 11, 12, 13, 14, 15, 16, 17, 18, 20, 23
Risks Regarding Auxiliary Engine			
26	Black-out	1, 9, 11	2, 8, 11, 12, 14, 15, 16, 17, 18, 20, 23
Risks regarding Cargo Management Systems			
27	Being out of order of cargo alarm monitoring system	1, 2, 3, 4, 5, 6, 8, 9, 10, 11	1, 2, 3, 6, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 21, 22, 23
28	Seems wrong level in cargo level indication system	1, 2, 3, 4, 5, 6, 8, 9, 10, 11	2, 4, 9, 6, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23
29	Blocking of cargo valve remote control system	1, 2, 3, 4, 5, 6, 8, 9, 10, 11	2, 4, 6, 9, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23
30	Seems wrong position of the valves on cargo lines	1, 2, 3, 4, 5, 6, 8, 9, 10, 11	2, 4, 6, 9, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23
31	Seems wrong position of the valves of steam lines on cargo lines	1, 2, 3, 4, 5, 6, 8, 9, 10, 11	2, 4, 6, 9, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23

4.3.1. Application of the Model in Matlab

In order to study fuzzy logic on MATLAB (Mathworks, 2019) 2019b, Fuzzy Logic Designer application must first be installed. After that, as shown in Figure 4.2, the subject application is run using the "fuzzy" command on the command window. Although it is a practical method to gain access through the command window, as an alternative method, the subject application can be run by clicking the Fuzzy Logic Designer button under the APPS menu.

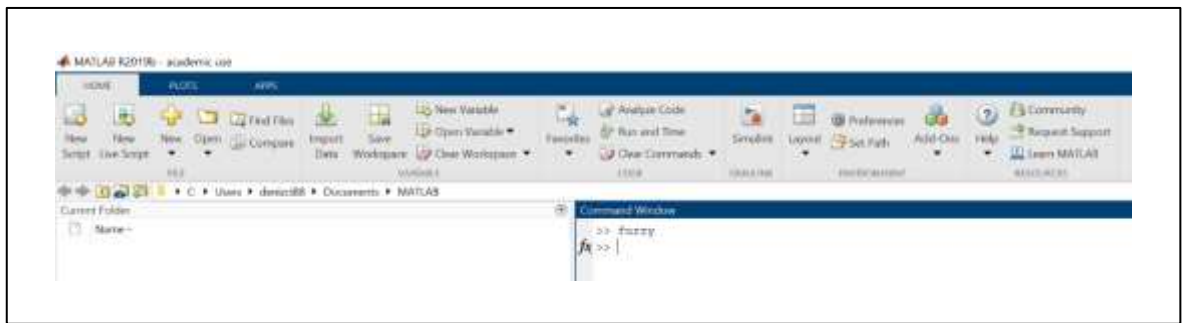


Figure 4.2. Command window of Matlab

When the designer is first launched, a simple model consisting of an input and output appears, as shown in Figure 4.3. There are two types of FIS (Fuzzy Inference System), Mamdani and Sugeno. In the opened model, Mamdani type is selected by default, but it is also possible to switch to Sugeno type. The primary reason among two methods lies in the consequent of fuzzy rules. Mamdani fuzzy systems use fuzzy sets as rule consequent, however Sugeno fuzzy uses linear functions of input variables as rule consequent (Sivanandam, Sumathi, & Deepa, 2007). In this study, Mamdani type as FIS is preferred.

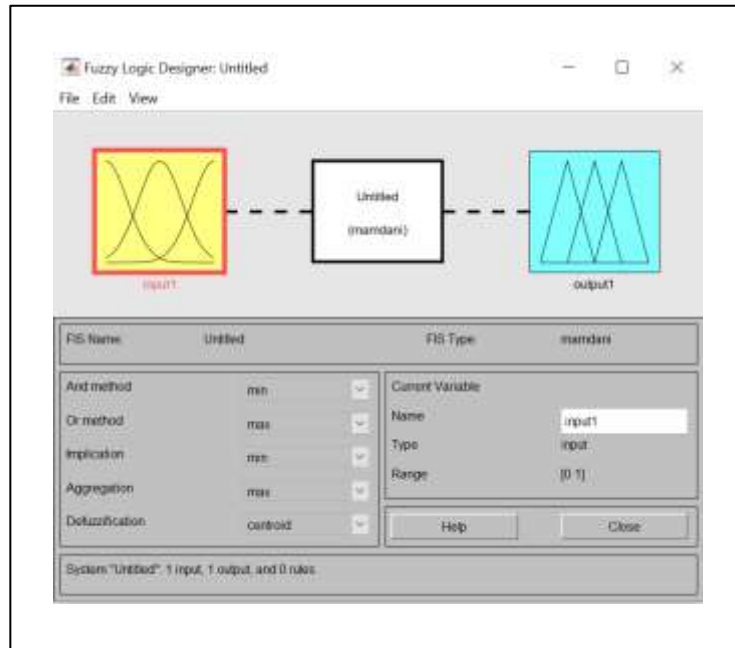


Figure 4.3. Matlab fuzzy inference system

Three inputs as “likelihood”, “frequency”, “consequence”, and an output as “Risk Score” are created in the FIS. “Likelihood” is named as “Olasılık”, “Frequency” is named as “Frekans”, “Consequence” is named as “Şiddet”, and “Risk Score” is named as “Risk” in the FIS. Inputs and output in FIS are shown at the Figure 4.4. below. Created inputs and outputs are also named FIS variables. Centroid was determined as defuzzification method.

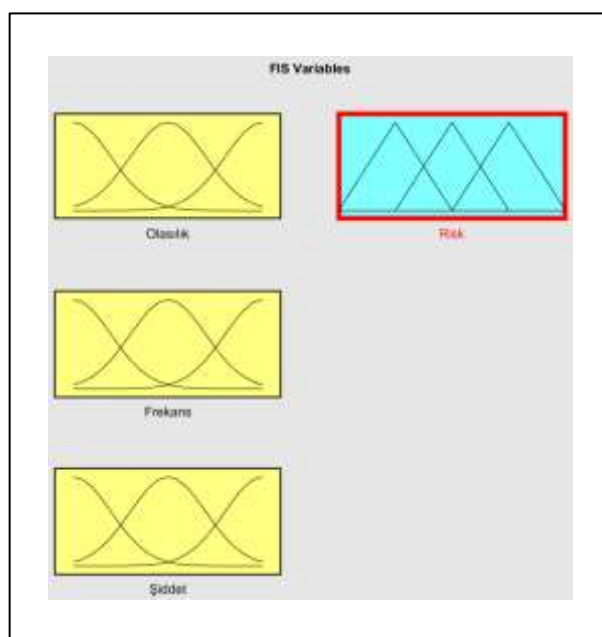


Figure 4.4. FIS variables

4.3.2. Defining of Membership Functions

As demonstrated in Figure 4.5, clicking on each variable created will determine the membership function that applies to the variable. In this study, triangular membership function is preferred for all variables because of ease of use.

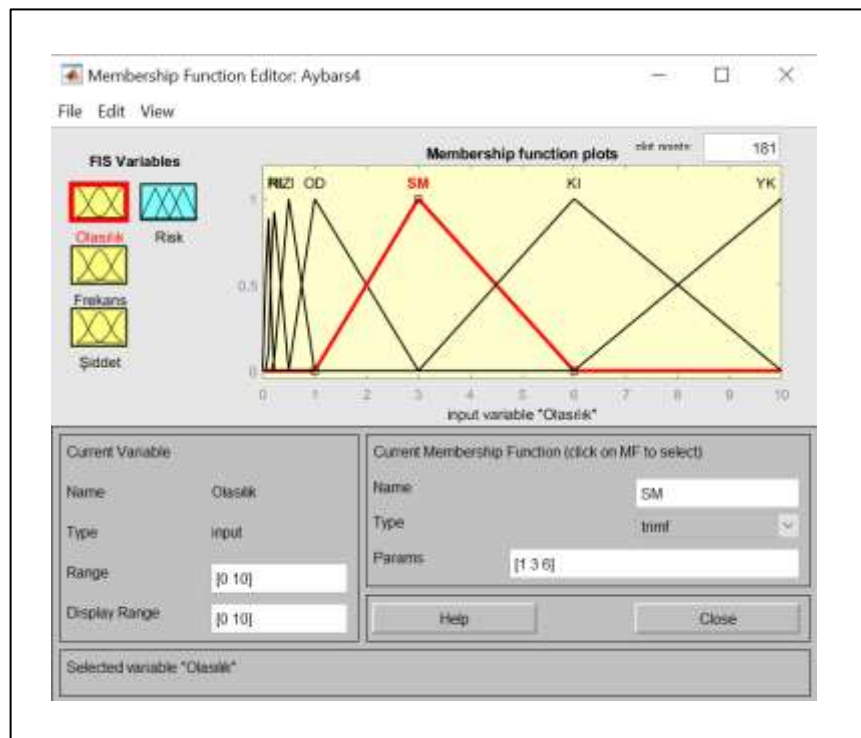


Figure 4.5. Defining of membership function

In the opened window, “range” and “display range” fields are entered the evaluation ranges that will enable the determination of the risk score. Likelihood and frequency are assessed between 0 and 10 values, and consequence is assessed between 0 and 100 values as per Fine-Kinney method. In the "Params" field, the values in the "params" column shown in Table 4.12, Table 4.13, Table 4.14 and Table 4.15 are entered in accordance with the variable. These values are given for triangular membership and are fixed (Sivanandam et al., 2007). Instead of typing in a long way, “name” fields are given simple abbreviations. Again, the expressions in the “name” column shown in Table 4.12, Table 4.13, Table 4.14 and Table 4.15 are used.

Table 4.12. The name and params for likelihood (L)

Likelihood (L)	Name	Params
Might well be expected	YK	(6, 10, 10)
Quite possible	KI	(3, 6, 10)
Unusual but possible	SM	(1, 3, 6)
Only remotely possible	OD	(0.5, 1, 3)
Conceivable but very unlikely	ZI	(0.2, 0.5, 1)
Practically impossible	PI	(0.1, 0.2, 0.5)
Virtually impossible	NI	(0, 0.1, 0.2)

Table 4.13. The name and params for frequency (F)

Frequency (F)	Name	Params
Continuous (Daily)	SUR	(6, 10, 10)
Frequently (Weekly)	SIK	(3, 6, 10)
Occasional (Monthly)	AS	(2, 3, 6)
Unusual (Yearly)	N	(1, 2, 3)
Rare (1 time per year)	SEY	(0.5, 1, 2)
Very rare (1 time every 10 years)	OS	(0, 0.5, 1)

Table 4.14. The name and params for consequence (C)

Consequence (C)	Name	Params
Catastrophic (many fatalities, or $> \$10^7$ damage)	FAC	(40, 100, 100)
Disaster (few fatality, or $> \$10^6$ damage)	FEL	(15, 40, 100)
Very serious (fatality, or $> \$10^5$ damage)	C.CID	(7, 15, 40)
Serious (serious injury, or $> \$10^4$ damage)	CID	(3, 7, 15)
Important (disability, or $> \$10^3$ damage)	ON	(1, 3, 7)
Noticeable (minor first aid accident, or $> \$10^2$ damage)	FAR	(0, 1, 3)

Table 4.15. The name and params for risk score (R)

Risk Score (R)	Risk Level	Action for Risk	Name	Params
$R < 20$	Risk	Perhaps acceptable	KE	(0, 20, 70)
$20 \leq R < 70$	Possible risk	Attention indicated	OR	(20, 70, 200)
$70 \leq R < 200$	Substantial risk	Correction needed	ORDI	(70, 200, 300)
$200 \leq R \leq 400$	High risk	Immediate correction required	YR	(200, 300, 400)
$R > 400$	Very high risk	Consider discontinuing operation	CYR	(300, 400, 400)

Fuzzy diagrams which are calculated using the triangular membership function of likelihood, frequency, consequence inputs, and risk score outputs are shown in Figure 4.6, Figure 4.7, Figure 4.8 and Figure 4.9, respectively.

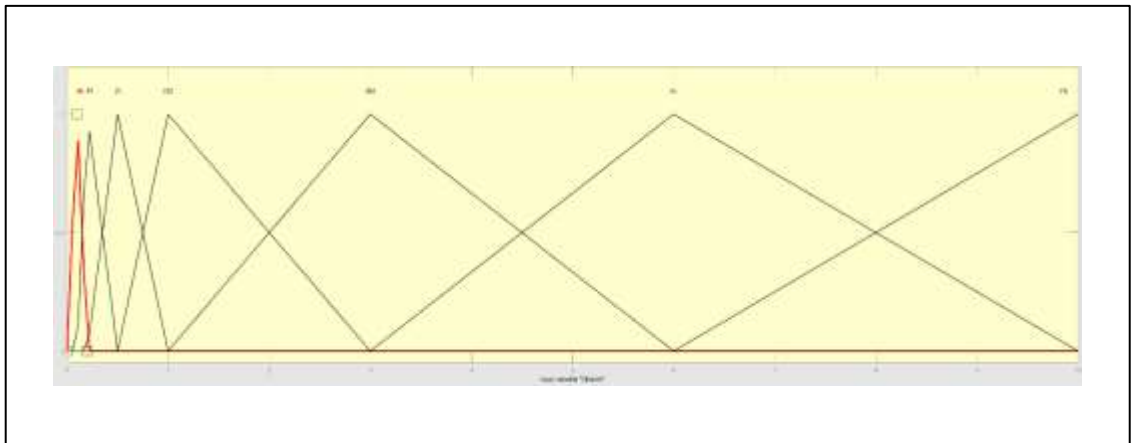


Figure 4.6. Fuzzy diagram for likelihood input

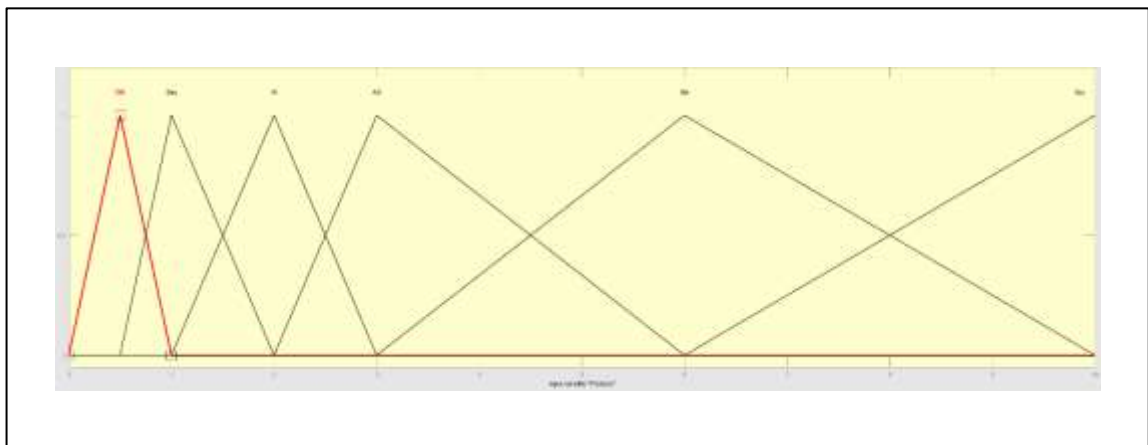


Figure 4.7. Fuzzy diagram for frequency input

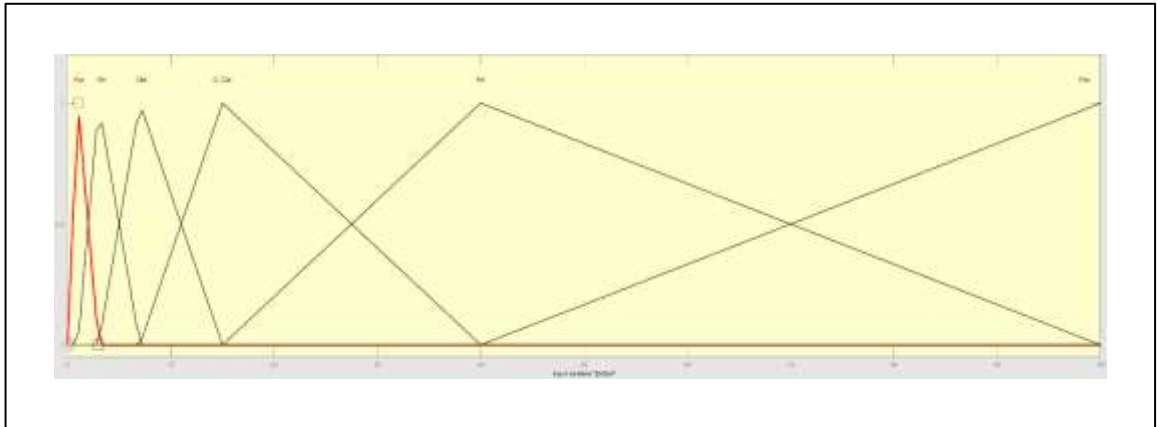


Figure 4.8. Fuzzy diagram for consequence input

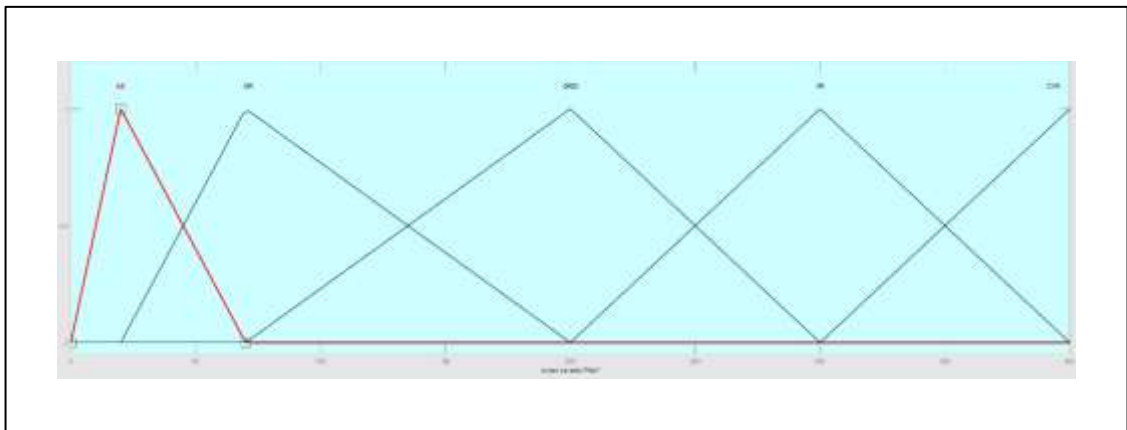


Figure 4.9. Fuzzy diagram for risk score output

4.3.3. Preparation of Fuzzy Rules

In Figure 4.10, rule editor is shown. A new rule can be created, an existing rule changed, or deleted through the rule editor. In order for the result to be correct, all rules must be entered correctly. A total of 252 rules were entered in the rule editor for this research. This is the highest rule number that can be added for the current study. Consequence and frequency have six linguistic variables, while likelihood has seven linguistic variables. The multiplication of these numbers gives the maximum number of rules that can be entered. Linguistic variables are linked by an “and” connection.

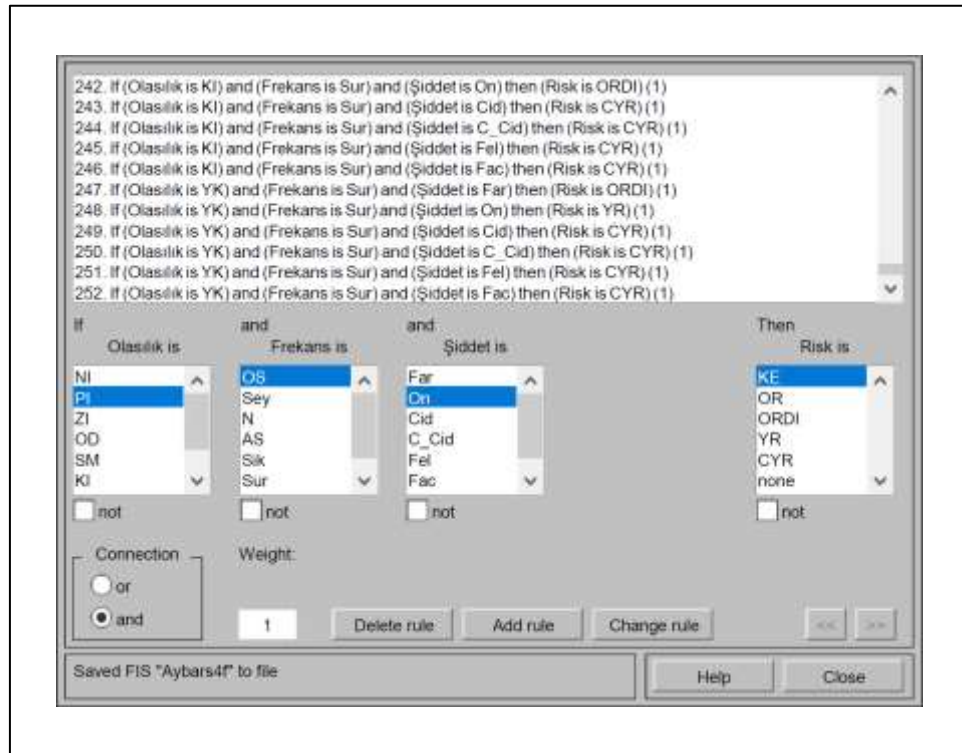


Figure 4.10. Rule editor of fuzzy logic designer

- Rule 1 as an example:

If (Olasılık is ZI) and (Frekans is N) and (Şiddet is C_Cid) then (Risk is KE)(1)

If (Probability is virtually impossible) and (Frequency is very rare) and (Consequence is noticeable) then (Risk is perhaps acceptable)

- Rule 250 as an example:

If (Olasılık is YK) and (Frekans is Sur) and (Şiddet is C_Cid) then (Risk is CYR)(1)

If (Probability is might well be expected) and (Frequency is continuous) and (Consequence is very serious) then (Risk is very high risk)

- Rule 251 as an example:

If (Olasılık is YK) and (Frekans is Sur) and (Şiddet is Fel) then (Risk is CYR)(1)

If (Probability is might well be expected) and (Frequency is continuous) and (Consequence is disaster) then (Risk is very high risk)

5. FINDINGS

After the focus group evaluations, the likelihood, frequency and consequence values of the risks are processed in the “Rule Viewer” on the Matlab fuzzy logic designer, and the risk scores are re-determined. For each determined risk, the focus group decision is entered in the input section shown in Figure 5.1 in the order of likelihood, frequency and consequence. Thus, new risk scores are obtained.

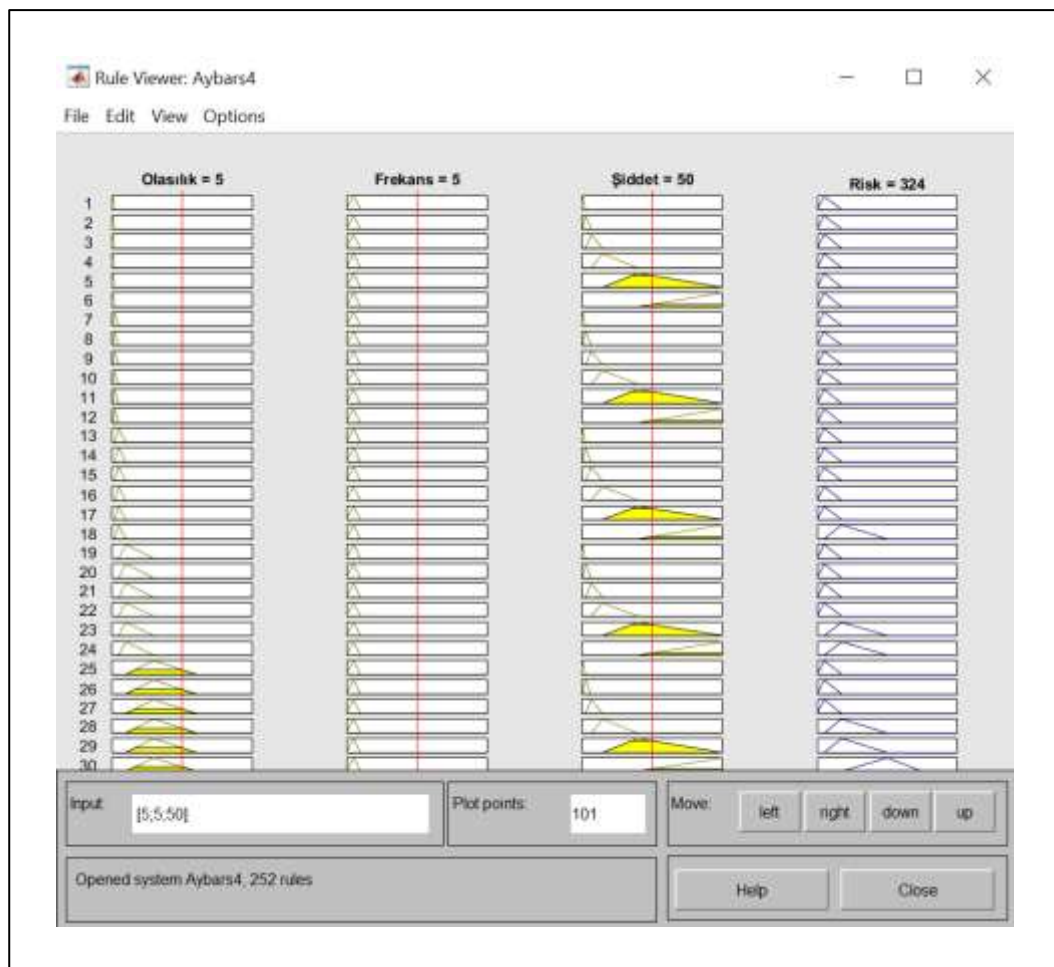


Figure 5.1. New risk scores as per the defined fuzzy rules

When the risks identified were evaluated by Fine-Kinney risk assessment method before taking measures, it was found that 17 risks were at the lowest risk level. In addition, 10 risks also have occurred at the “Possible Risk” level. One of the risks has been identified as “Substantial Risk”. The three risks also have identified as “High Risk”. The responses of the focus group were recalculated on Matlab by Fuzzy Fine-Kinney method. After the calculation, it was seen that the risk scores of all risks were increased except for the risk of “elimination of a target and deleting from the screen of ARPA-Radar”. The increased risk score did not change the risk level for many risks. The risks identified in the Fine-Kinney risk assessment method in “High Risk” level remained constant in the Fuzzy Fine-Kinney method as well. Also, all the risks that identified as “Risk” level have increased to the “Substantial risk” level when calculated in the Fuzzy Fine-Kinney method.

After the protection measures were taken, the risk group was re-assessed by the focus group, and the risk scores were calculated according to the Fine-Kinney method. Subsequently, 26 of the 31 risks listed were identified as “Risk”, four as "Possible Risk" and one as "Substantial risk". When these risk scores were calculated based on Fuzzy Fine-Kinney method, it was observed that the risk scores of all risks increased. Also the level of all risks except the risk of “Seems wrong location on ECDIS” were increased.

The risk assessment results before protection measures are taken by the Fine-Kinney method, are shown in Table 5.1. Table 5.2 demonstrates the risk assessment results after measures, are taken by the Fine-Kinney method. Also, the risk assessment shown in Table 5.3 and Table 5.4 was calculated using the Fuzzy Fine-Kinney method instead of Fine Kinney. The risk assessment results before measures are taken by the Fuzzy Fine-Kinney method, are shown in Table 5.3. Table 5.4 demonstrates the risk assessment results after measures, are taken by the Fuzzy Fine-Kinney method. The likelihood, frequency and consequence values that decreased after the measures were highlighted in yellow in Table 5.2 and Table 5.4. The numbers in column "No" in Tables 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 and 5.7 are fixed by the risks.

Table 5.1. Risk evaluation before taking protection as per Fine-Kinney method

No	Risk Definition	Method	L	F	C	Risk Score	Risk Level	Action for Risk
Risks regarding GPS								
01	GPS spoofing	Spoofing via antenna	1	1	40	40	Possible risk	Attention indicated
02	GPS jamming	Jamming via antenna	0.5	1	40	20	Possible risk	Attention indicated
Risks regarding ECDIS								
03	ECDIS is out of order because of blue screen	Malware infection	3	2	40	240	High risk	Immediate correction required
04	Modification of ECDIS map	HTTP Attack	0.5	1	100	50	Possible risk	Attention indicated
05	Seems wrong location on ECDIS	Malware infection	3	2	40	240	High risk	Immediate correction required
Risk regarding AIS								
06	Ship spoofing	Spoofing via antenna	3	0.5	7	10.5	Risk	Perhaps acceptable
07	AtoN spoofing	Spoofing via antenna	3	1	7	21	Possible risk	Attention indicated
08	Collision spoofing	Spoofing via antenna	1	0.5	40	20	Possible risk	Attention indicated
09	AIS-SART spoofing	Spoofing via antenna	1	0.5	1	0.5	Risk	Perhaps acceptable
10	Weather forecasting	Spoofing via antenna	0.1	0.5	1	0.05	Risk	Perhaps acceptable
11	Slot starvation	Spoofing via antenna	3	1	3	9	Risk	Perhaps acceptable
12	Frequency hopping	Spoofing via antenna	3	1	3	9	Risk	Perhaps acceptable
13	Timing attack	Spoofing via antenna	3	1	3	9	Risk	Perhaps acceptable
14	AIS hijacking	Spoofing via antenna	3	1	3	9	Risk	Perhaps acceptable
Risk regarding ARPA-Radar								
15	Elimination of a target and deleting from the screen	Through RJ-45	3	1	100	300	High risk	Immediate correction required
Risks regarding Alarm Console in Engine Room								
16	Being out of order of alarm monitoring system	N/A	1	0.5	7	3.5	Risk	Perhaps acceptable
17	Seems wrong level in bunker level indication system	N/A	1	0.5	15	7.5	Risk	Perhaps acceptable
18	Blocking of valve remote control system in bunker lines	Malware infection	3	1	40	120	Substantial risk	Correction needed
19	Blocking of valve remote control system in steam lines	Malware infection	3	1	15	45	Possible risk	Attention indicated
20	Seems wrong position of the valves on bunker system	N/A	1	0.5	40	20	Possible risk	Attention indicated
Risks regarding Steering Gear								
21	Remote control of steering gear by the attackers	Unknown	1	0.5	40	20	Possible risk	Attention indicated
22	Being out of control of the steering gear	N/A	3	0.5	40	60	Possible risk	Attention indicated
Risks regarding Main Engine								
23	Reducing the load	N/A	0.5	0.5	3	0.75	Risk	Perhaps acceptable
24	Increasing the load	N/A	0.5	0.5	15	3.75	Risk	Perhaps acceptable
25	Shut-Down of the main engine	N/A	0.5	0.5	40	10	Risk	Perhaps acceptable
Risks Regarding Auxiliary Engine								
26	Black-out	N/A	0.5	0.5	40	10	Risk	Perhaps acceptable
Risks regarding Cargo Management Systems								
27	Being out of order of cargo alarm monitoring system	N/A	0.5	0.5	40	10	Risk	Perhaps acceptable
28	Seems wrong level in cargo level indication system	N/A	0.5	0.5	40	10	Risk	Perhaps acceptable
29	Blocking of cargo valve remote control system	Malware infection	1	0.5	40	20	Possible risk	Attention indicated
30	Seems wrong position of the valves on cargo lines.	N/A	0.5	0.5	40	10	Risk	Perhaps acceptable
31	Seems wrong position of the valves of steam lines on cargo lines.	N/A	1	0.5	15	7.5	Risk	Perhaps acceptable

Table 5.2. Risk scores after taking protection as per Fine-Kinney method

No	Risk Definition	Method	L	F	C	Risk Score	Risk Level	Action for Risk
Risks regarding GPS								
01	GPS spoofing	Spoofing via antenna	0.5	1	40	20	Possible risk	Attention indicated
02	GPS jamming	Jamming via antenna	0.2	1	40	8	Risk	Perhaps acceptable
Risks regarding ECDIS								
03	ECDIS is out of order because of blue screen	Malware infection	0.5	2	7	7	Risk	Perhaps acceptable
04	Modification of ECDIS map	HTTP Attack	0.1	1	100	10	Risk	Perhaps acceptable
05	Seems wrong location on ECDIS	Malware infection	1	2	40	80	Substantial risk	Correction needed
Risk regarding AIS								
06	Ship spoofing	Spoofing via antenna	0.5	0.5	7	1.75	Risk	Perhaps acceptable
07	AtoN spoofing	Spoofing via antenna	0.5	1	7	3.5	Risk	Perhaps acceptable
08	Collision spoofing	Spoofing via antenna	0.5	0.5	15	3.75	Risk	Perhaps acceptable
09	AIS-SART spoofing	Spoofing via antenna	0.5	0.5	1	0.25	Risk	Perhaps acceptable
10	Weather forecasting	Spoofing via antenna	0.1	0.5	1	0.05	Risk	Perhaps acceptable
11	Slot starvation	Spoofing via antenna	1	1	3	3	Risk	Perhaps acceptable
12	Frequency hopping	Spoofing via antenna	1	1	3	3	Risk	Perhaps acceptable
13	Timing attack	Spoofing via antenna	1	1	3	3	Risk	Perhaps acceptable
14	AIS hijacking	Spoofing via antenna	1	1	3	3	Risk	Perhaps acceptable
Risk regarding ARPA-Radar								
15	Elimination of a target and deleting from the screen	Through RJ-45	0.2	0.5	100	10	Risk	Perhaps acceptable
Risks regarding Alarm Console in Engine Room								
16	Being out of order of alarm monitoring system	N/A	1	0.5	1	0.5	Risk	Perhaps acceptable
17	Seems wrong level in bunker level indication system	N/A	1	0.5	7	3.5	Risk	Perhaps acceptable
18	Blocking of valve remote control system in bunker lines	Malware infection	3	1	15	45	Possible risk	Attention indicated
19	Blocking of valve remote control system in steam lines	Malware infection	3	1	7	21	Possible risk	Attention indicated
20	Seems wrong position of the valves on bunker system	N/A	0.5	0.5	40	10	Risk	Perhaps acceptable
Risks regarding Steering Gear								
21	Remote control of steering gear by the attackers	Unknown	0.2	0.5	40	4	Risk	Perhaps acceptable
22	Being out of control of the steering gear	N/A	1	0.5	40	20	Possible risk	Attention indicated
Risks regarding Main Engine								
23	Reducing the load	N/A	0.2	0.5	3	0.3	Risk	Perhaps acceptable
24	Increasing the load	N/A	0.2	0.5	15	1.5	Risk	Perhaps acceptable
25	Shut-Down of the main engine	N/A	0.2	0.5	40	4	Risk	Perhaps acceptable
Risks Regarding Auxiliary Engine								
26	Black-out	N/A	0.5	0.5	15	3.75	Risk	Perhaps acceptable
Risks regarding Cargo Management Systems								
27	Being out of order of cargo alarm monitoring system	N/A	0.5	0.5	15	3.75	Risk	Perhaps acceptable
28	Seems wrong level in cargo level indication system	N/A	0.2	0.5	7	0.7	Risk	Perhaps acceptable
29	Blocking of cargo valve remote control system	Malware infection	0.5	0.5	15	3.75	Risk	Perhaps acceptable
30	Seems wrong position of the valves on cargo lines.	N/A	0.2	0.5	15	1.5	Risk	Perhaps acceptable
31	Seems wrong position of the valves of steam lines on cargo lines.	N/A	0.2	0.5	15	1.5	Risk	Perhaps acceptable

Table 5.3. Risk evaluation before taking protection as per Fuzzy Fine-Kinney method

No	Risk Definition	Method	L	F	C	Risk Score	Risk Level	Action for Risk
Risks regarding GPS								
01	GPS spoofing	Spoofing via antenna	1	1	40	96.7	Substantial risk	Correction needed
02	GPS jamming	Jamming via antenna	0.5	1	40	96.7	Substantial risk	Correction needed
Risks regarding ECDIS								
03	ECDIS is out of order because of blue screen	Malware infection	3	2	40	300	High risk	Immediate correction required
04	Modification of ECDIS map	HTTP Attack	0.5	1	100	96.7	Substantial risk	Correction needed
05	Seems wrong location on ECDIS	Malware infection	3	2	40	300	High risk	Immediate correction required
Risk regarding AIS								
06	Ship spoofing	Spoofing via antenna	3	0.5	7	30	Possible risk	Attention indicated
07	AtoN spoofing	Spoofing via antenna	3	1	7	96.7	Substantial risk	Correction needed
08	Collision spoofing	Spoofing via antenna	1	0.5	40	96.7	Substantial risk	Correction needed
09	AIS-SART spoofing	Spoofing via antenna	1	0.5	1	30	Possible risk	Attention indicated
10	Weather forecasting	Spoofing via antenna	0.1	0.5	1	30	Possible risk	Attention indicated
11	Slot starvation	Spoofing via antenna	3	1	3	30	Possible risk	Attention indicated
12	Frequency hopping	Spoofing via antenna	3	1	3	30	Possible risk	Attention indicated
13	Timing attack	Spoofing via antenna	3	1	3	30	Possible risk	Attention indicated
14	AIS hijacking	Spoofing via antenna	3	1	3	30	Possible risk	Attention indicated
Risk regarding ARPA-Radar								
15	Elimination of a target and deleting from the screen	Through RJ-45	3	1	100	300	High risk	Immediate correction required
Risks regarding Alarm Console in Engine Room								
16	Being out of order of alarm monitoring system	N/A	1	0.5	7	30	Possible risk	Attention indicated
17	Seems wrong level in bunker level indication system	N/A	1	0.5	15	30	Possible risk	Attention indicated
18	Blocking of valve remote control system in bunker lines	Malware infection	3	1	40	190	Substantial risk	Correction needed
19	Blocking of valve remote control system in steam lines	Malware infection	3	1	15	96.7	Substantial risk	Correction needed
20	Seems wrong position of the valves on bunker system	N/A	1	0.5	40	96.7	Substantial risk	Correction needed
Risks regarding Steering Gear								
21	Remote control of steering gear by the attackers	Unknown	1	0.5	40	96.7	Substantial risk	Correction needed
22	Being out of control of the steering gear	N/A	3	0.5	40	96.7	Substantial risk	Correction needed
Risks regarding Main Engine								
23	Reducing the load	N/A	0.5	0.5	3	30	Possible risk	Attention indicated
24	Increasing the load	N/A	0.5	0.5	15	30	Possible risk	Attention indicated
25	Shut-Down of the main engine	N/A	0.5	0.5	40	30	Possible risk	Attention indicated
Risks Regarding Auxiliary Engine								
26	Black-out	N/A	0.5	0.5	40	30	Possible risk	Attention indicated
Risks regarding Cargo Management Systems								
27	Being out of order of cargo alarm monitoring system	N/A	0.5	0.5	40	30	Possible risk	Attention indicated
28	Seems wrong level in cargo level indication system	N/A	0.5	0.5	40	30	Possible risk	Attention indicated
29	Blocking of cargo valve remote control system	Malware infection	1	0.5	40	96.7	Substantial risk	Correction needed
30	Seems wrong position of the valves on cargo lines.	N/A	0.5	0.5	40	30	Possible risk	Attention indicated
31	Seems wrong position of the valves of steam lines on cargo lines.	N/A	1	0.5	15	30	Possible risk	Attention indicated

Table 5.4. Risk scores after taking protection as per Fuzzy Fine-Kinney method

No	Risk Definition	Method	L	F	C	Risk Score	Risk Level	Action for Risk
Risks regarding GPS								
01	GPS spoofing	Spoofing via antenna	0.5	1	40	96.7	Substantial risk	Correction needed
02	GPS jamming	Jamming via antenna	0.2	1	40	30	Possible risk	Attention indicated
Risks regarding ECDIS								
03	ECDIS is out of order because of blue screen	Malware infection	0.5	2	7	30	Possible risk	Attention indicated
04	Modification of ECDIS map	HTTP Attack	0.1	1	100	30	Possible risk	Attention indicated
05	Seems wrong location on ECDIS	Malware infection	1	2	40	100	Substantial risk	Correction needed
Risk regarding AIS								
06	Ship spoofing	Spoofing via antenna	0.5	0.5	7	30	Possible risk	Attention indicated
07	AtoN spoofing	Spoofing via antenna	0.5	1	7	30	Possible risk	Attention indicated
08	Collision spoofing	Spoofing via antenna	0.5	0.5	15	30	Possible risk	Attention indicated
09	AIS-SART spoofing	Spoofing via antenna	0.5	0.5	1	30	Possible risk	Attention indicated
10	Weather forecasting	Spoofing via antenna	0.1	0.5	1	30	Possible risk	Attention indicated
11	Slot starvation	Spoofing via antenna	1	1	3	30	Possible risk	Attention indicated
12	Frequency hopping	Spoofing via antenna	1	1	3	30	Possible risk	Attention indicated
13	Timing attack	Spoofing via antenna	1	1	3	30	Possible risk	Attention indicated
14	AIS hijacking	Spoofing via antenna	1	1	3	30	Possible risk	Attention indicated
Risk regarding ARPA-Radar								
15	Elimination of a target and deleting from the screen	Through RJ-45	0.2	0.5	100	30	Possible risk	Attention indicated
Risks regarding Alarm Console in Engine Room								
16	Being out of order of alarm monitoring system	N/A	1	0.5	1	30	Possible risk	Attention indicated
17	Seems wrong level in bunker level indication system	N/A	1	0.5	7	30	Possible risk	Attention indicated
18	Blocking of valve remote control system in bunker lines	Malware infection	3	1	15	96.7	Substantial risk	Correction needed
19	Blocking of valve remote control system in steam lines	Malware infection	3	1	7	96.7	Substantial risk	Correction needed
20	Seems wrong position of the valves on bunker system	N/A	0.5	0.5	40	30	Possible risk	Attention indicated
Risks regarding Steering Gear								
21	Remote control of steering gear by the attackers	Unknown	0.2	0.5	40	30	Possible risk	Attention indicated
22	Being out of control of the steering gear	N/A	1	0.5	40	96.7	Substantial risk	Correction needed
Risks regarding Main Engine								
23	Reducing the load	N/A	0.2	0.5	3	30	Possible risk	Attention indicated
24	Increasing the load	N/A	0.2	0.5	15	30	Possible risk	Attention indicated
25	Shut-Down of the main engine	N/A	0.2	0.5	40	30	Possible risk	Attention indicated
Risks Regarding Auxiliary Engine								
26	Black-out	N/A	0.5	0.5	15	30	Possible risk	Attention indicated
Risks regarding Cargo Management Systems								
27	Being out of order of cargo alarm monitoring system	N/A	0.5	0.5	15	30	Possible risk	Attention indicated
28	Seems wrong level in cargo level indication system	N/A	0.2	0.5	7	30	Possible risk	Attention indicated
29	Blocking of cargo valve remote control system	Malware infection	0.5	0.5	15	30	Possible risk	Attention indicated
30	Seems wrong position of the valves on cargo lines.	N/A	0.2	0.5	15	30	Possible risk	Attention indicated
31	Seems wrong position of the valves of steam lines on cargo lines.	N/A	0.2	0.5	15	30	Possible risk	Attention indicated

Also, in Table 5.5, the values obtained after using the Fine-Kinney and Fuzzy Fine Kinney methods are given as a comparison table. After the protection measures taken by the Fine Kinney method, one of the risks occurred at the “Substantial risk”, four at the “Possible risk” and 26 at the “Risk” level. On the other hand, when evaluated with Fuzzy Fine-Kinney method, five of them were at "Substantial risk", and 26 of them were at "Possible Risk" level.

Table 5.5. The comparison table for Fine-Kinney and Fuzzy Fine-Kinney risk scores

		Before Protection Measures		After Protection Measures	
No	Risk Definition	Fine-Kinney Risk Score	Fuzzy Fine-Kinney Risk Score	Fine-Kinney Risk Score	Fuzzy Fine-Kinney Risk Score
Risks regarding GPS					
01	GPS spoofing	40	96.7	20	96.7
02	GPS jamming	20	96.7	8	30
Risks regarding ECDIS					
03	ECDIS is out of order because of blue screen.	240	300	7	30
04	Modification of ECDIS map	50	96.7	10	30
05	Seems wrong location on ECDIS	240	300	80	100
Risk regarding AIS					
06	Ship spoofing	10.5	30	1.75	30
07	AtoN spoofing	21	96.7	3.5	30
08	Collision spoofing	20	96.7	3.75	30
09	AIS-SART spoofing	0.5	30	0.25	30
10	Weather forecasting	0.05	30	0.05	30
11	Slot starvation	9	30	3	30
12	Frequency hopping	9	30	3	30
13	Timing attack	9	30	3	30
14	AIS hijacking	9	30	3	30
Risk regarding ARPA-Radar					
15	Elimination of a target and deleting from the screen.	300	300	10	30
Risks regarding Alarm Console in Engine Room					
16	Being out of order of alarm monitoring system	3.5	30	0.5	30
17	Seems wrong level in bunker level indication system	7.5	30	3.5	30
18	Blocking of valve remote control system in bunker lines.	120	190	45	96.7
19	Blocking of valve remote control system in steam lines.	45	96.7	21	96.7
20	Seems wrong position of the valves on bunker system.	20	96.7	10	30
Risks regarding Steering Gear					
21	Remote control of steering gear by the attackers	20	96.7	4	30
22	Being out of control of the steering gear	60	96.7	20	96.7
Risks regarding Main Engine					
23	Reducing the load	0.75	30	0.3	30
24	Increasing the load	3.75	30	1.5	30
25	Shut-down of the main engine	10	30	4	30
Risks Regarding Auxiliary Engine					
26	Black-out	10	30	3.75	30
Risks regarding Cargo Management Systems					
27	Being out of order of cargo alarm monitoring system	10	30	3.75	30
28	Seems wrong level in cargo level indication system	10	30	0.7	30
29	Blocking of cargo valve remote control system	20	96.7	3.75	30
30	Seems wrong position of the valves on cargo lines.	10	30	1.5	30
31	Seems wrong position of the valves of steam lines on cargo lines.	7.5	30	1.5	30

In Table 5.6, based on the Fuzzy Fine-Kinney method, the comparison of the results of “before protection measures” and “after protection measures” is given. Both of the score and level of the 21 of 31 risks remained constant except the risk of “Blocking of valve remote control system in bunker lines”. Although only the risk score of “Blocking of valve remote control system in bunker lines” decreased, the level of “Substantial risk” remained constant.

Table 5.6. Risks in same level in despite of protection measures

			Before Protection Measures	After Protection Measures
No	Risk Definition	Risk Level	Risk Score	Risk Score
Risks regarding GPS				
01	GPS spoofing	Substantial risk	96.7	96.7
Risk regarding AIS				
06	Ship spoofing	Possible risk	30	30
09	AIS-SART spoofing	Possible risk	30	30
10	Weather forecasting	Possible risk	30	30
11	Slot starvation	Possible risk	30	30
12	Frequency hopping	Possible risk	30	30
13	Timing attack	Possible risk	30	30
14	AIS hijacking	Possible risk	30	30
Risks regarding Alarm Console in Engine Room				
16	Being out of order of alarm monitoring system	Possible risk	30	30
17	Seems wrong level in bunker level indication system	Possible risk	30	30
18	Blocking of valve remote control system in bunker lines.	Substantial risk	190	96.7
19	Blocking of valve remote control system in steam lines.	Substantial risk	96.7	96.7
Risks regarding Steering Gear				
22	Being out of control of the steering gear	Substantial risk	96.7	96.7
Risks regarding Main Engine				
23	Reducing the load	Possible risk	30	30
24	Increasing the load	Possible risk	30	30
25	Shut-down of the main engine	Possible risk	30	30
Risks Regarding Auxiliary Engine				
26	Black-out	Possible risk	30	30
Risks regarding Cargo Management Systems				
27	Being out of order of cargo alarm monitoring system	Possible risk	30	30
28	Seems wrong level in cargo level indication system	Possible risk	30	30
30	Seems wrong position of the valves on cargo lines.	Possible risk	30	30
31	Seems wrong position of the valves of steam lines on cargo lines.	Possible risk	30	30

Table 5.7 shows the comparison of the results of “before protection measures” and “after protection measures” based on Fuzzy Fine-Kinney method. Both the score and the level of 10 of 31 risks decreased. The risks of “ECDIS is out of order because of blue screen” and “Elimination of a target and deleting from the screen” were decreased by two levels. For other eight risks, the risks were decreased by one level.

Table 5.7. Mitigated risk level difference after protection measures

No	Risk Definition	Before Protection Measures		After Protection Measures		Mitigated Risk Difference
		Risk Level	Risk Score	Risk Level	Risk Score	
Risks regarding GPS						
02	GPS jamming	Substantial risk	96.7	Possible risk	30	1
Risks regarding ECDIS						
03	ECDIS is out of order because of blue screen.	High risk	300	Possible risk	30	2
04	Modification of ECDIS map	Substantial risk	96.7	Possible risk	30	1
05	Seems wrong location on ECDIS	High risk	300	Substantial risk	100	1
Risk regarding AIS						
07	AtoN spoofing	Substantial risk	96.7	Possible risk	30	1
08	Collision spoofing	Substantial risk	96.7	Possible risk	30	1
Risk regarding ARPA-Radar						
15	Elimination of a target and deleting from the screen.	High risk	300	Possible risk	30	2
Risks regarding Alarm Console in Engine Room						
20	Seems wrong position of the valves on bunker system.	Substantial risk	96.7	Possible risk	30	1
Risks regarding Steering Gear						
21	Remote control of steering gear by the attackers	Substantial risk	96.7	Possible risk	30	1
Risks regarding Cargo Management Systems						
29	Blocking of cargo valve remote control system	Substantial risk	96.7	Possible risk	30	1

In Table 5.8, the risk scores that identified subsequent to the after protection measures with regard to the Fuzzy Fine-Kinney method are sorted from higher to lower. It is seen that the risk of “Seems wrong location on ECDIS” has the highest risk score based on this table. Five of them are at "Substantial risk", and 26 of them are at "Possible Risk" level. There is no risk at the “Risk”, “High Risk” and “Very High Risk” levels. Additional measures should be taken for risks of “Substantial Risk” level.

Table 5.8. Sort of risks as per Fuzzy Fine-Kinney method after protection measures

		As per Fuzzy Fine-Kinney method, after Protection Measures		
No	Risk Definition	Risk Score	Risk Level	Action for Risk
05	Seems wrong location on ECDIS	100	Substantial risk	Correction needed
01	GPS spoofing	96.7	Substantial risk	Correction needed
18	Blocking of valve remote control system in bunker lines.	96.7	Substantial risk	Correction needed
19	Blocking of valve remote control system in steam lines.	96.7	Substantial risk	Correction needed
22	Being out of control of the steering gear	96.7	Substantial risk	Correction needed
02	GPS jamming	30	Possible risk	Attention indicated
03	ECDIS is out of order because of blue screen.	30	Possible risk	Attention indicated
04	Modification of ECDIS map	30	Possible risk	Attention indicated
06	Ship spoofing	30	Possible risk	Attention indicated
07	AtoN spoofing	30	Possible risk	Attention indicated
08	Collision spoofing	30	Possible risk	Attention indicated
09	AIS-SART spoofing	30	Possible risk	Attention indicated
10	Weather forecasting	30	Possible risk	Attention indicated
11	Slot starvation	30	Possible risk	Attention indicated
12	Frequency hopping	30	Possible risk	Attention indicated
13	Timing attack	30	Possible risk	Attention indicated
14	AIS hijacking	30	Possible risk	Attention indicated
15	Elimination of a target and deleting from the screen.	30	Possible risk	Attention indicated
16	Being out of order of alarm monitoring system	30	Possible risk	Attention indicated
17	Seems wrong level in bunker level indication system	30	Possible risk	Attention indicated
20	Seems wrong position of the valves on bunker system.	30	Possible risk	Attention indicated
21	Remote control of steering gear by the attackers	30	Possible risk	Attention indicated
23	Reducing the load	30	Possible risk	Attention indicated
24	Increasing the load	30	Possible risk	Attention indicated
25	Shut-down of the main engine	30	Possible risk	Attention indicated
26	Black-out	30	Possible risk	Attention indicated
27	Being out of order of cargo alarm monitoring system	30	Possible risk	Attention indicated
28	Seems wrong level in cargo level indication system	30	Possible risk	Attention indicated
29	Blocking of cargo valve remote control system	30	Possible risk	Attention indicated
30	Seems wrong position of the valves on cargo lines.	30	Possible risk	Attention indicated
31	Seems wrong position of the valves of steam lines on cargo lines.	30	Possible risk	Attention indicated

During the preparation of this study, different findings were also identified besides the risk assessment. While reports of the last five year that contains 2014 – 2018 are examined, both the number of tankers and rate of them increased each year. Also, this growth can be also examined as deadweight tons change. Among tanker types, gas carriers are seen to increase more by rate every year compared to oil tankers and chemical tankers. Total cargo that is transported through the marine transport increases every year. Even though the amount of the crude oil, the petroleum product and the gasses transported by tankers has increased, its ratio in total cargo remains constant at around 29%.

The only mandatory regulation that studies directly maritime cybersecurity is ISM Code. As per ISPS Code, it's written that it is a must to have an SSA test on ship computer systems, but there is no direct statement on cyber threats. As required by ISM Code, all shipping companies must add a section of Maritime Cyber Risk Management to their company safety management systems, and this will be verified by the assessment that will be made. This assessment will be inspected in the first annual DoC verification following this date.

Non-mandatory vetting programs, such as TMSA, SIRE, CDI and RightShip have criterias on maritime cybersecurity and are polled between inspections. OCIMF that has developped TMSA and SIRE is a non-profit organization, and it is given "Consultative Status" by IMO. CDI is also a powerful non-profit organization. Both organizations aim to increase quality, safety and security standards of tanker operators. RightShip, as well, services vetting for drycargo vessels, but since RightShip is a private held company, it is not as powerful as OCIMF or CDI.

Old edition of "Guidelines on Cybersecurity Onboard Ships" is taken as references in the questions about cybersecurity in CDI Ship Inspection Report. This has been informed to CDI, and accepted that the reference was outdated.

6. CONCLUSION

In this thesis, it is aimed to identify the cyber risks that may occur in tankers and to develop measures to be taken against these risks. This study involves cyber risks including bridge, engine room and CCR. In nine categories, 31 cyber risks have been identified, and risk scores have been attempted to be reduced with 37 different barriers. Moreover, the impact of the implementation of these identified barriers on the levels of risks is also researched.

Risk assessment methods are divided into two groups as quantitative and qualitative. In the application of quantitative risk assessment methods, numerical calculations are used. Therefore, using quantitative risk assessment methods enable to easier interpretation of the results obtained. During the literature review, it is seen that there is not adequate data on cyber incidents in maritime sector. Hence, risk assessment was undertaken by taking expert opinions. However, the fuzzy logic approach had to be used in order to minimize the differences of interpretation in expert opinions. Fine-Kinney is a quantitative risk assessment method that allows practical calculation of risk scores. It is also possible to combine with fuzzy logic. Further, risks can be calculated quickly and simply by using Matlab. For these reasons, it is decided to use the Fuzzy Fine-Kinney risk assessment method to assess the detected cyber risks.

After the risk assessment of the focus group, it was seen that the fuzzy logic approach increased the risk score for all risks. This applies both before and after protection measures. The increase in the risk score has led to an increase in the risk levels for almost all risks as well. In the risk assessment carried out after the measures taken, it was observed that the level of 21 risks remained constant. The remaining 10 risk levels also has mitigated by one or two levels. As a result of the measures taken, 26 of the 31 identified risks were found to be at the “Possible Risk” level. It is sufficient to be careful against these risks.

On the other hand, despite the measures taken, it was observed that five of the risks remained at the “Substantial risk” level. Additional measures should be taken for these five risks. Despite the measures taken, the risk with the highest assessment score was found to be “Seems wrong location on ECDIS”. As a result of the research, it is seen that it is possible to fight against cyber threats at sea if necessary measures are taken.

The numbers of cyber risks on tankers and barriers may be increased. Risks may be re-assessed with different risk methods, such as Fault Tree Analysis, Event Tree Analysis, Failure Mode Effect Analysis, and the results of the risk assessment can be compared with each other. The study was conducted for tankers underway, but risks may also be assessed for different ship types, such as dry vessel, container vessel and RO-RO. A focus group consisting of seven people was formed in the study. The number of people in the group may be increased, or a different focus group may be set up with people with different backgrounds. Protection measures can be sorted by priority. Thus, among the measures, the most effective against cyber threats at sea can be identified.

Even though maritime cybersecurity is a new matter, due to cyber incidents experienced, it occupies the agenda of world maritime. Especially in autonomous and remote control ship projects, cybersecurity becomes prominent as one of the important question marks. Also, it doesn't seem to be possible for it to be out of the agenda in the future of the marine industry. For this reason, seafarers must be raised awareness about cyber attacks. In order to accomplish this, a training on cybersecurity must be counted into the STCW (Standards of Training, Certification and Watchkeeping) Convention. Both qualification of the trainer and the curriculum must be determined in detail. Also, the maritime cybersecurity is studied under the title of maritime security. Due to this reason, cybersecurity must be evaluated also within the ISPS Code. For now, the respect of cybersecurity in the marine is tried to be brought under control by the vetting organizations. IMO must have a more active part in this period.

REFERENCES

- ABS. (2016a). *Cybersecurity Implementation for the Marine and Offshore Industry* (Vol. 2). American Bureau of Shipping.
- ABS. (2016b). *Data Integrity for Marine and Offshore (Volume 3)*. American Bureau of Shipping.
- ABS. (2016c). *The Application of Cybersecurity Principles to Marine and Offshore Operations* (Vol. 1).
- Allianz. (2019). *Safety and Shipping Review*.
- Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A Security Evaluation of AIS Automated Identification System.
- Bateman, T. (2013). Police Warning after Drug Traffickers' Cyber-Attack. Retrieved November 30, 2019, from <https://www.bbc.com/news/world-europe-24539417>
- Belmont, K. B. (2016). *MARITIME CYBERSECURITY: Cyber Cases in the Maritime Environment*.
- Bhatti, J., & Humphreys, T. E. (2014). Covert control of surface vessels via counterfeit civil GPS signals, 1–10.
- Bhatti, J., & Humphreys, T. E. (2017). Hostile Control of Ships via False GPS Signals : Demonstration and Detection. <https://doi.org/10.1002/navi.183>
- BIMCO. (2018). *The Guidelines on Cyber Security Onboard Ships* (3rd ed.).
- Birgören, B. (2017). Calculation Challenges and Solution Suggestions for Risk Factors in the Risk Analysis Method in the Fine Kinney Risk Analysis Method. *Uluslararası Muhendislik Arastırma ve Gelistirme Dergisi*, 9(1), 19–25. <https://doi.org/10.29137/umagd.346168>
- Blake, T. (2017). Hackers took 'full control' of container ship's navigation systems for 10 hours. Retrieved August 31, 2019, from <https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/>
- Bodeau, D. J., Graubart, R., & Fabius-Greene, J. (2010). Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels. IETT. <https://doi.org/10.1109/SocialCom.2010.170>

- Boyes, H., & Isbell, R. (2017). *Code of Practices Cyber Security for Ships*.
- Branch, T. A., & January, C. S. (2019). Threat Assessment The cyber threat against the Danish maritime sector, (January).
- Bruce, G., & Eyres, D. (2012). *Ship construction* (7th ed.). Elsevier Ltd.
- C-DAC. (2015). *Cyber Security Awareness Handbook*.
- C4ADS. (2019). *Above Us Only Stars*. C4ADS.
- CDI. (2019a). CDI Introduction. Retrieved August 31, 2019, from <https://www.cdi.org.uk/Introduction.aspx>
- CDI. (2019b). *CDI SIR 9.8.1*. CDI.
- CESG. (2015). *Common Cyber Attacks: Reducing The Impact*. National Cyber Security Centre.
- Chugh, A., Chaudhary, P., & Rizwan, M. (2015). Fuzzy Logic Approach for Short Term Solar Energy Forecasting.
- Cyber Keel. (2014). *Maritime Cyber Risks*.
- DNV-GL. (2016). *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*. DNV-GL.
- Dyryavy, Y. (2014). *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*. NCC Group.
- EC3. (2013). *Hackers deployed to facilitate drugs smuggling*.
- Eirik, A. (2003). Security vs Safety.
- Equasis. (2015). *World Merchant Fleet Statistics - 2014*.
- Equasis. (2016). *World Merchant Fleet Statistics - 2015*.
- Equasis. (2017). *World Merchant Fleet Statistics - 2016*.
- Equasis. (2018). *World Merchant Fleet Statistics - 2017*.
- Equasis. (2019a). Data providers. Retrieved November 30, 2019, from https://www.equasis.org/EquasisWeb/public/About?fs=About&P_ABOUT=Providers.html
- Equasis. (2019b). Overview. Retrieved November 30, 2019, from https://www.equasis.org/EquasisWeb/public/About?fs=HomePage&P_ABOUT=MainConcern.html
- Equasis. (2019c). *World Merchant Fleet Statistics - 2018*.
- Esage, A. (2018). British Shipping Company Clarksons Hacked. Retrieved November 30, 2019, from <https://www.securitynewspaper.com/2018/08/02/british-shipping->

- company-clarksons-hacked/
- Falah, Z. (2018). Types of Membership Function. Retrieved November 30, 2019, from www.uobabylon.edu.iq/eprints/pubdoc_11_6921_1712.docx
- Goward, D. (2017). Mass GPS Spoofing Attack in Black Sea? Retrieved August 31, 2019, from <https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea>
- Graham, L. (2017). Shipping industry vulnerable to cyber attacks and GPS jamming. Retrieved August 31, 2019, from <https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html>
- Grant, A., Williams, P., Ward, N., & Basker, S. (2014). GPS Jamming and the Impact on Maritime Navigation, (December). <https://doi.org/10.1017/S0373463308005213>
- Havold, J. I. (2010). Safety culture and safety management aboard tankers, *95*(5), 511–519. <https://doi.org/10.1016/j.res.2010.01.002>
- Humphreys, T. (2017). Ships fooled in GPS spoofing attack suggest Russian cyberweapon. Retrieved November 30, 2019, from <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/>
- Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., Hanlon, B. W. O., & Kintner, P. M. (2009). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.
- IMO. (1997). *IMO Resolution A.861(20)*.
- IMO. (2006). *IMO Resolution MSC.232(82)*.
- IMO. (2012). *ISPS Code* (2012th ed.).
- IMO. (2014a). *ISM Code* (2014th ed.).
- IMO. (2014b). *SOLAS Convention* (2014th ed.).
- IMO. (2017a). *IMO MSC-FAL.1/Circ.3*.
- IMO. (2017b). *MARPOL Convention* (2017th ed.).
- IMO. (2017c). *Resolution MSC.428 (98)*.
- International Organization for Standardization, & International Electrotechnical Commission. (2018). *ISO/IEC 27000:2018(en) Information technology - Security techniques - Information security management systems*.
- IRM. (2014). *Cyber Risk Executive Summary*. IRM.
- John, L. (2018). UK shipping biz Clarksons blames megahack on single point of pwnage. Retrieved November 30, 2019, from

- https://www.theregister.co.uk/2018/08/01/clarksons_breach_update/
- Joint Hull Committee. (2015). *Cyber Risk*. Joint Hull Committee.
- Jonathan, S., & Torbati, Y. (2012). Cyber Attack to Islamic Republic of Iran Shipping Lines. Retrieved November 30, 2019, from <https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022>
- Joseph, D., Drumhiller, N. K., & Roberts, F. S. (2017). Issues in Maritime Cyber Security. JWC International. (2017). Phish & Ships.
- Kaplan, E. D., & Hegarty, C. J. (2017). *Understanding GPS/GNSS* (3rd ed.).
- Karti, E. N. (2017). Vetting and TMSA: Role and Requirements in the Shipping Industry, (June).
- Kaya, H. (2018). *Akciğer Hastalıkları Teşhisinde Sınıflandırma ve Bulanık Mantık Yöntemlerinin Uygulanması*. Ankara University.
- Kinney, G. F., & Wiruth, A. D. (1976). Practical Risk Analysis for Safety Management.
- Kochetkova, K. (2015). Australian Customs and Border Protection Service Agency. Retrieved November 30, 2019, from <https://www.kaspersky.com/blog/maritime-cyber-security/8796/>
- Li, Y. (2003). *Addressing major maritime security issues of global, regional and national significances : law and policy implications in the context of China*.
- Lund, M. S., Hareide, O. S., & Jøsok, Ø. (2018). An Attack on an Integrated Navigation System. *Necessite*, 3(2), 149–163. <https://doi.org/10.21339/2464-353x.3.2.149>
- Maersk. (2017). Maersk News Release. Retrieved August 31, 2019, from <http://investor.maersk.com/news-releases/news-release-details/cyber-attack-update>
- Manoj, P. P., & Shah, A. P. (2014). Fuzzy Logic Methodology for Short Term Load Forecasting. *International Journal of Research in Engineering and Technology*.
- Maritime Executive. (2017). Ferry Builder Austal Hit by Cyberattack. Retrieved November 30, 2019, from <https://www.maritime-executive.com/article/ferry-builder-austal-hit-by-cyberattack>
- Mathworks. (2019). *Fuzzy Logic Toolbox: User's Guide (r2017b)*. Retrieved November 20, 2019 from https://www.mathworks.com/help/pdf_doc/fuzzy/fuzzy.pdf
- Mejia, M. Q. J. (2002). Defining Maritime Violence and Maritime Security.
- Moaiied, M. M., & Mosavi, M. R. (2016). Increasing accuracy of combined GPS and GLONASS positioning using fuzzy kalman filter. *Iranian Journal of Electrical and Electronic Engineering*, 12(1), 21–28. <https://doi.org/10.22068/IJEEE.12.1.21>

- Ngai, S. (2017). BW Group steps up cyber security after IT infringement. Retrieved November 30, 2019, from <https://safetyatsea.net/news/2017/bw-group-steps-up-cyber-security-after-it-infringement/>
- OCIMF. (2017). *TMSA 3*. OCIMF.
- OCIMF. (2018). *VIQ 7*. OCIMF.
- OCIMF. (2019). OCIMF. Retrieved November 30, 2019, from <https://www.ocimf.org/organisation/introduction.aspx>
- OCIMF, & CCNR. (2010). *International Safety Guide for Inland Navigation Tank-barges and Terminals* (1st ed.). OCIMF Central Commission for the Navigation of the Rhine.
- Paganini, P. (2019). After 1 Million of malware samples analyzed. Retrieved December 28, 2019, from After 1 Million of malware samples analyzed
- Raz, T., & Hillson, D. (2005). A Comparative Review of Risk Management Standards, 7(4), 53–66.
- Rightship. (2017). *Rightship Questionnaire*.
- Rishikesh Sahay, & Daniel Sepúlveda Estay. (2018). *Cyber Resilience for the Shipping Industry*. Technical University of Denmark.
- Ross, T. J. (2010). *Fuzzy Logic with Engineering Applications*. (3rd ed.). John Wiley & Sons. <https://doi.org/10.1002/9781119994374>
- Safety4Sea. (2018). Maersk Line: Surviving from a cyber attack. Retrieved November 30, 2019, from <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/>
- Sameer, C. M. (2017). BW Group's computer systems hacked; steps up cyber security. Retrieved November 30, 2019, from <https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/101317-shipping-bw-groups-computer-systems-hacked-steps-up-cyber-security>
- Saul, J. (2017). GPS Jamming off South Korean. Retrieved November 30, 2019, from <https://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT>
- Sead, F. (2017). Shipping giant Maersk reveals \$300 million cyber-attack loss. Retrieved December 28, 2019, from <https://www.itproportal.com/news/maersk-lost-300-million-due-to-notpetya/>
- Sen, R. (2016). Cyber and Information Threats to Seaports and Ships. In M. McNicholas (Ed.), *Maritime Security: An Introduction* (2nd ed., pp. 281–302). Elsevier Inc. <https://doi.org/10.1016/B978-0-12-803672-3.00009-1>

- Shao, Z., Teng-da Sun, Jia-cai Pan, & Xian-biao, J. (2007). Vessel Information Service System based on ECDIS and AIS, *2007*(1), 1678–1683.
- Sharples, P. (2018). How to improve crew welfare at sea. Retrieved December 28, 2019, from <https://safety4sea.com/cm-how-to-improve-crew-welfare-at-sea/>
- Shefi, A. (2017). Tests Show Ease of Hacking ECDIS, Radar and Machinery. Retrieved August 31, 2019, from <https://www.maritime-executive.com/article/tests-show-ease-of-hacking-eccdis-radar-and-machinery>
- Sin, B. (2013). Attack to Oil Rig Platform. Retrieved November 30, 2019, from <https://www.slashgear.com/offshore-oil-rigs-suffer-from-malware-attacks-24271125/>
- Sivanandam, S. N., Sumathi, S., & Deepa, S. N. (2007). *Introduction to fuzzy logic using MATLAB. Introduction to Fuzzy Logic using MATLAB*. <https://doi.org/10.1007/978-3-540-35781-0>
- Solmaz, M. S. (2012). *In the Context of the Maritime Security, Evaluation of the ISPS Code Port Security Implementations' Effectiveness and Turkey's Implementations*.
- Sophos. (2013). *The A-Z of Computer and Data Security Threats*. Sophos.
- Su, J., He, J., Cheng, P., & Chen, J. (2016). A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle. *IFAC-PapersOnLine*, *49*(22), 291–296. <https://doi.org/10.1016/j.ifacol.2016.10.412>
- The Local. (2014). State-sponsored hackers spied on Denmark. Retrieved November 30, 2019, from <https://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies>
- Transas. (2017). *Cyber Security Guideline*.
- Trend Micro. (2017). Ransomware. Retrieved December 28, 2019, from <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>
- Tung, L. (2018). Maerks Chairman. Retrieved November 30, 2019, from <https://www.cso.com.au/article/632622/maersk-took-just-10-days-install-4k-servers-45k-pcs-after-notpetya-attack/>
- Ulstein. (2019). Remote Connection. Retrieved November 30, 2019, from <https://ulstein.com/marine-automation>
- UNCTAD. (2015). *Review of Maritime Transport*. United Nations Publications.
- UNCTAD. (2016). *Review of Maritime Transport*. United Nations Publications.
- UNCTAD. (2017). *Review of Maritime Transport*. United Nations Publications.
- UNCTAD. (2018). *Review of Maritime Transport*. United Nations Publications.

- UNCTAD. (2019). *Review of Maritime Transport*. United Nations Publications.
- UpGuard. (2017). *The Non-Technical Guide to Cyber Risk*. UpGuard.
- UpGuard. (2019). 22 Types of Malware and How to Recognize Them. Retrieved December 28, 2019, from <https://www.upguard.com/blog/types-of-malware>
- Vistiaho, P. (2017). Maritime Cyber Security Incident Data Reporting for Autonomous Ships, (November).
- WMN. (2018a). COSCO Shipping Lines Falls Victim to Cyber Attack. Retrieved November 30, 2019, from <https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/>
- WMN. (2018b). Data Theft Affects Hundreds of Svitzer Australia's Employees. Retrieved November 30, 2019, from <https://worldmaritimenews.com/archives/247526/data-theft-affects-hundreds-of-svitzer-australias-employees/>
- Zain, S. (2013). Attack to Oil Rig. Retrieved November 30, 2019, from <https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php>

APPENDIXES

Appendix - A

Questionnaire and Options for Fine-Kinney Method

Risks	Methods
Risks regarding GPS	
Misleading the location of the GPS and transmitting incorrect location information to other integrated systems due to spoofing attack	Spoofing (Via antenna)
Due to jamming attack, giving a failure and not positioning of the GPS	Jamming (Via antenna)
Risks regarding ECDIS	
For the reason of the blue screen error, not using the ECDIS	Virus infection
Modification of ECDIS map	HTTP Attack (Physical access to ECDIS is required)
Misdirection of the location on ECDIS	Virus infection
Risk regarding Cargo Management System	
The cargo alarm monitoring system not raising the alarm	Scenario
Faultiness of the cargo level indication system	Scenario
Inhibiting the operation of the valve remote control system for cargo lines	Virus infection via USB Stick
Incorrect indication of the positions of the valves on the valve remote control system of cargo lines	Scenario
Incorrect indication of positions of steam valves of cargo circuits	Scenario
Risks regarding Steering Gear	
Remote control of the steering gear by attackers	There is no information about the method, but it has occurred.
Not using the steering gear in any command	Scenario
Risks regarding Alarm Console in Engine Room	
Silencing the alarm monitoring system	Scenario
Faultiness of the indication of the level in the bunker tanks	Scenario
Inhibiting the operation of the valve control system in the bunker system	Virus infection via USB Stick
Inhibiting the operation of the valve control system in the steam system	Virus infection via USB Stick
Incorrect indication of valve positions in the bunker system	Scenario
Incorrect indication of valve positions by the valve control system in steam system	Scenario

Risk regarding AIS	
<p>Ship Spoofing: A fake ship is being created. This fake ship can also have flag, speed, position, course, destination, transported cargo, ship type, dimension, call sign and MMSI information just like the real ship. Further, it can provide the situations of the ship, such as underway, moored and anchored. Many different scenarios can be described upon this attack. To illustrate, the scenario of a ship carrying nuclear substances in the territorial waters of a country where nuclear is not allowed can be defined.</p>	Spoofing (Via antenna)
<p>AtoN Spoofing: “AtoN” is an abbreviation meaning “Aids-to-Navigation”. It warns seafarers about the dangers around them, such as low tides, rock outcropping and shoals. Through fake signals, a route change may be required.</p>	Spoofing (Via antenna)
<p>Collision Spoofing: One of the reasons AIS is installed is that it reduces the collision risk of ships. “Closest Point of Approach (CPA)” is an AIS feature that makes this possible. A distance is identified when using this feature. If any vessel is within the limits of this distance, the system alarms. Through fake signals, a route change may be required.</p>	Spoofing (Via antenna)
<p>AIS-SART Spoofing: Through a SART alarm by the AIS, the crew may cause unnecessary involvement in the Search and Rescue (SAR) operation.</p>	Spoofing (Via antenna)
<p>Weather Forecasting: AIS also provides environmental information, such as current and climate condition. It may force crew to change course by creating incorrect weather information.</p>	Spoofing (Via antenna)
<p>Slot Starvation: This attack affects all ships and AIS gateways within coverage area and prevents the use of the AIS system in this area.</p>	Spoofing (Via antenna)
<p>Frequency Hopping: The attacker introduces himself as a maritime authority, and forces the AIS transponder to change the operating frequency. In accordance with the operating system, AIS adapts itself to this frequency. Thus, the AIS becomes unusable.</p>	Spoofing (Via antenna)
<p>Timing Attack: The attacker forces the AIS transponder to delay transmission time. In order to accomplish this, the attacker repeatedly sends the necessary command. This prevents the AIS transponder from transmitting its signals, also make the AIS unusable.</p>	Spoofing (Via antenna)
<p>AIS Hijacking: There are two variations of the AIS Hijacking method. In one of these variations, the attacker listens to the AIS signals from the ship and changes them. In the other variation, the attacker suppresses the actual signals by emitting false signals that are stronger than the actual AIS signals. In both variations, the receiving station receives messages modified by the attacker instead of the original AIS messages.</p>	Spoofing (Via antenna)

Risks regarding Main Engine	
Reducing the load	Scenario
Increasing the load	Scenario
Stopping the main engine during the operation	Scenario
Risk regarding Auxiliary Engine	
Black-out situation on a ship due to failure of power generators	Scenario
Risk regarding ARPA-Radar	
Removing the target on the ARPA radar and deleting it from the screen	Via ethernet port

Options for Likelihood

- Might well be expected
- Quite possible
- Unusual but possible
- Only remotely possible
- Conceivable but very unlikely
- Practically impossible
- Virtually impossible

Options for Frequency

- Continuous (Daily)
- Frequently (Weekly)
- Occasional (Monthly)
- Unusual (Yearly)
- Rare (1 time per year)
- Very rare (1 time every 10 years)

Options for Consequence

- Catastrophic (many fatalities, or $> \$10^7$ damage)
- Disaster (few fatality, or $> \$10^6$ damage)
- Very serious (fatality, or $> \$10^5$ damage)
- Serious (serious injury, or $> \$10^4$ damage)
- Important (disability, or $> \$10^3$ damage)
- Noticeable (minor first aid accident, or $> \$10^2$ damage)

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.



E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

- 1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.
- 2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.
- 3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.
- 4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

I:\CIRC\MSC-FAL\1\MSC-FAL 1-Circ 3.docx



ANNEX

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 INTRODUCTION

1.1 These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, *maritime cyber risk* refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

1.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

1.3 For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

1.4 Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

1.5 Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization.

2 GENERAL

2.1 Background

2.1.1 Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

- .1 Bridge systems;
- .2 Cargo handling and management systems;
- .3 Propulsion and machinery management and power control systems;
- .4 Access control systems;
- .5 Passenger servicing and management systems;
- .6 Passenger facing public networks;
- .7 Administrative and crew welfare systems; and
- .8 Communication systems.

2.1.2 The distinction between information technology and operational technology systems should be considered. Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.

2.1.3 While these technologies and systems provide significant efficiency gains for the maritime industry, they also present risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyberthreats.

2.1.4 Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

2.1.5 Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyberdiscipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised.

2.1.6 Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g. inappropriate use of removable media such as a memory stick).

2.1.7 Further information regarding vulnerabilities and threats can be found in the additional guidance and standards referenced in section 4.

2.1.8 These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these Guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.

2.1.9 In considering potential sources of threats and vulnerabilities and associated risk mitigation strategies, a number of potential control options for cyber risk management should also be taken into consideration, including amongst others, management, operational or procedural, and technical controls.

2.2 Application

2.2.1 These Guidelines are primarily intended for all organizations in the shipping industry, and are designed to encourage safety and security management practices in the cyberdomain.

2.2.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

2.2.3 These Guidelines are recommendatory.

3 ELEMENTS OF CYBER RISK MANAGEMENT

3.1 For the purpose of these Guidelines, *cyber risk management* means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

- .1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
- .2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- .3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
- .4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
- .5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.2 Additional guidance and standards may include, but are not limited to:¹

- .1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
- .2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- .3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

4.3 Reference should be made to the most current version of any guidance or standards utilized.

¹ The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.

CURRICULUM VITAE

Aybars Oruc who was born in 1988, is a marine engineer. He is M.Sc. student of Piri Reis Universitesi Maritime Transportation Management Engineering.

He worked in rescue, training, LPG, aframax and container vessels. As a marine engineer onboard ships, he has worked for 1.5 years as sea service time. For three years, he worked as HSEQ Coordinator in a tanker operator. He has been already working as a HSEQ Superintendent at the same company for six months.

He gave seminars to cadets in reputable universities in Turkey about subject of maritime cybersecurity. Moreover, one of his articles related to maritime cybersecurity has been published through Current Awareness Bulletin (January 2018) issued by International Maritime Organisation (IMO). He attended as a speaker with his paper titled “Tanker Industry is more Ready against Cyber Threats” in the ICMET Oman 2019 international maritime conference.

He took part in EU projects which were eGMDSS.com and MarTEL (Maritime Tests of English Language) as a test user. He became the referance for a maritime project of European Bank of Reconstruction and Development. He has already three websites regarding maritime. One of them is relavent with maritime cybersecurity (CyberOnboard.com).

He is member of IMarEST (Institute of Marine Engineering, Science & Technology), IET (Institution of Engineering and Technology) and Engineering Council-UK.