ISSN 2810-9171 [print]

SNAMES

Society of Naval Architects and Marine Engineers Singapore

40th ANNUAL JOURNAL 2020/2021

Sustainable Development & Digital Innovation

SNAMES ANNUAL JOURNAL

CELEBRATING 40 YEARS OF TRENDS, ADVANCEMENT, AND TECHNOLOGY

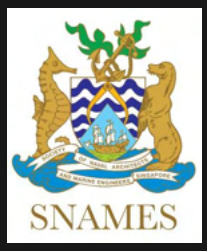
Contents

Anniversary Issue

The Technical Papers

Society of Naval Architects and Marine Engineers Singapore

40th Annual Journal 2020/2021



Publication Committee

SNAMES Secretariat Address
51 Goldhill Plaza #21-10
Singapore 308900
Email: admin@snames.org.sg
www.snames.org.sg

ISSN 2810-9171 [print]
ISSN 2810-9163 [e-periodical]

President's Message

Dear Fellow SNAMES Members,

On behalf of the council members, my warmest greetings to all of you.

2021 is a special year as it marks the Society of Naval Architects and Marine Engineers Singapore (SNAMES) 40th journal publication. This year, SNAMES will be printing copies of the journal which will be distributed to Institutes of Higher Learning, Trade Associations, and SNAMES Corporate Partners to commemorate this 40th publication.

The Covid 19 situation has disrupted our normal way of life and has forced businesses to develop new business processes and accelerate digitalization. This has led the SNAMES Council to choose the theme "Sustainable Development & Digital Innovation' for our 40th Annual Journal. Considering the Covid situation, businesses have transformed to be more resilient by adopting digitalization like Zoom, Augmented Reality (AR) and Virtual Reality (VR), and many more to conduct their businesses. Our major shipyards have also transformed their key business activities from traditional Oil and Gas to Renewable Energy to be sustainable and in line with the Environmental, Social, and Governance (ESG) criteria.

Although 2020/2021 has been challenging, SNAMES Technical Committee has continued to hold monthly technical talks with the Institute of Marine Engineering, Science and Technology - Singapore Joint Branch (IMarEST) and Singapore Shipping Association (SSA) to share on issues of mutual interests, knowledge, and experiences for our members

SNAMES has also successfully launched the LNG Primer Course together with Ngee Ann Polytechnic where we have recently completed the 3rd session of the course. It has been well received with a good turnout of 28 participants. The Technical Committee is also in talks with the Association of Marine Industry (ASMI) and Nanyang Technology University (NTU) to jointly organize an Offshore Wind Course which is scheduled to start in December 2021.

This year, SNAMES has successfully signed a Memorandum of Understanding with the National Trades Union Congress (NTUC) as NTUC's U Associate Partner and we are proud to be the first Marine Association to form this partnership with NTUC. With this, SNAMES and NTUC will explore joint programmes and co-organize events to engage current and potential Naval Architects, Marine Engineers, and other Maritime Professionals for the purpose of enhancing the careers of These professionals.

The Council will continue to work hard for our members. Our Media Committee and Membership Committee have put in tremendous efforts throughout the past months in bringing updated news and information on the industry to our members as well as enhancing members' benefits in all areas. I am pleased to announce that our membership numbers have grown this year through the awareness programs by the two Committees.

Although social interaction is restricted in many ways, our Social Committee has never stopped exploring options to organize events where members can get together while keeping to the rules and regulations of the safe distance measures.

The council would like to take this chance to express our thanks to the publication committee headed by Dr Ji Xi and her team as well as the members and authors who have contributed to the SNAMES 40th Journal. The publishing of the Journal will not be possible without the commitment and support from all of you.

Last but not least, I sincerely thank all our members and industry partners for their unreserved and unwavering support to Society over the years. SNAMES will continue our mission set forth by our forefathers in nurturing talents and advancing the maritime profession and I hope that you will continue to walk this path with us for the many years to come.

Ee Win LEE
President
SNAMES Council 2021/2022

Bureau Veritas

Dear Council Members and Members of SNAMES,

Bureau Veritas offers our warmest congratulations to SNAMES on this 40th Anniversary Annual Journal 2020 & 2021 milestone.

Over the past 4 years of partnerships, Bureau Veritas have had the pleasure of working with some of the most amazing members of SNAMES for various events such as webinars and primer courses. Bureau Veritas hope that SNAMES's goal to bring together dynamism and creative ideas of the industry will successfully attract more members to participate in SNAMES activities in the coming days. Nonetheless, in celebration of this milestone, Bureau Veritas would like to wish the newly formed council all the best in their future endeavours and many more successes to come.

Bureau Veritas embrace the idea of increasing collaborations with SNAMES to continue value-adding to the industry through the "Kampung Spirit". To which, Bureau Veritas looks forward to the plans SNAMES have in line. Once again, congratulations on SNAMES 40th Anniversary! Bureau Veritas look forward to many more with you!

Koh Shu Yong
Director
Innovation, Centre of Alternative Fuels & Renewable Energy
Bureau Veritas, Southeast Asia & Pacific Zone

Bureau Veritas (BV) is listed French company on the Paris Stock Exchange, founded in 1828. As one of the world's leading ship classification societies and offshore safety and verification bodies, BV specialises in the testing, inspection, and certification.
On 7th October 2021, Bureau Veritas Marine & Offshore Singapore (BV) has launched a new Centre of Excellence – the innovation Centre of Alternative Renewables Energy (iCARE), supported by the Singapore Economic Development Board (EDB).
Together with our BV Green Line of services & solutions, and other core competency within our global network, iCARE will empowers organizations to implement, measure and achieve their sustainability objectives better together and helping the industry to grow.

Wärtsilä

Dear SNAMES

Wärtsilä Singapore likes to congratulate SNAMES on your 40th Journal. We also like to show our appreciation to the publication team for all their hardwork and dedication to make this possible. The content of the journal has always been very informative and interesting. Keep up the good work and we are all looking forward to reading this 40th Journal.

Best regards

Ong Kong Young
Managing Director
Wärtsilä Singapore Pte Ltd

Wärtsilä is a global leader in smart technologies and complete lifecycle solutions for the marine and energy markets. By emphasising sustainable innovation, total efficiency and data analytics, Wärtsilä maximises the environmental and economic performance of the vessels and power plants of its customers. In 2020, Wärtsilä's net sales totalled EUR 4.6 billion with approximately 18,000 employees. The company has operations in over 200 locations in more than 70 countries around the world. Wärtsilä is listed on Nasdaq Helsinki.

IMarEST & RINA

Dear Council Members and Members of SNAMES,

On behalf of the Singapore Joint Branch of RINA & IMarEST I would like to congratulate you on your 40th Anniversary Annual Journal 2020/2021. The Annual Journal serves as a great opportunity for the organization to keep the members informed, share news and details of future plans and past achievements.

The content of the journal is always well laid out and often full of exciting and interesting content which shows off SNAMES as a leading society in the field of Naval Architecture and Marine Engineering with a very rich history in the industry and region.

The work that is put in by all the team to bring this publication together for the benefit of the members is a testament to the commitment that the council has to deliver content that they feel will benefit the members. In the Joint Branch of RINA & IMarEST we also very much understand the drive to deliver for the membership and many of our members are also members of SNAMES. This relationship between SNAMES, IMarEST and RINA is very valuable as we share the same passions for our profession, and we are all driven by similar goals. The collaboration that we enjoy between the societies in organizing technical talks that are always very popular amongst the membership is further proof of the strong bond that we share in Singapore and across our industry to share our ideas and resources for the benefit of our members.

This year also marks 40 years since SONAS overhauled its constitution to allow Marine Engineers to join the society forming SNAMES and this was obviously a very wise move by the society at that time, for which it has reaped the rewards and I believe is cause for further celebration.

Once again, I would like to congratulate you on your achievements and look forward to many more years of partnership between our Institutes/Societies.

Wishing you all good health and future prosperity, especially during these difficult times for many.

"The Annual Journal serves as a great opportunity for the organization to keep the members informed, share news and details of future plans and past achievements."

Mike Watt IEng., IMarEng., MIMarEST, MTA Dip SBR.
Chairman
Singapore Joint Branch (IMarEST & RINA)

Apex Chemicals

On behalf of APEX Chemicals (S) Pte Ltd, I would like to extend our heartfelt congratulations to SNAMES and its editorial team on the publication of its 40th annual journal. This outstanding accomplishment is truly a testament of the Society having firmly established itself as an important platform for its members to share credible knowledge and technical capabilities.

The highly regarded journal has served a key role in informing and educating its readers, presenting itself as a reliable source of invaluable information with professionally written articles and insightful reports that are vital to the advancement of the industry. I look forward to the continued publishing of high-quality editorial works that reflect the development and innovations of the marine and naval architectural sector.

I would also like to take this opportunity to thank the past and present teams at SNAMES for your strong dedication and commitment in championing and addressing the various challenges to move towards a more sustainable solution for its members. I look forward to the Society continuing its significant role in nurturing and advancing the industry with even more collaborative efforts in the future.

Here is wishing SNAMES many more years of well-deserved success!

MJ Foo
Director of Sales, Apex Chemicals (S) Pte Ltd

Apex CHEMICALS

Founded in 1993 and headquartered in Singapore, **Apex Chemicals (S) Pte Ltd** is proud to have transformed into one of the leading manufacturers and global suppliers of marine, water treatment, industrial chemicals.

We offer a complete range of chemicals for tank cleaning, cargo hold cleaning, water treatment and maintenance chemicals. Our extensive portfolio of marine products was developed to meet every need of our international customers.

Our global network consists of strategic alliances formed in partnership with our stakeholders to provide our clients with the right chemicals for the right job, each time, every time.

ASSURANCE RELIABILITY COMPLIANCE

Dear Council Member and Members of SNAMES,

The management of Assurance Reliability Compliance Pte Ltd (ARC) congratulates SNAMES on the publication of the 40th Anniversary Annual Journal 2020/2021. The Annual Journal serves as a great opportunity for the organization to keep the members informed on future plans and past achievements.

The hard work and dedication of the team and personnel who bring this publication together, demonstrates a strong commitment from the council to deliver content to the benefit of all members.

We extend our warm wishes from the entire organization of Assurance Reliability Compliance Pte Ltd (ARC) and look forward to building a strong relationships with the members and many more years of partnership with SNAMES.

Rob Egan
Technical Director
Assurance Reliability
Compliance Pte Ltd

ASSURANCE RELIABILITY COMPLIANCE PTE LTD

We are amongst the leading Assurance and Risk Management companies in Australasia. Through understanding and working closely with our clients, we have jointly achieved successful outcomes on a number of high-profile Rig Acceptance, Facility Assurance and Risk Management work scopes.

Being a serviced- based company, our strength is Operational Capability with an in-house ability to align critical processes, resources and technologies according to the overall requirements.

We provide customer focused value propositions to deliver these processes effectively, efficiently and above all safely. www.arc-assure.com

DEUTZ Asia Pacific & Torqeedo

"DEUTZ Asia Pacific with Torqeedo congratulate SNAMES in celebrating its 40th year anniversary. *Magnum Opus*! "

Desmond Ho
Technical Service & Training
DEUTZ Asia-Pacific (Pte) Ltd & Torqeedo Singapore

Hydrov

Dear SNAMES

Hydrov Singapore likes to congratulate SNAMES on your 40th Journal. We also like to show our appreciation to the publication team for all their hardwork and dedication to make this possible. The content of the journal has always been very informative and interesting. Keep up the good work and we are all looking forward to reading this 40th Journal.

Best regards
Michael Gan,
Managing Director

Hydrov Singapore Pte Ltd is a spinoff from Underwater Contractors Pte Ltd who has been in the business of Ship Husbandry since 1979. Leveraging on decades of underwater experience and passion for robotics technology, we strive to redefine status quo to improve safety and efficiency through our patented inhouse design Hull cleaning ROV (UCM series) with surface torque control system.

Pinnacle Marine

Dear Council Members and Members of SNAMES,

Pinnacle Marine (S) Pte Ltd would like to congratulate you on the 40th Anniversary of your annual journal. This is the first year of Pinnacle Marine in SNAMES and we are very honoured to be part of this community with rich history and achievements field of Naval Architecture and Marine Engineering.

We would like to thank the great effort put up by the council and team in making the annual journals possible. By compiling the journals is no easy task. It requires great commitment and passion to deliver rich, informative and engaging content to members especially in these difficult times now where physical gatherings are no longer frequent or possible. With these journals, members are able to connect in a way and able to keep ourselves updated on what is happening in the industry.

Once again, we would like to congratulate everyone in SNAMES and we wish all with good health and success in the years ahead!

Pinnacle Marine (S) Pte Ltd was established in 2009, It is the holding company of various well recognised subsidiary companies including Primus Shipping Agencies (S) Pte Ltd and Prestige Ocean Pte Ltd.

Collectively, the group provides an integrated 1 stop service ranging from ship building, ship supplying, boat repairs, custom fabrication, shipping agency services, and supply boat services.

Pinnacle Marine started building aluminium boats in 2018 under the Singapore Flag, with BV classification and is now the fastest 15m boat builder in Singapore by delivering a boat within 3 months.

The group is now actively involved in various governmental contracts and has gained reputable recognition for their standards within the maritime industry.

SeaTech Solutions

Dear Council Members and Members of SNAMES,

SeaTech Solutions International (s) Pte Ltd wishes you, our sincere and warm congratulations on this very auspicious 40th Anniversary of your Annual Journal; 2020/2021. Your remarkable growth over the last four decades is, indeed, a time for a truly well deserved, and well-earned celebration. Our appreciation shows no bounds, and we cannot be any prouder than we now are, to be a member of SNAME. SNAME'S Annual Journal has always stood out as one of the leading names in the industry, and that is always an immense tribute.

Over the years, SNAMES Annual Journal has charted an impressive path, attaining widespread recognition as the go-to for all challenges with strength, determination, and confidence with a well-established reputation in the field of Naval Architecture and Marine Engineering. Coupled with exciting content collaboration we have together chalked up, on milestones, achievements, and more milestones.

Once again, may our business relationship flourish and continue in the years ahead to eventually, bloom, blossom and illumine this exciting and invaluable partnership.

"Kudos on delivering 40 years of inspiring content. Best wishes for reaching new heights and continue to leave a mark in the years to come!"

Mr. Prabjot Singh Chopra
Vice President,
Technology of SeaTech
Solutions International

About SeaTech Solutions International
Naval architecture firm SeaTech is a centre for marine and offshore excellence, exemplifying innovation, technology and expertise in 380 unique vessel designs. Currently, over 640 vessels operating worldwide bear the SeaTech hallmark of energy efficiency, safety and reliability.

www.seatechsolutions.com

SecuriState

Dear Council Members and Members of SNAMES,

Securistate Private Limited extends its best wishes to SNAMES on their 40th Anniversary Annual Journal 2020 & 2021. We are a new entity who joined SNAMES recently. However, we are looking forward to seeing and meet more members and distinguished people.

As we are new to SNAMES we understand that there are virtual events and knowledge sharing episodes being carried out. We are looking forward to participating in such events to keep abreast of what happening and what is new in the marine industry.

Once again Securistate congratulates the 40th Anniversary of SNAMES.

SecuriState Pte Ltd is a privately owned security company that was founded to assist companies and organizations with a variety of security services and solutions. The company has been established in 2010.

SecuriState Pte Ltd provides Anti-Piracy Armed Guards to International Shipping Clients. It has offices in Singapore, Sri Lanka, India, Ghana, Malaysia, and Indonesia. In Singapore, SecuriState Pte Ltd provide Unarmed Security services, Security Systems, and polygraph Services. In safeguarding the essence of protection against the threat of sea piracy onboard merchant vessels, SecuriState Pte Ltd. has a keen sense of observation, operations expertise, and experience in protection service.

Virvit

Dear Council Members and Members of SNAMES,

Talent-Merge would like to congratulate SNAMES on their 40th Anniversary Annual Journal. The annual journal provides vast great knowledge for us and we are humbled to have gained the knowledge and insight that have been shared. It has truly been a wonderful learning experience for us and this will definitely be of great help in our future endeavours.

We are excited and eagerly look forward to your next interesting Naval Architecture and Marine Engineering content.

Virvit app is available for download on Play store and Apple store from October 2021. Virvit allows candidates to upload video resumes and video testimonials seamlessly.
Submitting a video resume and video testimonial is trending for companies seeking to find the best talent and also provides a more accurate description of candidate's personality, attitude and skill sets. With Virvit, it makes the hiring process easier, faster and more fun!
Download VirVit today for an exciting experience.

OceanMaster

Dear Council Members of SNAMES,

On behalf of the Board of Directors, Management and Staffs of OceanMaster Engineering Pte Ltd, we would like to express our heartfelt congratulations to SNAMES for making the SNAMES 40th Annual Journal possible and with great success

We sincerely appreciate the commitment and hard work from the SNAMES Publication Team, Council Members as well as the Authors and Members who have contributed to the journal.

Every year, the SNAMES journal provides great content and information on the latest technology for the industry and we look forward to reading the upcoming publication of the SNAMES 40th Annual Journal.

Andy Lee
Director
OceanMaster Engineering Pte Ltd

OceanMaster Engineering Pte Ltd was established in 1989 as a company that specializes in providing ship repairs services and in RHVAC.

With time, the company grew in size and diversify into serving clients from the Renewable, Offshore, Oil and Gas sector. Up to date, OceanMaster provides services primarily to Drilling Contractors, FPSO and LNG Vessel Owners, Oil Majors and Ship Owners around the world.

We possess an excellent track record in executing full turnkey projects, offering quality and cost-effective Engineering Solutions to our clients in the areas of Scrubber Systems, mechanical, electrical, carpentry and steel works.

Council Member 2020/2021

President

Mr. Shu Yong KOH
Bureau Veritas

Vice-President

Mr. Teck Chye YEO
MediaComz International Pte Ltd

Vice-President

Mr. Yujin CHIA
Jurong Port

Honorary Secretary

Mr. Ee Win LEE
Oceanmaster

Honorary Treasurer

Mr. Dan KWEK
Eastern Pacific Shipping

Council Member 2020/2021

Media Chairperson

Ms. Dawn SETOH
Wilsafe System

Memberships Chairperson

Ms. Joyce TAN
Oil Rich Marine & Offshore

Technical Chairperson

Dr. Joo Hock ANG
Sembcorp Marine

Publication Chairperson

Dr. Xi JI
Worley

Social Chairperson

Mr. Tuck Wei ONG
NgeeAnn Polytechnic

Secretary

Mr. YEO Liangyi Gabriel
Bureau Veritas

Technical Committee

Dr. LIM Chin Lee
Sembcorp Marine

Publication Committee

Dr. Giulio GENNARO
1888 Gennaro Consulting

Publication Committee

Dr. Iris Jiyeon KIM
Cistron Offshore & Trading

Membership Committee

Mr. Clarence KHOH
Talent-Merge

Social Committee

Mr. LOO Tat Chung
DNV GL

Media Committee

Mr. CHONG Wan Seong

Membership Committee

Mr. CHIN Kok Ken
RINA

Technical Committee

Mr. Jeffrey MACASERO
MODEC

Publication Committee

Mr. Ivan STOYCHEV
Consultant

Past Presidents of SONAS/SNAMES

SOCIETY OF NAVAL ARCHITECTS SINGAPORE (SONAS)

YEAR	PRESIDENT	VICE
1973/1974	Mr Tan Kim Chuang	Mr Keki R Vesuna
1974/1975	Mr Tan Kim Chuang	Mr Ho Ming Yeh
	Mr Ho Ming Yeh	Mr Keki R Vesuna
1975/1976	Mr Chua Chor Teck	Mr Alan Bragassam
1976/1977	Mr Chua Chor Teck	Mr Kalman E Nagy
1977/1978	Mr Chua Chor Teck	Mr Alan Bragassam
1978/1979	Mr Chua Chor Teck	Mr Alan Bragassam
1979/1980	Mr Chua Chor Teck	Mr Tan Kim Chuang
1980/1981	Mr Chung Chee Kit	Mr Lim Boon Heng

SOCIETY OF NAVAL ARCHITECTS AND MARINE ENGINEERS SINGAPORE (SNAMES)

YEAR	PRESIDENT	VICE
1981/1982	Mr Cheng Huang Leng	Mr Choo Chiau Beng
1982/1983	Mr Cheng Huang Leng	Mr Choo Chiau Beng
1983/1984	Mr Choo Chiau Beng	Mr Ronald M Pereira
1984/1985	Mr Ronald M Pereira	Mr Tay Kim Hock
1985/1986	Mr Choo Chiau Beng	Mr Charlie Foo
1986/1987	Mr Choo Chiau Beng	Mr Charlie Foo
1987/1988	Mr Charlie Foo	Mr Toh Ho Tay
1988/1989	Mr Toh Ho Tay	Mr Teh Kong Leong
1989/1990	Mr Teh Kong Leong	Mr Loke Ho Yong
1990/1991	Mr Loke Ho Yong	Mr Dennis Oei
1991/1992	Mr Dennis Oei	Mr Goh Choon Chiang
	Mr Goh Choon Chiang	Mr Wong Kin Hoong
1992/1993	Mr Tan Kim Pong	Mr Zafrul Alam
1993/1994	Mr Zafrul Alam	Mr Ng Thiam Poh
1994/1995	Mr Ng Thiam Poh	Mr Dennis Oei
1995/1996	Mr Dennis Oei	Mr Kan Seng Chut
1996/1997	Mr Kan Seng Chut	Mr James Tan
1997/1998	Mr James Tan	Mr Phua Cheng Tar
1998/1999	Mr Phua Cheng Tar	Mr Leslie Low
1999/2000	Mr Leslie Low	Mr Wong Kin Hoong
2000/2001	Mr Wong Kin Hoong	Mr Leow Ban Tat
2001/2002	Mr Leow Ban Tat	Mr Ying Hing Leong
2002/2003	Mr Ying Hing Leong	Mr Tan Chor Hiong
2003/2004	Mr Tan Chor Hiong	Mr Dennis Chua
2004/2005	Mr Dennis Chua	Mr Ernest Wee
2005/2006	Mr Ernest Wee	Mr Fabian Chew
2006/2007	Mr Fabian Chew	Mr Goh Boon Guan
2007/2008	Mr Goh Boon Guan	Mr Chen Chin Kwang
2008/2009	Mr Chen Chin Kwang	Mr Simon Kuik
2009/2010	Mr Ronald M Pereira	Mr Kenneth Kee
	Mr Kenneth Kee	Mr David Kinrade
2010/2011	Mr Kenneth Kee	Mr Simon Kuik
2011/2012	Mr Kenneth Kee	Prof Choo Yoo Sang
2012/2013	Prof Choo Yoo Sang	Mr Ang Ee Beng
2013/2014	Prof Choo Yoo Sang	Mr Prakash Balasubramaniam
2014/2015	Prof Choo Yoo Sang	Dr Nigel Koh
2015/2018	Mr Foo Nan Cho	Mr Prem Shankar
2018/2019	Mr Koh Shu Yong	Mr Yeo Teck Chye
2019/2020	Mr Koh Shu Yong	Mr Yeo Teck Chye
2020/2021	Mr Koh Shu Yong	Mr Chia Yujin

SNAMES 49th Annual General Meeting

The SNAMES 49th Annual Meeting (AGM) was held on 28th April 2021 at the Republic Of Singapore Yacht Club (RSYC).

Due to the COVID-19 situation, the maximum capacity for members to be present at RSYC for the AGM was 45 persons. Other members attended the AGM via Zoom.

The AGM elected Members of the Council for the year 2021/2022.

Council 2021/2022 New Era, New Strategies

Mr. Tat Chung LOO
Co-opted Council Member (Social)
(DNV)

Dr. Chin Lee LIM
Council Member (Technical)
(Sembcorp Marine)

Mr. Preston SOH
Council Member (Media)
(Cheng Xin ShipManagement)

Mr. Yujin CHIA
Vice-President
(Pacific International Lines)

Dr. Joo Hock ANG
Council Member (Chairperson – Technical)
(Sembcorp Marine)

Mr. Ivan STOYTCHEV
Council Member (Publication)
(Consultant)

Dr. Xi JI
Council Member (Chairperson – Publication)
(Worley)

Ms. Joyce TAN
Co-opted Council Member (Social)
(Oil Rich Marine & Offshore)

Mr. Ee Win LEE
President
(Ocean Master)

Mr. Jun ER
Honorary Treasurer
(Edge Group)

Mr. William HWANG
Council Member (Membership)
(Jurong Port)

Mr. Gabriel YEO
Co-opted Council Member (Secretariat)
(Bureau Veritas)

Mr. Tuck Wei ONG
Council Member (Chairperson – Social)
(Ngee Ann Polytechnic)

Mr. Kai Cheong WONG
Honorary Secretary
(Intertanko)

Mr. Dan KWEK
Council Member (Chairperson – Media)
(Eastern Pacific Shipping)

Mr. Shu Yong KOH
Past President
(Bureau Veritas)

Mr. Wan Seong CHONG
Co-opted Council Member (Media)
(Consultant)

Mr. Clarence KHOH
Council Member (Chairperson – Membership)
(Talent-Merge)

Ms. Catherine CHONG
Co-opted Council Member (Media)
(Seabliss Marine Services)

Mr. Benny LIM
Council Member (Membership)
(Maersk)

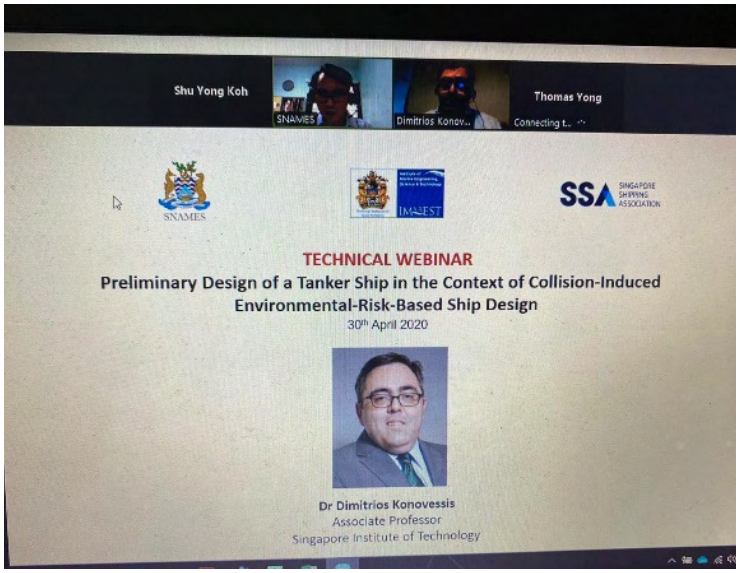
Mr. Jeffrey MACASERO
Council Member (Technical)
(Modec)

Technical Talks & Primer Course

1

Dr Ang Joo Hock

"Transforming the Marine and Offshore Industry through Digitalisation and Industry 4.0"



2

Dr Dimitrios Konovessis

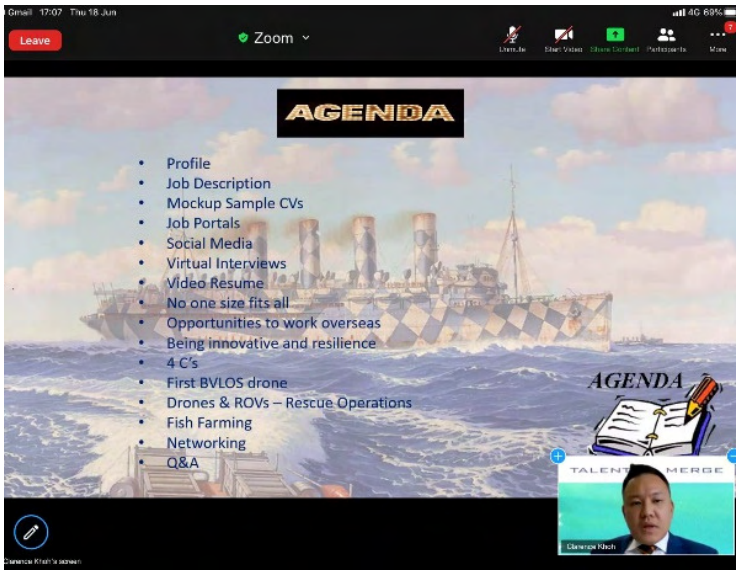
"Smart Ships - Paradigm shift with IoT and Data analytics"

3

Mr Toh Keng Hoe

“Digitalisation and Innovation in the Maritime Industry”

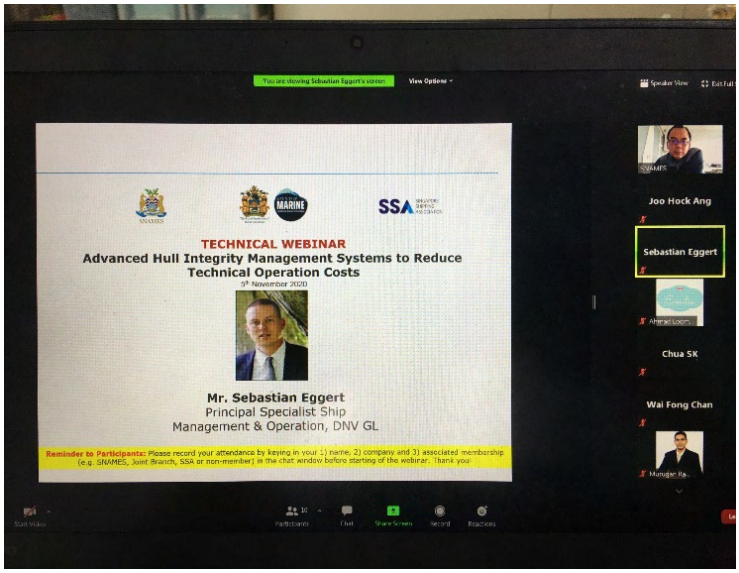
Technical Talks & Primer Course



4

Mr Clarence Khoh

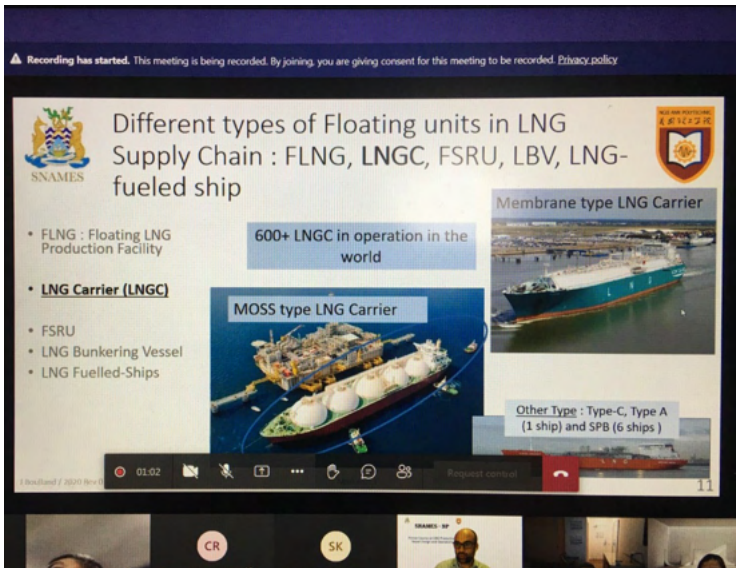
"The New HR Norm, Virtual Interviews To Hiring"



5

Mr Sebastian Eggert

"Advanced hull integrity management systems to reduce technical operation costs"



6

SNAMES-NP Primer Course

"LNG Production, Vessel Design and Operations"

SNAMES Book Prize Awardees 2020/ 2021

SNAMES contribute Book Prizes to schools to recognise outstanding young individuals who demonstrate academic excellence and personal qualities in courses such as Naval Architecture, Marine Engineering or in any other branches of maritime-related engineering profession.

Bagus Galih Loo

Diploma in Marine Engineering by Singapore Maritime Academy of Singapore Polytechnic

You can't cross the ocean unless you're willing to lose sight of land. This saying applies not only to sailors but to all of us; if you lack the courage, you will be unable to do anything that you desire. Over the past three years, I've realized that working alone can only get you so far. Make sure that you are with people who will support you. When in doubt, there is no harm asking! Make friends, not enemies. There is always something to learn from others, no matter how intangible it may seem.

Benjamin Hay Kay Xiang

Diploma in Marine and Offshore Technology - School of Engineering, Ngee Ann Polytechnic

In my 3 years as a student pursuing the Diploma in Marine and Offshore Technology, I have been exposed to various technical, theoretical, and practical skills and knowledge through the modules I have encountered.

"Fundamentals of Naval Architecture" had provided me with the necessary information when it came to understanding how a vessel is designed from the start to end. "Marine Production Technology" equipped me with invaluable information as to the real-world workflow of how a vessel is assembled. Lastly, the "Marine Design Project" which was the Final Year Project. It gave me an opportunity to put the knowledge I had accumulated over the years into real use. Designing the subsea flow line, selecting the vessel of choice (FPSO), and equipping the vessel with the relevant topside modules where we performed the necessary calculation for each module and to sum things up, to calculate the stability of the vessel to ensure that it would meet classification requirements. Despite the many trials and tribulations, it has been a fulfilling and memorable journey throughout. Through the skills and knowledge acquired, I have come to appreciate the complexities and intricacies of designing a vessel. The immense levels of coordination, teamwork and wide range of expertise uniting to construct a vessel are truly admirable. As for what the future holds for me, I am keeping my options open to any opportunity that may provide me growth and meaning to life.

Kok Jia Xing

Diploma in Marine Engineering by Singapore Maritime Academy of Singapore Polytechnic

Marine Engineering consists of a wide range of engineering disciplines. Through this course, I have learned to apply engineering science, mechanical and electrical engineering principles to understand the operations and maintenance of a vessel. I was exposed to the 'heart' of the ship, learning marine engineering systems such as main propulsion engines to auxiliary machinery and many other subsystems such as air compressors, heat exchangers, fresh water generators, and hydraulic systems in ensuring the overall smooth operations of a ship. Though it was a difficult and complex course, through hard work and an inquisitive learning attitude I was able to understand these interesting systems and how a ship works. I look forward to being part of the maritime industry and I am interested in innovating, digitalizing, and designing better port and vessel operations.

Mevyn Teo Jia Jun

Diploma in Marine and Offshore Technology - School of Engineering, Ngee Ann Polytechnic

I'm glad that I have managed to complete this program, The program has been tough but I have gotten tons of help from my friends, family, and lecturers, I would say that I would not have gotten such results if not for them. They helped ignite my passion to work harder and strive to do my best.

I would say meeting the right people here, in Ngee Ann Polytechnic, has helped tremendously with how I work towards my goal in Polytechnic.

Muhammad Syazwan Hidayat Bin Shamsuddin

Diploma in Marine and Offshore Technology - School of Engineering, Ngee Ann Polytechnic

First and foremost, I had to thank all of the lectures that have taught me and my fellow classmates throughout the years of my polytechnic life. I am glad that I am able to complete the program despite coming from ITE. I hope that I prove to the doubters that no matter where you came from. If you want to achieve, you got to work for it. There is no easy way out. As I will be enlisting soon for my National Service, I am looking forward to furthering my studies after that. I hope that at the end of the journey, it will be a fruitful one.

The Technical Papers

Can Shipyards in Singapore Remain Relevant? The Threats and Opportunities Ahead

Lim Soon Heng
Senior Advisor / Past President, Society of FLOATING SOLUTIONS (Singapore)

Abstract

With the inevitable decline of the shipyard industry, naval architects and marine engineers need to engage themselves meaningfully. The knowledge and skill that they acquired over several decades delivering some of the best offshore structures to the world will stand them well to deliver solutions to Singapore's pressing need for space.

Singapore's landmass increased by 25% through land reclamation. It still needs another 56 sq. km by 2030 according to official projection. The supply lines for sand have dried up. Floating solutions offer a way to overcome the shortage. It is environmentally friendly and climate-resilient.

The only professionals in Singapore who are trained and who have the necessary experience to engineer construct and deliver mega floating islands are in the shipyards. It is incumbent on them to stand up and be counted.

This nation can be a Centre of Excellence for mega floats just it was for offshore oil rigs and FPSOs. SNAMES must play a key role towards that end.

Introduction

In the 1960s unemployment was high. Labor-intensive industries were attractive investment targets. Ship repairing and shipbuilding being hugely labor-intensive featured brightly on the investment radar.

Fifty years on, the socio-economic landscape of Singapore has changed, so much so we are importing foreign workers instead. Singapore has lost its prime position as a ship repairer in Asia. It is hegemonic position as an offshore rig building hub west of South Korea and Japan is threatened by newcomers in India, Vietnam China, and others.

The shareholders of the two giants of the industry, Keppel and Semb Marine have declared their plan to exit their core business. A chapter has closed. A new one begins for shipyards and their supply chain.

If the experience of the US, UK, and Japan is anything to go by, no government has adequate resources to reverse the declining fortunes of their shipyards.

This paper presents the case for the professionals in the industry to rise to the occasion by deploying their skills and expertise to help Singapore become a Centre of Excellence for other floating solutions. Just as semi-subs and spars are solutions to resolve depleting oil sources on land, Singapore needs to find floating solutions to depleting land resources.

In this regard, no engineering professionals are better equipped to offer solutions than those who have spent the best part of their careers in shipyards. It is this human resource that members of institutions such as SNAMES, RINA, IMarEST, ASMI, and SFSS must collectively muster to offer a helping hand to the government agencies in their search for space for this overcrowded island state.

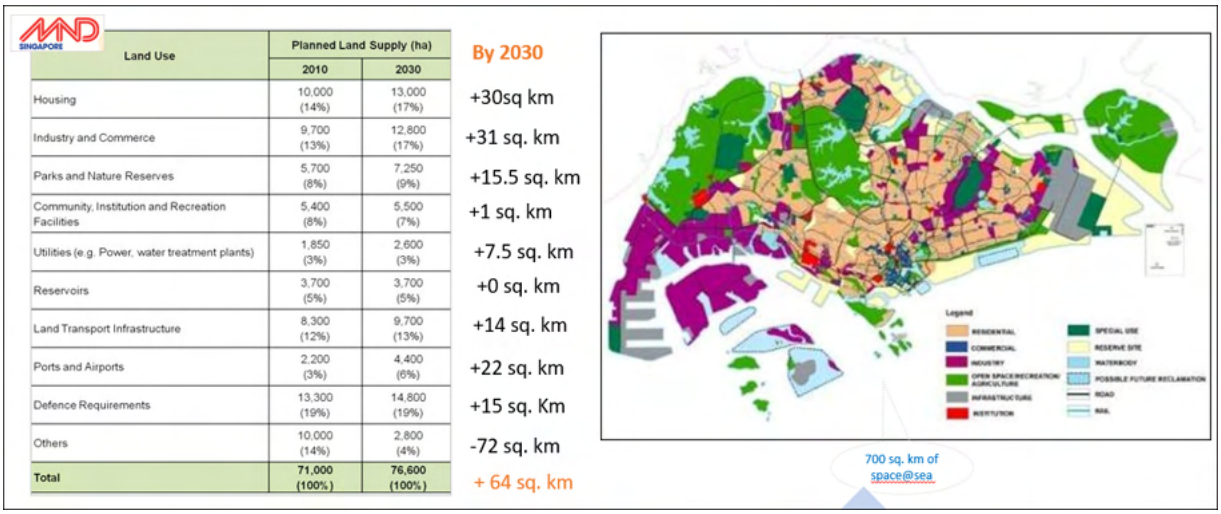
How Much More Land Does Singapore Need?

The Ministry of National Development projects that Singapore would need 56 sq. km more land by 2030. One can see from the graphics below that the plan is to reclaim coastal land around the mainland and offshore islands.

To put this in context, 56 sq. km represent 8% of our territorial waters. It is not an issue that will affect shipping and with smart planning, the space to be created need not abut the coastline. It can be hundreds of meters offshore thereby giving more scope for the planner to express his vision. This is possible whatever the depth of water is well sheltered by the Riau Archipelago.

The current method of creating space in the sea that is in use in Singapore is by land reclamation, either fully to a few meters above or partially to a few meters below the highest astronomical tide and surrounded by embankments. The latter case reduces the demand for sand and is currently employed in the project at Tekong. The system is called dykes and polders. We shall refer to this as poldering for short.

Reclamation and poldering suffer from several deficiencies. Instead, space at sea using mega floaters is increasingly finding favor.



Land Use	Planned Land Supply (ha)		By 2030
	2010	2030	
Housing	10,000 (14%)	13,000 (17%)	+30sq km
Industry and Commerce	9,700 (13%)	12,800 (17%)	+31 sq. km
Parks and Nature Reserves	5,700 (8%)	7,250 (9%)	+15.5 sq. km
Community, Institution and Recreation Facilities	5,400 (8%)	5,500 (7%)	+1 sq. km
Utilities (e.g. Power, water treatment plants)	1,850 (3%)	2,600 (3%)	+7.5 sq. km
Reservoirs	3,700 (5%)	3,700 (5%)	+0 sq. km
Land Transport Infrastructure	8,300 (12%)	9,700 (13%)	+14 sq. km
Ports and Airports	2,200 (3%)	4,400 (6%)	+22 sq. km
Defence Requirements	13,300 (19%)	14,800 (19%)	+15 sq. Km
Others	10,000 (14%)	2,800 (4%)	-72 sq. km
Total	71,000 (100%)	76,600 (100%)	+ 64 sq. km

Figure 1 Additional land areas needed by 2030 according to a projection by the government

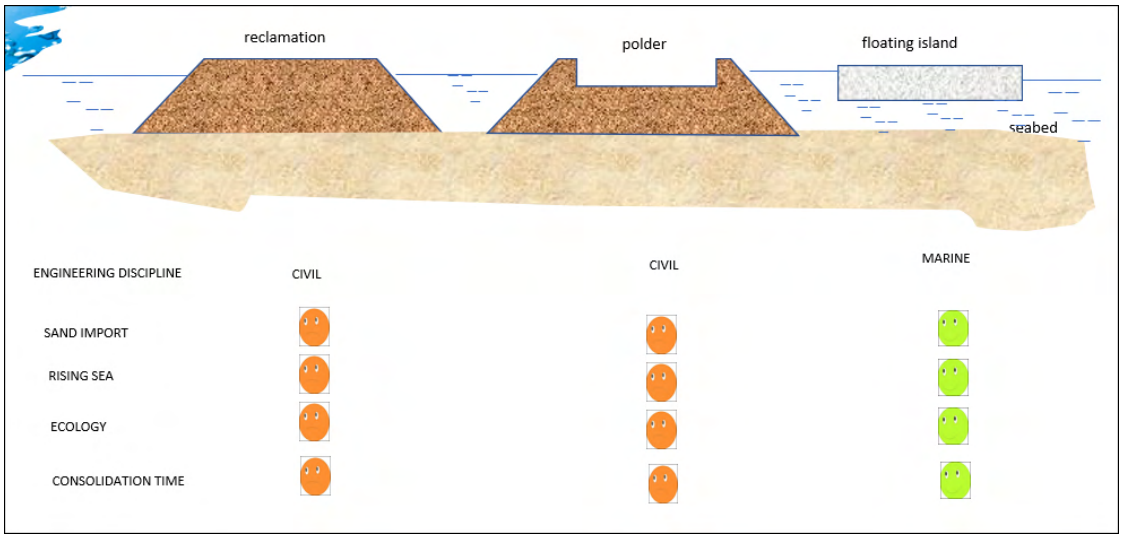


Figure 2 The merits of the floating solution as opposed to full or polder-type reclamation are easy to discern

Floating Islands Is a Holistic Space Creation Solution

Floating islands are a holistic solution to create space that overcomes many of the shortcomings of empoldering and reclamation.

Mega floats or floating islands are artificial islands sometimes referred to in engineering literature as VLFSs (Very Large Floating structures.) They are built offsite, towed to their final destination, and maybe joined to increase their footprint. The floating stadium in Marina Bay is an example, comprising 15 smaller modules connected so that the assembly behaves as a single rigid structure larger than a football field. Larger structures such as a runway for aircraft are possible, in fact, one, measuring 1000 meters in length has been successfully tested.

Figure 2 shows schematically the three possible ways of creating space at sea. Singapore has reclaimed 150 km2 and is now constructing an 8 sq. km polder as sand supply runs out. The largest floating island constructed in one of our shipyards is about one hectare in the area (excluding those in the oil and gas sector)

Both land reclamation and poldering require importing massive volumes of sand. It becomes impractical or prohibitively costly when water depth exceeds six meters. Both are vulnerable to rising sea levels. They both annihilate the marine biodiversity at the place where the sand is sourced and where it is deposited. Both require years for the reclaimed space to consolidate. Consequently, the financing cost could amount to 10 to 20 percent more than the construction cost.

Dykes can fail for a variety of reasons from erosion by pounding waves to damage by collision with ships and damage by coastal creatures including moles, otters, rats, and crabs. Google dyke failure mechanism to learn more. Dykes are not earthquake or tsunami-proof.

Polders are costly to maintain. Much energy is needed to operate the supersize pumps to dewater the enclosed space especially with our annual precipitation of more than 2 meters.

A disproportionate area of a polder has no practical use: the dyke itself, catchment ponds, and large drains to transport surface and subterranean water to catchment ponds.

Floating islands overcome all of the above shortcomings. They are safer, more robust, and their life cycle cost is substantially lower. The folks in the marine industry need to call the attention of our city planners to the overwhelming advantage of floating islands vis-à-vis the other two solutions.

The marine industry is an innovative one. When the demand for oil and gas escalated, they rose to the challenge and produce floating rigs that could recover and process oil and gas in some of the most hostile oceans in the world. Such innovations as jack-up, semi-submersible, spar, FPSO, FLNG, and FRSU have become by-words in the lexicography of energy.

Likewise, it is incumbent on those who have the expertise to step forward and excite the government agencies with a new way to create space.

How Big Is The Market For Floating Islands In Singapore?

By 2030, if floating islands were created to meet the government's target of 56 sq. km, there would be enough opportunities to keep all maritime professionals in the shipyard industry fruitfully employed for the rest of their careers. I conservatively estimate the market is worth 50 to 60 billion dollars over the next ten years.

What are the assets that could be erected on floating islands? That is something that the folks in the maritime industry need to help the planning agencies including URA, JTC, MINDEF, BCA SFA sort out.

Technically any asset that exists around us may be replaced by an equivalent on a floating island: the height, footprint, or mass of the structure is not an issue. The heaviest man-made structure is floating in some of the worlds harshest oceans, a floating 3 sq. km port is being model tested in Rotterdam, a 1000-m long runway was constructed in a shipyard in Japan and successfully tested.

I have in the past few years written opinion pieces for the Straits Times advocating floating the East Coast Park, shipyards, nuclear power plants, data centers, dormitories, and condominiums. Other worthwhile assets to erect on a floating island that now occupies repurposable land include oil refineries, fuel storage tanks, incinerators, desalination plants, power stations, vegetable and meat farms, military training facilities, including naval bases, fighter craft runways.

The easy ones are recreation grounds such as golf courses and beaches. There is little reason not to kick start with these for planners to gain confidence. East Coast Park need not be where it is. It could be floating half a kilometer out in the sea at Bedok. Recreation would be no less accessible or exciting with a floating park served by ferries taking no more than a few minutes to transport holidaymakers.

In every case, there is a good reason for urban planners to reach out to the maritime fraternity for advice. They need domain support services to develop a master plan of the sea that would also address maritime transportation systems for the movements of megastructures during erection and demobilization as well as the movements of goods and passengers.

Jurisdiction, Finance, and Underwriting

The United Nations Convention on the Law of the Sea (UNCLOS) specifically recognizes the "exclusive right (of the coastal State) to construct and to authorize and regulate the construction, operation, and use of artificial islands; " and "have

exclusive jurisdiction over such artificial islands, installations and structures, including jurisdiction with regard to customs, fiscal, health, safety and immigration laws, and regulations."

A floating island is a mortgageable asset. Like a ship, it can be pledged as collateral to secure loans to finance its construction.

Ship financing is an industry which the Maritime and Port Authority (MPA) actively promotes. International financial institutions are keen to finance the maritime sector through Singapore. The Maritime Finance Incentive (MFI) Scheme will further enhance shipbroking/ management, marine insurance/finance, maritime legal/ arbitration services, R&D initiatives, and manpower expertise.

This is another dimension that urban planners should take cognizance of. There is no valid reason why it is necessary to dip into the state coffers to fund space creation when it is possible to leverage on the global financial market.

The marine fraternity must task itself to drive home this point. The option to leverage on the equity market may encourage government agencies to look outside the box, in their search for space.

Exporting floating solutions

Floating islands like ships and offshore rigs are exportable products.

With access to ship financing and a robust regulatory framework, Singapore is well-positioned to be a successful center for the export of floating islands. This does not necessarily mean these floaters and their payload have to be built in Singapore. Parts of a ship's hull and superstructure are oftentimes built in several places and integrated into a country that is designated as the country of manufacture. Likewise, it would be possible to build a floating island in Batam, its 5-star hotel superstructure in China and integrate the two in Singapore and label the asset as a product of Singapore; financed, owned, and registered in Singapore.

The final product can be exported to say the US if it attracts a buyer there.

Of course, the asset can be anything else: a port, a stadium, a casino, a floating horticultural dome, or a condominium.

A consortium of shipyards can be formed first to identify suitable assets and then to market them globally. MPA could be brought in to support the project to invite financiers.

Because a substantial proportion of the work can be performed outside Singapore, local yards would be able to scale down their dependence on foreign workers, decommissioned some of their physical assets such as docks, berths, and workshops. This would result in a significant reduction of overheads.

Integration of topside structures with the floating platform can be done afloat with heavy lift cranes. They may be carried out in open waters as opposed to shipyard quaysides. Power, water, gas, and other utilities as well as machine shops may be mounted on floating berths to support the integration effort. These floating facilities can be deployed wherever they are needed.

Concrete, the Material of Choice

Hardly any shipyard in Singapore produces any floating structure in concrete. Designing in reinforced concrete would be a new skill that some need to acquire.

Concrete is less costly than steel. Pouring concrete and bending steel reinforcement bars do not require highly skilled workers, unlike welding steel. Quality control is more easily administered. The labor cost component of fabricating floating concrete structures is a fraction of that its steel equivalent.

Concrete is more durable in seawater than steel. If properly batched, concrete can be extremely impervious and can prevent corrosion of the rebars for a hundred years without painting. Steel on the other hand requires scraping, cleaning, and repainting in a drydock every five years or so.

Figure 3 The Adriatic LNG storage and regasification facility was constructed in a temporary yard with only a temporary earth cofferdam which was removed to float the structure. Cost is reduced

Major classification societies have rules to guide the design of concrete floating structures. Their structural integrity when designed to the rules is unquestionably acceptable to underwriters.

The Condeep series of drilling and storage rigs include some of the largest and heaviest man-made floatable structures. As the name suggests, they are made in concrete and first went into operation in 1975. The structure's enormous weight with its 245,000 m^3 of concrete and 100,000 tons of steel reinforcement would have defeated many civil engineers tasked with producing a construction plan.

Floating Dormitories

In late 2019, the world was hit by a new virus that today has claimed millions of lives and infected more than 140 million people. Millions faced economic hardship and are in despair. Even as the end is nowhere in sight, public health experts are warning of a more deadly disease called Disease X.

Figure 4 Condeep platforms were the innovation of the Norwegians. Such structures did not require shipyard facilities for their construction. Their enormous weight would be too much for any drydock floor to bear

In Singapore, one of the most vulnerable groups is the foreign workers who live in crowded dormitories. In May 2020, I suggested through an op-ed piece in the Straits Times that dormitories be built on

floating islands that will not face the tight space constraints that those on land are facing. Also, as

floating dormitories are movable it is always possible to site them close to major construction centers. This would reduce workers' commuting time to workplaces and their interaction with the Public.

The piece attracted public censure on the grounds that housing workers in the sea was unacceptable, insensitive, and callous and many may suffer from motion sickness.

Such reaction reflects the public misconception that life on a floating island must necessarily be stressful, restrictive, and boring. But nothing is further from the truth. What we proposed was dormitories erected on three concrete islands linked in the center to another island where residents may congregate, socialize, and participate in sport and cultural activities as well as for meals as illustrated in Figure 5.

Figure 5 The proposed floating dormitory features a central core for social interaction, sports activities, and for meals. The dorm can be moved as needed to be close to the workplace of the residents

Each complex which will have 2500 beds is estimated to cost $25 million. The shipyards in Singapore can mobilize to supply five to ten such identical units. The design will be classed. The concrete platforms may be built in Batam, Karimun, or Johor. The containerized cabins can be procured from China fully outfitted with toilets, lockers, and beds, shipped to Singapore for integration.

Could this be a project that the government is seeking under its Industry Transformational Map initiative? SNAMES or the Association of Singapore Marine Industry (ASMI) would be welcome to discuss with the author to work out how best to advance the idea to the authorities. Floor plans and more artist impressions including a video are available on request from the author.

Concluding Remarks

The shareholders of the two largest shipyards in Singapore have announced that they will exit the industry.

The government has called for the industry to transform itself. It offers the vision that the future could lie in LNG. However, our shipyards will be competing with others in the world with one hand tied behind their backs.

Our labor, land, and utilities are among the most expensive in Asia. We import 70 percent of the cost of a typical ship or rig building project. We depend too heavily on foreign workers and Covid-19 shows the impact of relying on workers who have to live in cramped dormitories. The brightest and the best have left the industry.

Instead, the professionals in shipyards and the supporting services should consider applying their expertise and knowledge to creating space for the nation. In the past, space has been created exclusively by land reclamation and lately by poldering. A number of reasons compel us to consider the floating option.

Naval architects and marine engineers have the wherewithal to offer floating islands as the third and vastly superior option. They are the only

group of professionals in the country who intimately understand floating structures, and who are able to design, build and commission them.

The market to satisfy our domestic need for more space is huge, in monetary terms larger than the value of all the rigs we exported in the last ten years. However, do not expect the government to offer that opportunity on a silver platter. The thought has yet to reach their mind. Action is needed from the industry itself.

The Straits Times on 22 April carries several pages of observations about rising sea levels and how to overcome the challenge. It is clear that floating solutions have yet to enter the minds of these experts looking at the problem, not surprisingly as none are marine engineers or naval architects.

My concern also goes to the professors and students in the polytechnics and universities who are pursuing shipyard-related subjects. They need to be imbued with an exciting vision of a fruitful transformation of the industry. If the seniors in the industry fail to do so, many of them will quit their course.

So, let us not scrape the barrel for more work in the offshore and marine industry, but strike a new path with your existing skills. Floating islands can be as fulfilling professionally as offshore oil rigs and FPSOs. They are needed to combat issues related to the degradation of the environment as well as rising sea levels. Let us make Singapore a Centre of Excellence for Floating Solutions.

Reference

1. Lim Soon Heng, Seascape the Landscape of Singapore, Repurposing Land in a Land Scarce Nation, WCFS2019: Proceedings of the World Conference on Floating Solutions pp. 385-410, Springer Nature Singapore (2020)

2. S. B Wetmore The Concrete Island Drilling System: Super Series (Super CIDS), pp OTC-4801-MS Offshore Technology Conference Houston Texas, May 1984

3. Lim Soon Heng, Jacopo Buongiorno, Singapore's Energy Dilemma: Would the Nuclear Option help? The HEAD Foundation, April 2018

4. Sugeng Wiwanto et al, Hybrid Floating Structures Case Study: Marisco's Floating Dry Dock, Proceedings of the International Conference on Civil, Offshore and Environmental Engineering Pp 325 -334 Springer Nature.

5. William Otto et al, WCFS2019: Wave Induced motions of a Mega Island, WCFS2019 Proceedings of the World Conference on Floating Solutions pp. 173-190, Springer Nature Singapore (2020)

6. Torgeir Moan et al, Floating Bridges and Submerged Tunnels in Norway, The History and Future Outlook, WCFS2019: Proceedings of the World Conference on Floating Solutions pp. 81-111, Springer Nature Singapore (2020)

7. Kwang Hoe Jun et al, Design and Construction of the Floating Concrete Harbor Incheon, WCFS2019 Proceedings of the World Conference on Floating Solutions pp283-298 Springer Nature Singapore (2020)

8. Aditya Sankalp et al, WCFS2019: Mooring System for Very Large Floating Structure, Proceedings of the World Conference on Floating Solutions pp. 253-274, Springer Nature Singapore (2020)

9. Bahador Sabet Divsholi, Durability of Floating Concrete Platforms, WCFS2019: Proceedings of the World Conference on Floating Solutions pp. 275-282, Springer Nature Singapore (2020)

10. Haicheng Zhang et al, Dynamics of Super-Scale Modularized Floating Airport, WCFS2019: Proceedings of the World Conference on Floating Solutions pp. 113-134, Springer Nature Singapore (2020)

Chi Zhang, Allan Magee, et al, Hydrodynamic Response and Loads of a Model Floating Hydrocarbon Storage Tank System, pp. 155-172 WCFS2019: Proceedings of the World Conference on Floating Solutions pp. 113-134, Springer Nature Singapore (2020)

Authors Biography

Mr. Lim Soon Heng, a mechanical engineering graduate of the National University of Singapore. He is a Fellow of the IMarEST.

Joining the industry in 1968, he is one of the pioneers of the Singapore marine industry. His expertise ranges from shipbuilding to the feasibility assessment, planning, and design of shipyards across several countries around the world.

He founded the Society of Floating Solutions (Singapore) in 2017, initiated the First World Conference on Floating Solutions, and advised the organization of the second World Conference on Floating Solutions in Rotterdam in October 2020.

He is an avid believer that mega floating structures are the best way to mitigate the threat of rising seas, and climate change and leave a smaller carbon footprint than polders.

He opposes the practice of land reclamation with imported sand for the harm it does to the livelihood of others and to coastal marine life.

As President of the Society, he has engaged key officials of the Singapore government, encouraging them to be more receptive to floating solutions and share with them their inherent benefits compared to land reclamation.

Challenges in Meeting Upcoming EEXI Requirement

Shukui Liu(1), Baoguo Shang(2), Joo Hock Ang(3), Jun Jie Tan(4)

(1)Nanyang Technological University, skliu@ntu.edu.sg
(2)Marine Design and Research Institute of China, shbg708@163.com
(3)Sembcorp Marine Integrated Yard, joohock.ang@sembmarine.com
(4)Sembcorp Marine Integrated Yard, junjie.tan@sembmarine.com

Abstract

The adoption of the Energy Efficiency Existing Ship Index (EEXI) is targeted to make newer ships more energy-efficient than older ships on the market, thus, enable the acceleration of global fleet replacement to support IMO's maritime Green House Gas (GHG) reduction strategy. This article first reviews the rapid development and endorsement of the EEXI at International Maritime Organisation (IMO) as a new requirement to cut the carbon intensity of existing ships. Secondly, it highlights the high percentage of non-compliance of the existing world fleet which requires equal, if not higher, attention as compared to the Energy Efficiency Design Index (EEDI). Finally, it reviews the various measures that can be adopted to improve the EEXI performance of a ship, followed by a critical discussion on the technical issues in implementing the EEXI, such as extending the use of Engine Power Limitation (EPL), minimum propulsion power assessment, power reserve, and determination of reference speed.

Keywords: Energy Efficiency Existing Ship Index (EEXI), Energy Efficiency Design Index (EEDI), Green House Gas (GHG), Decarbonisation

1. The Development of EEXI

The concept of EEXI, namely, Energy efficiency Existing Ship Index, was first put forward in Feb 2019 at MEPC 74 by Japan (MEPC74/7/2). This new index serves as a possible approach for the reduction of GHG emissions from international shipping in the short term and a regulatory measure on the energy efficiency of existing ships based on existing IMO instruments. This is expected to contribute to the 40% carbon intensity reduction target by 2030, as compared to 2008. The rationale of introducing this index is that those existing ships, including pre-EEDI ships, feature higher engine power and lower cost while producing more GHG emissions than those new ships, which have lower engine power and require higher investment. Consequently, the EEDI compliant new ships are deemed to be less competitive on the market as they often feature lower speed, resulting in a situation that older ships have stronger market power than new ships. Therefore, there is a lack of incentive for fleet replacement. The EEXI can hence serve as a remedy for this issue and help to improve the overall operational efficiency of existing ships.

in Nov. 2019, Japan and Norway submitted ISWG-GHG 6/2/3 and provided a revised proposal for goal-based energy efficiency improvement measure utilizing EEXI, which refines the initial proposals on EEXI submitted by Japan (MEPC 74/7/2) and Norway (ISWG-GHG 5/4). An initial impact assessment concluded that the proposed EEXI has positive impacts on the reduction of GHG emissions and voyage cost, and overall transport cost could be reduced. In this context, interested IMO member states and non-governmental organizations formed an informal group, and 20 developed draft legal instruments to incorporate the EEXI measure into MARPOL Annex VI as a goal-based measure through a technical approach (ISWG-GHG 7/2/6, Feb. 2020). During MEPC 75 in November 2020, IMO approved the draft amendments to MARPOL Annex VI. Subject to adoption at MEPC 76 session in June 2021, the requirements will enter into force in 2023.

This EEXI will impose a requirement equivalent to EEDI Phase 2 or 3 (with some adjustments) to all existing ships regardless of the year of build and is intended as a one-off certification (ISWG-GHG 7J5Rev.1, 2020). Following this regulation, a ship that is compliant with GHG emission index EEDI when constructed may become non-EEXI-compliant, which essentially broke the Grandfather Clause - a provision where an old rule continues to apply to some existing situations while a new rule will apply to all future cases. Therefore, an extensive discussion has been stimulated in the maritime sector. As pointed out, with the introduction of EEXI, IMO intends to level the playing field by matching the efficiency of both existing and new ships- where newer ships will become more competitive on the market and replacement of older ships to be accelerated, so as to support the IMO's decarbonization strategy.

2. Calculation of EEXI

According to ISWG-GHG 7/2/7, the formula to calculate attained EEXI follows the basic structure of the EEDI formula and takes the form as follows:

$$EEXI\left(\frac{g}{t \times nm}\right) = \left[\left(\prod_{j=1}^{n} f_j\right)\left(\sum_{i=1}^{nME} P_{ME(i)} \cdot C_{FME(i)} \cdot SFC_{ME(i)}\right) + (P_{AE} \cdot C_{FAE} \cdot SFC_{AE}) + \left(\prod_{j=1}^{n} f_j \cdot \sum_{i=1}^{nPTI} P_{PTI(i)} - \sum_{i=1}^{neff} f_{eff(i)} \cdot P_{AEeff(i)}\right) \cdot C_{FAE} \cdot SFC_{AE} - \sum_{i=1}^{neff} f_{eff(i)} \cdot P_{eff(i)} \cdot C_{FME} \cdot SFC_{ME}\right] \Big/ f_i \cdot f_e \cdot f_l \cdot Capacity \cdot f_w \cdot V_{ref} \quad (1)$$

The form of the formula is the same as the EEDI calculation and the definition of each parameter is not presented here. Besides some subtle differences in the detailed definition, one noteworthy point is that EEDI calculation is often done by the designer and certified by classification societies, while the EEXI calculation is to be handled by shipowners, who may not possess all necessary design information of his/her ship. Thus, the first step for the shipowner is to compile all the necessary documents, such as EEDI technical file, if available. Otherwise, the following data/documents will be needed to support EEXI calculation:

- Report for ship speed/power trial
- Model test report(s), if any
- Stability booklet
- Nox technical files for both main engine(s) and auxiliary engine(s)
- Ship lightweight

3. Status of World Fleet Compliance

According to the estimation of BIMCO & RINA (ISWG-GHG 8-2, 2021), the regulation will likely affect around 30 000 existing ships, and possibly half of these ships (15,000) may require measures such as engine power limitation to comply with the EEXI requirements.

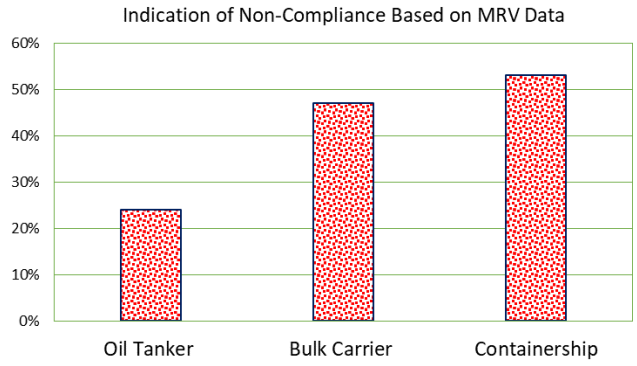


Figure 1 Non-EEXI-compliance of major types of cargo ships based on EU Monitoring, Reporting, and Verification (MRV) data.

Figure 1 shows the EEXI non-compliance of major types of ships based on the EEDI data recorded in the EC MRV system (Vergetis et al., 2020). According to this result, a significant portion of these major types of cargo ships does not comply with the EEXI requirement. It is noted that this result does not consider those ships which do not report their EEDI index. Other sources, such as Clarkson, also reported a very high ratio of non-EEXI-compliance of world fleet based on their database.

4. Measures to Meet EEXI Requirement

In the situation where the attained EEXI value is higher than the required EEXI value, the first action should be to search for original model test data and shop test data of the engine. This is aimed to replace conservative reference speed and standard values of the specific fuel oil consumption, as defined by the regulation. As experimental data are sometimes not available, data based on numerical simulations might be used, as drafted in the guidance.

If no better data is available, or even after applying the original test data, the attained EEXI value is still higher than the required EEXI value, then retrofitting measures can be considered to modify the design, as required. These retrofitting measures are discussed as follows.

i. SHaPoLi / Engine Power Limitation (EPL)

Shaft/Engine Power Limitation is expected to be the easiest means for existing ships to meet EEXI requirements. It should be noted that when EPL is employed, the Specific Fuel Oil Consumption (SFOC) used in the EEXI calculation can be SFOC at 75% of limited Maximum Continuous Rating (MCR). Another candidate is 87% of the limited MCR, noting that engine margins would be different in the application of Shaft/Engine Power Limitation. This is to be finalized in MEPC 76 (ISWG-GHG 7/2/7, 2020). When power reduction is significant, an assessment of the required minimum propulsion power should be conducted.

ii. Energy-saving devices (ESD)

This measure normally refers to the design and installation of various foils, appendages at the stern of the ship and/or around the propeller, as shown in Figure 2. The design of such devices is very delicate, often requires a highly customized case-by-case optimization study according to given hull/propeller/rudder conditions. More importantly, the validation of their effects is always very challenging, especially for the existing ship which is normally operated under not-so-ideal conditions.

Figure 2 Simplified Compensative Nozzle and rudder thrust fin (MARIC design) applied to a VLCC to improve propulsive efficiency.

iii. Bow optimization

This often refers to the optimization of the bow form of fast vessels such as containerships to achieve better resistance performance at a speed that is different from (lower than) what the ship was designed for initially. While the involved design and yard retrofitting work may not be significant, it may involve a sea trial or equivalent process required by the authority to ascertain the EEXI index.

iv. Air lubrication system

Air lubrication system, as shown in Figure 3, is an effective technology that does not involve significant modification of the ship structure and propulsion system, thus can be conveniently applied. For justifying the use of such a system, a critical examination of the required energy to pump air into water as well as resistance that can be reduced is needed. This technology is normally applied to containerships, LNG carriers, and cruise ships, etc, which features a smaller draft and wide flat bottom surfaces.

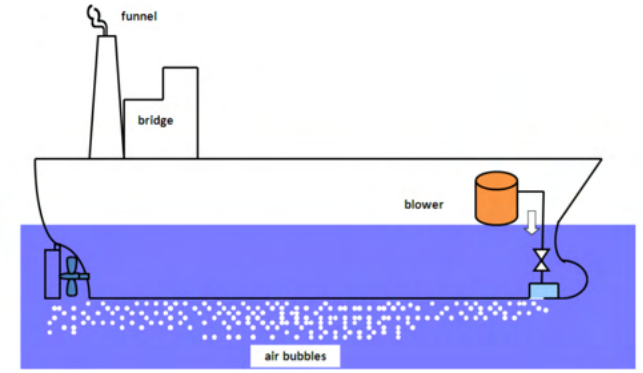


Figure 3 Schematic illustration of an air lubrication system (IMO MEPC.1/Circ. 815)

v. Wind assistance system

Recent years have seen much research and advance in the rotor sail system exploiting the Magnus effect, see Figure 4. This technology is attractive for ships with large deck space. Major considerations include environmental conditions and route settings, in addition to the retrofitting cost.

Figure 4 Installation of rotor sail system on a ship (picture by Jamieson Aberdeen, licensed with CC BY 2.0)

vi. High-Performance Coating

In the case where the applied painting post-newbuilding (during dry-dock) is more efficient than what was applied during new building, a sea trial may be conducted following an

approved procedure to establish a new speed-power relationship for the EEXI calculation. This is an effective measure that can improve the speed-power performance of a ship and does not require any design modification. Besides its positive effect on the attained EEXI value, it can also significantly improve the operational index Carbon Intensity Indicator (CII).

vii. Alternative Fuels

This refers to the use of low carbon alternative fuels, such as LNG, whose equivalent carbon content is lower and can readily reduce the EEXI index by 20%. Though there are serious concerns that the use of LNG as a fuel will shift the emission from marine industry to land-based industry and does not effectively contribute to global decarbonization (Speirs et al., 2019), many new-building vessels are still implementing as a transitional measure. For existing ships, the involved effort and cost are often too complicated to implement for the purpose of improving the EEXI index only.

viii. Engine Derating and Propulsion Optimisation

Engine derating and propeller resizing is not a convenient choice as it affects the design and operation of the whole propulsion system including the shafting system, as well as the minimum propulsion power requirement. The scope and the extent of the design and retrofitting work are often too large and complicated.

ix. Deadweight Increase

Technically, as a major parameter involved in the EEXI calculation, the deadweight cannot be conveniently changed, as it is the foundation of the whole ship structure and hull form design.

5. Key Discussions and Considerations

i. Although various technologies are available, the shipowner needs to consider the required investment in detail. In most cases, techno-economic analysis needs to be conducted on a vessel-to-vessel basis. This should be done considering also other ship performances, such as CII performance.

ii. Considering a large number of affected ships and a small window to implement, measures that involve the least design and retrofitting work are usually preferred.

iii. Considering the implementation of EEXI requires the attained energy efficiency index to reduce by about 20%, hydrodynamic retrofitting and innovative energy-saving measures cannot serve as the main solutions to achieve the target. The cost of retrofitting existing ships to use LNG as fuel is too high, and also may actually transfer the emission from the marine industry to other sectors. Thus, the limitation of engine power would practically be the most effective countermeasure, with other measures as supporting choices. Following the formula of calculating EEXI, if only the propulsion power of the main engine is considered,

$$EEXI \approx \frac{(P_{ME} \cdot SFC_{ME} \cdot C_{FME})}{Capacity \cdot V_{ref}} = C \cdot \frac{P_{ME}}{V_{ref}} \propto V_{ref2} \propto P_{ME2/3} \quad (2)$$

namely, the energy efficiency index is proportional to PME2/3. Therefore, to improve the EEXI by 20% only through reducing the installed power, 28% of power reduction is required. It has been reported that some pre-EEDI bulkers may require up to a 45% reduction of the installed power to comply with EEXI requirements. Such a significant reduction of the installed power will affect the speed performance of a ship in service conditions where fouling is a normal phenomenon (I-TECH,

2020) and make the subject vessel less competitive in the chartering market. Further, to have an engine continuously operate at such a low speed is very demanding from the view of engine management. Thus, from an owner's perspective, achieving the required EEXI index by purely limiting engine power is not the optimal choice when significant GHG index reduction is required. Instead, the power needs to be carefully determined to balance the EEXI requirement and ship speed performance. Ideally, it should be implemented concurrently with other measures.

iv. Minimum Propulsion Power Assessment

In line with IMO's regulatory framework, ships complying with EEDI requirements set out in regulations on energy efficiency for ships should have sufficient installed propulsion power to maintain the maneuverability in adverse conditions, as regulated currently by the 2013 Interim Guideline 1. To incorporate the goal-based energy efficiency improvement measure utilizing EEXI, in cases where the SHaPoLi / EPL system is applied and NOX critical settings are altered beyond what is allowed by the engine technical file, the engine would need to be re-certified. In such case, for an EEDI-certified ship where the SHaPoLi /EPL system is applied at a power below that is required by regulation 21.5 of MARPOL Annex VI (minimum power requirement), the certified engine power should be set at the power satisfying that requirement.

Another issue is related to the Interim Guideline itself, which assesses the ship's performance in operational conditions without considering the imperfection or fouling of the hull and propeller surfaces. That means, even ships that pass the assessment may still encounter such critical scenarios that they are unable to maintain manoeuvrability. This is particularly true for existing ships in operation (Liu et al., 2021). How can we then ensure a ship's safe navigation? Last but not least, as the 2013 Interim Guideline is under revision and many delegations already agreed to define the "adverse condition" to even worse condition, it appears that the new criteria will be more stringent.

v. Use of Power Reserve

Following ISWG-GHG 7/2/7, the power reserve can be triggered only under conditions referring to the regulation 3.1 and 21.5 of MARPOL Annex VI, including avoidance of occasions that may endanger safety (e.g. hurricanes, pirates) and sailing in ice-infested waters requiring the use of more than limited power for safe operation. Any use of a power reserve should be recorded in the Management Plan for SHaPoLi/EPL. It should be noted that 21.5 of MARPOL Annex VI refers to maintaining maneuverability in adverse conditions. It essentially concerns the torque availability of an engine at slow RPM and has little to do with the release of power limitation.

One concern refers to article regulation 3.1 in terms of "any emission necessary for purpose of securing the safety of a ship". When a ship navigates in harsh seaway conditions that do not reach the criteria defined as "adverse condition", but the ship is not able to maintain its course and is in danger of collision or grounding, will the ship be still allowed to use the power reserve? There seems to be some inconsistency in practice. And, as of now, no penalty for the misuse of power reserve is specified.

vi. Determination of Reference Speed

For EEXI calculation, it is necessary to determine the reference speed (Vref) at a certain draft of the

1 Note that the Interim Guideline is under discussion by an IMO Correspondence Group with a view to finalizing the revision, see MEPC 76/5/1.

vessel. From shipowners' perspective, for many existing ships subject to the EEXI assessment, they may not be able to supply compliant model test results at the required draft (BIMCO estimates there could be as many as 5,000 – 10,000 ships with inadequate documentation from the original sea trial). And building a model and conducting towing tank tests only for the purpose of screening EEXI of the entire fleets is not practical. Therefore, the EEXI calculation guideline offers the option to calculate reference speed using an approximate formula for the ship type and installed power. With an included margin factor of 5%, this approximated reference speed will be conservative. As this 5% conservativeness may become very critical in certain cases, and unfair particularly for well-maintained ships, various parties are discussing alternative methods, for instance, as proposed by BIMCO and RINA (2021).

Another controversial point in relation to this point is the acceptance of the CFD approach in such a regulation. CFD is known to be non-transparent, thus, "expertise" in CFD simulations does play a role in producing reliable results. In addition to the fact that it needs a careful set-up ship model that considers ship geometry, how can classification societies effectively examine and approve/certify the calculation based on CFD simulations? Further, some of the classes are already offering such advisory services to the industry. Then, another question arises, how can an organization offer such service and approve their own results? Is there any measure to avoid potential conflict of interest?

6. Conclusion

The introduction of new regulation EEXI and apply to all existing ships broke the Grandfather Clause, which means that a new regulation is applicable to new cases only. This demonstrates IMO's strong determination to reduce GHG emissions in shipping. The new regulation will affect many ships and across multiple maritime stakeholders. The entire maritime industry needs to get ready to effectively respond to this new IMO's requirement.

Though the regulation on EEXI is still under discussion and decisions to be made at MEPC 76 in June 2021, this article discussed, based on the latest developments and opinions of involved stakeholders, the technical challenges and uncertainties in calculating the EEXI index. Secondly, potential practical measures to support shipowners to meet the EEXI requirement are described, and several regulatory procedural issues and uncertainties are also pointed out, which may help relevant stakeholders to make the best decision at the earliest possible stage.

While this article highlighted the various technical issues encountered in calculating the EEXI and the challenges in searching for the most practical way of meeting the according to requirement, we should keep in mind that the introduction of EEXI is essentially to make newer ships more competitive than older ships on the market, and as a result, accelerate the global fleet replacement and to support the IMO's maritime GHG reduction strategy. In this respect, all these technical solutions are transitional and temporary. The ultimate goal is to design, construct and deploy greener ships contributing to a lower-carbon future.

Acknowledgement

This study is partly conducted within the project of "Prediction of the added resistance of a ship in seaways for the rational determination of installed power" financially supported by Sembcorp Marine Lab Fund.

References

Vergetis E., Matthew W. and Chris C. (2020) "GHG emissions regulation: examining the outcomes of MEPC 75". Lloyd's Register webinar.

International Maritime Organization (2013). "Interim Guidelines for Determining Minimum Propulsion Power to Maintain the Manoeuvrability in Adverse Conditions", MEPC. 232(65), London, UK

International Maritime Organization, MEPC 71/INF.28. 2017. "Draft revised guidelines for determining minimum propulsion power to maintain the manoeuvrability of ships in adverse conditions", London, UK.

International Maritime Organization, MEPC 73/5/1. 2018. "Proposal for an option to limit the shaft power while ensuring a sufficient safety power reserve in adverse weather conditions", London, UK.

International Maritime Organization (2020). Draft guidelines on the Shaft / Engine Power Limitation system to comply with the EEXI requirements and use of a power reserve, ISWG-GHG 7/2/7, Retrieved from https://docs.imo.org

International Maritime Organization (2020). Draft guidelines associated with draft amendments to MARPOL Annex VI to incorporate the goal-based energy efficiency improvement measure utilizing Energy Efficiency Existing Ship Index (EEXI), ISWG-GHG 7/2/7, Retrieved from https://docs.imo.org

International Maritime Organization (2021). ISWG-GHG 8/2 Comments on draft guidelines associated with EEXI (Submitted by BIMCO-RINA), Retrieved from https://docs.imo.org

International Maritime Organization (2021). MEPC 76/5/1 Report of the Correspondence Group on Air Pollution and Energy Efficiency (Submitted by Japan, Pre-session public release). Retrieved from https://docs.imo.org

International Maritime Organization. (2020). Elements to Be Added in The MEPC Resolution Accompanying the Draft Amendments (ISWG-GHG 7J5Rev.1). Retrieved from https://docs.imo.org

I-TECH. (2020). "Quantifying the scale of the barnacle fouling problem on the global shipping fleet", https://selektope.com/whitepapers/, accessed on 10 Oct 2020.

Liu S., Papanikolaou A. Bezunartea-Barrio A., Shang B.G. and Sreedharan M. (2021). On the Effect of Biofouling on the Minimum Propulsion Power of Ships for Safe Navigation in Realistic Conditions. Journal of Biofouling.

Speirs J., Balcombe P., Blomerus P., Stettler M., Brandon N., and Hawkes A. Can natural gas reduce emissions from transport? Heavy goods vehicles and shipping; Sustainable Gas Institute, Imperial College London. January 2019

Authors Biography

Dr. Liu Shukui is a graduate of Harbin Engineering University (B.Eng. & M.Eng. in Naval Architecture and Ocean Engineering). He completed his Ph.D. research on the seakeeping

subject at the National Technical University of Athens in 2011. Currently, he is a lecturer at Nanyang Technological University. His scientific interests cover the fields of ship hydrodynamics, including in general the resistance, propulsion, seakeeping, manoeuvering subjects, and their impacts on ship design and operation. His work on added resistance in waves has been adopted by the ITTC procedure on analysis of speed/ power trials. He is a member of SNAME.

Mr. Shang Baoguo obtained his BEng in Naval Architecture and Ocean Engineering from Harbin Engineering University and MEng from Shanghai Jiao Tong University. He has been working at the Marine Design and Research Institute of China since 2003 and currently serves as a senior expert, mainly involved in the design of merchant ships. He is the chief designer of more than ten types of tanker ships.

Dr. Ang Joo Hock is currently a senior manager in Research and Development (R&D). He joined Sembcorp Marine in 2001 and was involved in various functions such as production (hull), project management, and engineering design.

He obtained his BEng (Hons) in Naval Architecture and Ocean Engineering from the University of Strathclyde, MSc in Management of Technology from the National University of Singapore, and Ph.D. in Mechanical Engineering from the University of Glasgow. He is currently leading the development of sustainable innovation and solutions, including decarbonization and digitalization. He currently serves as a technical chairperson in SNAMES (Singapore) and also an associate member of RINA (UK).

Mr. Tan Jun Jie has obtained his Masters of Science in Marine Technology with Merit from the University of Newcastle upon Tyne (UK & Singapore) and has graduated from the Universities of Glasgow and Strathclyde (UK) with a Bachelor of Engineering in Naval Architecture with Ocean Engineering with First Class Honours. Previously, he studied Advanced Diploma inv Ship & Master Technology as well as Diploma in Marine and Offshore Technology in Ngee Ann Polytechnic (Singapore). Currently, he is working with Sembcorp Marine as an R&D Manager. He has also co-published the paper, "CFD Analysis on Gas Flow and Droplet Dynamics within Exhaust Gas Scrubbers"

Application of Artificial Intelligent on Cargo Identification during Port Tally

Johnson Zhu

Asia Intelligence Technology Pte. Ltd, Tele: +65 8111 2062, service@aitechnology.ai

Abstract

Work efficiency and productivity of port tally have been of high importance to achieving and maintaining the first level of the international marine hub, especially for a steel cargo hub.

This study explored and applied the front-edge Artificial Intelligent (AI) technique to identify the steel cargo categories automatically upon its lifting from the cargo-hold of vessels. For the application of Artificial Intelligent, object detection of Computer Vision (CV) has been utilized to identify nine (9) categories, such as rebars, coils, plates, pipes, structural steel, etc. In this application, we propose the first anchor-free and NMS (non-maximum suppression)-the free object detection model, called weakly supervised multimodal annotation segmentation (WSMA-Seg), which utilizes segmentation models to achieve an accurate and robust object detection without NMS.

To overcome the telecommunication barrier of steel ship-body, we propose a novel solution during edge identification. The whole solution works well as a phototype testing after the arrangement of the camera angles on-site, which were introduced in this work as well.

Keywords: Artificial Intelligent, Steel Section Identification, Port terminal Gas (GHG), Decarbonisation

1. Introduction

Singapore is the busiest port in the world in terms of shipping tonnage, with more than 130,000 vessel calls annually. In the year of 2020, Singapore won once again the world's premier maritime hub after topping the Xinhua-Baltic International Shipping Centre Development (ISCD) index. It has been reported that Singapore had retained the top spot for the 7th year in a row, beating London, Shanghai, Hong Kong and Dubai. The city-state, Singapore, earned its place due to its favorable geographical location, shipping industry ecosystem and supportive government policies. Furthermore, the detailed and in-time application of front-edge technology is a key point for this achievement.

To offer reliable and efficient cargo handling, Singapore is keen to apply the most advance Artificial Intelligent (AI) technique to enhance the efficiency of the port.

In the present highly competitive world economy, all customers seek fast, low cost, efficient and reliable shipping of cargo between

busy ports. In response to these demands, port terminals are automating their handling processes and investing in high-tech loading and unloading equipment. This is in the ports' best interests since it allows them to improve efficiency by minimizing the amount of time that ships are docked in the berths. High efficiency will also allow the consigner to fetch their cargo as earlier as possible. To enhance efficiency, Computer Vision (CV) is a hot technique in all Artificial Intelligent (AI) technologies that are already to apply in port.

In this study, the algorithm for steel category identification by Computer Vision (CV) has been detailed and the CV identification on cargos follows.

2. Computer Vision Algorithm using Segmentation

Object detection in images is one of the most widely explored tasks in computer vision. To detect the steel category in the ship cargo hold, image data of the following steel categories have been collected in one of the Ports in Singapore:

- wire coils
- rebars
- I&H beams
- angled beams,
- plates
- cold/hot rolls
- piles
- wood
- Damaged/undamaged containers

If we apply the current deep learning approaches, eg the R-CNN method, to solve the steel detection, it will mainly rely on region proposal mechanisms (e.g., region proposal networks (RPNs)) to generate potential bounding boxes in an image and then classify these bounding boxes to achieve object detection. This mechanism can generally achieve a good detection performance under ideal circumstances such as being in the lab, their recall in port or in the ship cargo hold will encounter two challenges:

1. The performance of proposal mechanisms on steel category will highly depend on the purity of steel boundary; however, the annotated steel boundary in port or ship cargo hold usually contains much more environmental noise than those being in the lab. This inevitably increases the difficulty of model learning and decreases the resulting confidence scores of steel categories, which consequently weakens the detection performance.
2. Non-maximum suppression (NMS) operations are used in region proposal mechanisms to select steel sections by setting an intersection over the union (IoU) threshold to filter other steel boundaries, such as the forklift and the truck in port

In this regard, this paper invokes a weakly supervised multimodal annotation segmentation (WSMA-Seg) method with segmentation models to achieve an accurate and robust steel detection without NMS. This method consists of two phases, a training phase and a testing phase for steel categories. In the training phase, WSMA-Seg first converts weakly supervised steel boundary annotations in detection tasks to multi-channel segmentation-like masks, called multimodal annotations; then, a segmentation model for steels will be trained using multimodal annotations as labels to learn multimodal heatmaps for the training steel images captured in an international Port in Singapore. In the testing phase, the resulting heatmaps of a given test steel image are converted into an instance-aware segmentation map based on a pixel-level logic operation; then, a contour tracing operation is conducted to generate contours for steels

using the segmentation map; finally, steel bounding boxes are generated as circumscribed quadrilaterals of their corresponding steel contours.

2.1 Weakly Supervised Multimodal Annotation Segmentation

To apply Weakly Supervised Multimodal Annotation Segmentation (WSMA-Seg) for steel detection will be illustrated in this section. WSMA-Seg generally consists of two phases: a training phase and a testing phase. In the training phase, WSMA-Seg first converts the weakly supervised steel boundary annotations to pixel-level segmentation-like masks with three channels, representing interior, boundary, and boundary on interior masking information of all steel categories, respectively; the resulting annotations are called multimodal annotations; then, multimodal annotations are used as labels to train an underlying segmentation model to learn corresponding multimodal heatmaps for the training steel images. In the testing phase, the given testing image will be sent into the well-trained segmentation model to obtain multimodal heatmaps for steel After that, the resulting three heatmaps are converted into an instance-aware segmentation map based on a pixel-level logic operation; At last, a contour tracing operation for steels is conducted to generate contours for steel categories using the segmentation map, and the steel boundaries are created as circumscribed quadrilaterals of their contours to exclude the affecting of the ship cargo hold.

2.2 Generation of Multimodal Annotations

To annotate all-steel categories, we choose a methodology to automatically convert steel boundary annotations to segmentation-like multimodal annotations on pixel-level. As found in previous research [1, 2] that pixel-level segmentation information is not fully utilized by segmentation models for steel categories in a complex environment. Therefore, we propose that well-designed pixel-level segmentation annotations may not be essential to achieve a reasonable performance for steel detection; rather, pixel-level geometric annotations should be sufficient in the port application. Moreover, to generate a bounding box for the steel category in the image, an instance-aware segmentation is required; to achieve this, multimodal annotations are designed to have multiple channels to introduce additional information for all steel categories as well as common steel type in port tools.

As shown in Fig 1, multimodal annotations for steels utilize three channels to represent pixel-level masking information regarding the interior, the steel boundary, and the boundary on the interior of geometries of the ship cargo hold. These three different pixel-level masks are generated in the steps as below:

Step 1: Given a steel image with steel bounding box annotations, an inscribed ellipse for each steel bounding box will be obtained.

Step 2: We will achieve the interior mask (channel 0) by setting the values of pixels on the edge of or inside the ellipses to 1, and setting the values of other pixels to 0.

Step 3: We will obtain the steel boundary mask (channel 1) by setting the values of pixels on the edge of or within the inner width w of the ellipses to 1, and setting the rest to 0.

Step 4: In a similar manner, the boundary on the interior mask (channel 2) is generated by setting the values of pixels on the edge of or within the inner width w of the area of the elliptical overlap to 1.

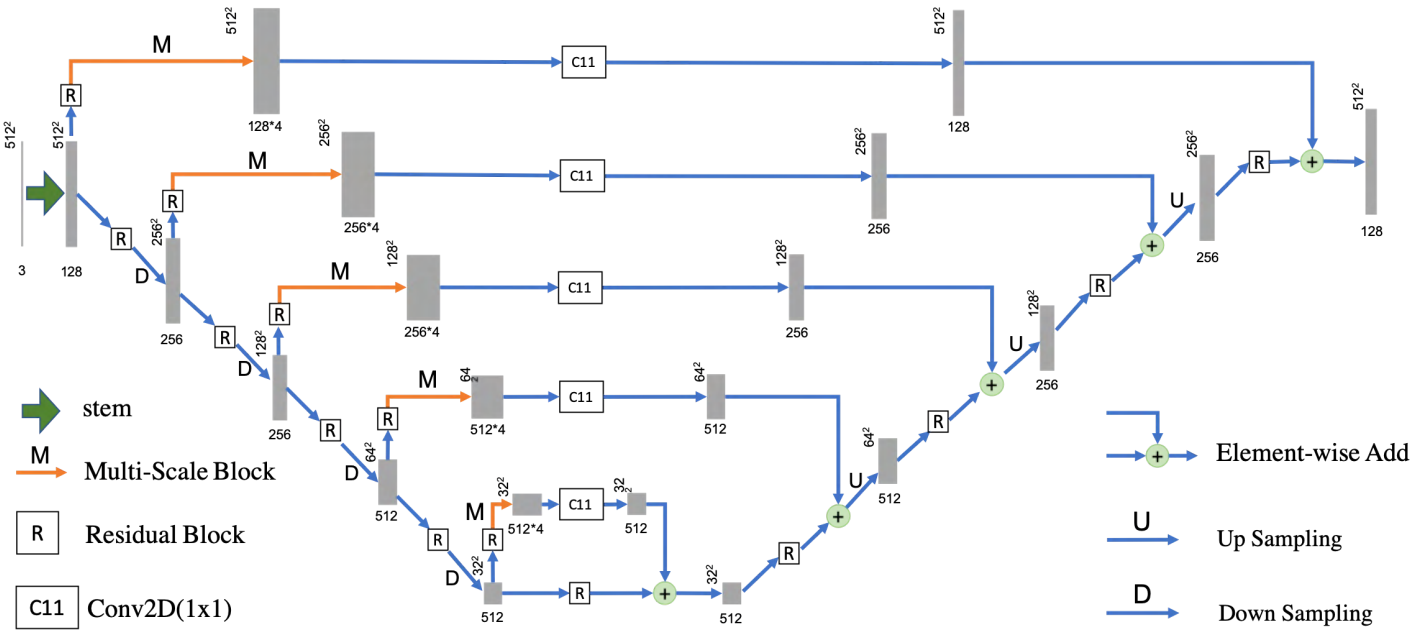


Figure 1 Multi-scale pooling segmentation model.

2.3 Steel Detection by Segmentation and Contour Tracing

Since we have obtained a well-trained segmentation model for the steel categories, the model is now capable of conducting steel detection. As shown in Fig 2, given a test steel image as the input of the segmentation model, WSMA-Seg first generates three heatmaps, i.e., interior, boundary, and boundary on interior heatmaps, which are denoted as I, B, and O, respectively. These three heatmaps are then converted to binary heatmaps, where the values of pixels in the interested area are set to 1, and the rest is set to 0. This conversion is conducted following the approach in [1]. Furthermore, a pixel-level operation, $I \oplus (B \wedge O)$, is used to merge three heatmaps into an instance-aware segmentation map.

At last, a contour tracing operation is conducted to generate contours for steels using the instance aware segmentation map, and the bounding boxes of steels are created as circumscribed quadrilaterals of their steel contours. One conventional way to trace a contour is to use a scan-based-following algorithm [2].

However, in the case of a large image with many steel categories, the scan-based-following algorithm is very time-consuming. To enhance the running efficiency, a modified run-data-based (RDB) following algorithm has been proposed. This modified RDB mothed remarkably reduces the computing time and memory costs of the contour tracing operation. The pseudocode of the RDB following algorithm is shown in Algorithm 1. Different from the pixel-following algorithm that requires to scan the entire steel image to find the starting point and tracing contour pixels along the clockwise direction to generate the results recurrently, the RDB method only needs to save two lines of pixel values and to scan the whole image once. Thus, this method will reduce the computer memory and therefore save the computer resources.

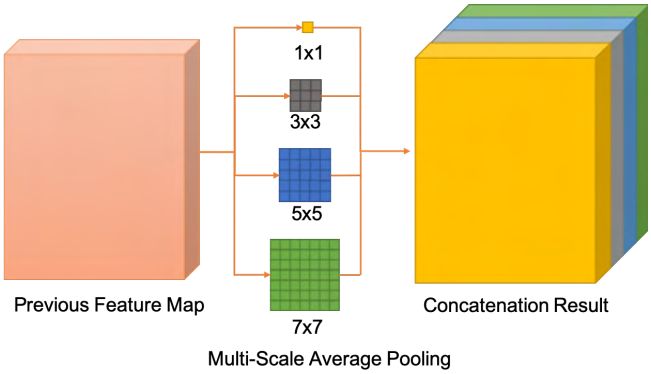


Figure 2 Multi-scale block sequence during training

Algorithm 1 Run-data-based following algorithm

Input: A binary image with h (height) and s (width). Output: A list of contour sets.

1: ledge = null, redge = null
2: for j in [0 : h) do
3: for i in [0 : s) do
4: if pixel(i,j) == 1 and pixel(i − 1,j) == 0 then
5: ledge = Pixel(i,j)
6: end if
7: if pixel(i,j) == 1 and pixel(i + 1,j) == 0 then
8: redge = Pixel(i,j)
9: end if
10: if redge != null and ledge != null then
11: if there exists a pair of redge0 and ledge0 in row j − 1 and

12: $\left|x_{coordOf}(l'_{edge}) - x_{coordOf}(l_{edge})\right| \leq 1$ and

13: $\left|x_{coordOf}(r'_{edge}) - x_{coordOf}(r_{edge})\right| \leq 1$ then

14: Add ledge and redge to the same contour set as redge0 and ledge0
15: else
16: Creat a new contour set and add ledge and redge to it
17: end if
18: redge = null and ledge = null
19: end if
20: end for
21: end for

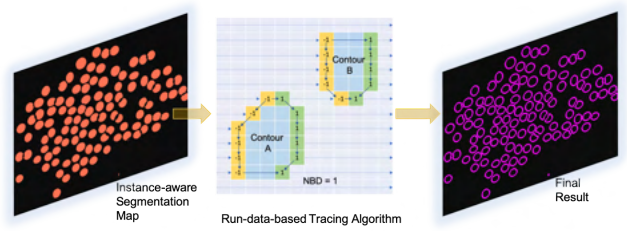


Figure 3 contour tracing examples for training

2.4 Implementation of Steel Detection

The AI algorithm in sections 2.2 & 2.3 have been programed and implemented for steel detection in Port in Singapore.

2.4.1 Steel Section Detection for Initial Testing

Two state-of-the-art anchor-based models, Faster R-CNN and Cascade R-CNN [1] are selected as the baselines for steel section identifications. Table 1 lists the detection performances of our proposed WSMA-Seg and baselines on this dataset. As shown in Table 1, the proposed method in this study with Stack = 2, Base = 40, Depth = 5 has achieved the best performance among all solutions in terms of F1 Score. The F1 Score is defined as 2*((precision*recall)/(precision + recall)).

In addition, the number of parameters needed for WSMA-Seg is much less than the baselines (only 1/7 of Cascade RCNN and 1/4 of Faster RCNN), while the number of training epochs for WSMA-Seg is also less than those of the baselines. Therefore, we are glad to draw the conclusion that, compared to the state-of-the-art baselines, WSMA-Seg is much more simplified, more effective, and more efficient in steel section detections. Figure 4 shows the detection of steel rebar with all rebar heads are successfully identified in an ideal environment, eg. in the lab. This algorithm is thus regarded as mature in an ideal environment for initial testing.

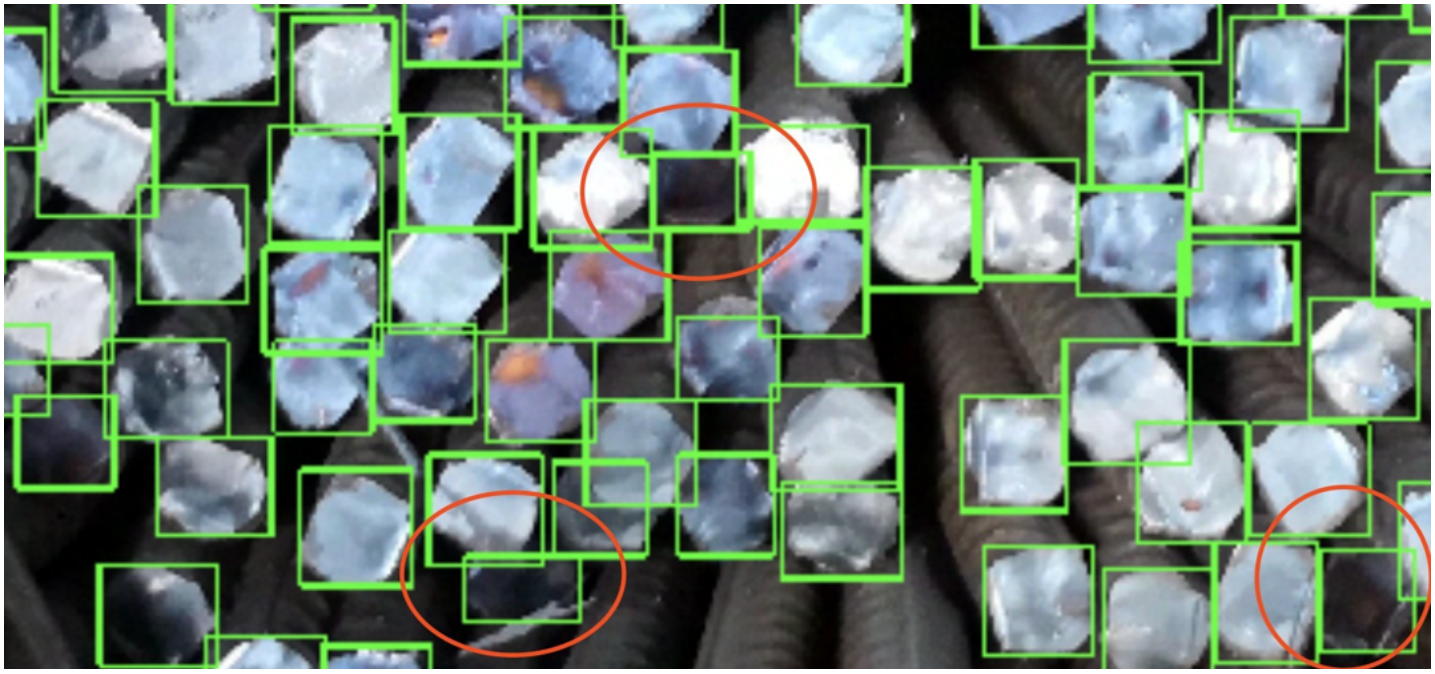


Figure 4 An example of complex occlusion in the Rebar Head dataset.

Table 1 Detection performances of WSMA-Seg and baselines on the Rebar Head dataset

Method	#parms	Epoch	F1 Score
Faster RCNN	23.2M	100	98.50%
Cascade RCNN [1]	42.1M	100	98.80%
WSMA-Seg (stack=1, base=72, depth=3)	6.1M	70	95.56%
WSMA-Seg (stack=2, base=40, depth=5)	5.8M	70	98.67%
WSMA-Seg (stack=4, base=28, depth=5)	5.7M	70	96.55%

For the parameter for WSMA-Seg, stack, base number and depth are of great concern during training.

2.4.2 Steel Section Detection for Practice

Although the initial testing in section 2.4.1 has illustrated to us the ideal usage in the lab, the algorithm needs to enhance so that we can apply it to the engineering practice. To fit for the environment in port, we have an improvement in performance considering the following factor

1) Image enhancement for Computer Vision on the dark image captured in the night
2) Exclusion of similar objects in the port, such as forklifts, equipment skids.
3) Adding the object detection of workers and lifting hook & lifting shackle
4) Identification of performance improvement due to the camera distance

The results of steel identification have been shown in Figure 5~7. The on-site testing of steel pipe identification during lifting has been illustrated in Figure 8.

Figure 5 Steel Section identification – steel pipes

Figure 6 Steel Section identification – steel bundles

Figure 7 Container criteria by IICL-6 (Institute of International Container Lessors)

2.4.3 Identification of Container Damage

We have also trained and tested the identification performance of container damage for the AI algorithm. The AI identification process has also referred to the **Guide for Container Equipment Inspection, 6th edition ("IICL-6")** issued by the Institute of International Container Lessors.

Figure 8 Container damage identification - Dent

Figure 9 Identification of wood in Port

Figure 10 Identification of ship near the Port

2.4.4 Identification of Ship and Wood

For more applications in port terminals, the AI algorithm has been extended to wood and ship detection as shown in figure 9 & Figure 10.

3. Conclusion

Computer Vision theory has been applied to the steel cargo categories and other objects in the port. In regard to the AI theory, we have developed and modified the WSMA-Seg theory to the following advantages: (i) as an NMS-free solution, WSMA-Seg avoids all hyperparameters related to anchor boxes and NMS; so, the above-mentioned threshold selection problem is also avoided; (ii) the complex occlusion problem can be alleviated by utilizing the topological structure of segmentation-like multimodal annotations; and (iii) multimodal annotations are pixel-level annotations; so, they can describe the steels and other cargo types more accurately and overcome the above-mentioned environment noise problem.

The AI algorithm is thus implemented for steel cargos and other objects in port terminals with all practical factors considered. The algorithm has been validated to be with high performance in identifying the following objects:

1) Steel Sections (wire coils, rebars, I-beams, angled beams, plates, angles, and C-channels)
2) Container number and container damage
3) Wood
4) Ships
5) Lifting hook and lifting shackles

Reference

[1] Common objects in context," in Proceedings of European Conference on Computer Vision, 2014.

[2] J. Dai, K. He, and J. Sun, "Boxsup: Exploiting bounding boxes to supervise convolutional networks for semantic segmentation," in Proceedings of the IEEE International Conference on Computer Vision, 2015.

[3] IICL, Guide for Container Equipment Inspection, 6th edition ("IICL-6") (September 2016)

Authors Biography

Dr. Zhu was awarded his Doctor Degree from Mechanical & Aerospace Engineering School of Nanyang Technological University in 2013. He started his career in ocean engineering and also service for port in Singapore. In 2018, Dr. Zhu created his own business to provide intelligent solutions for port terminals and vessels. The skills in Computer Vison of Dr. Zhu have been successfully applied in the operation and maintenance in port terminals and shipping industries.

A Cyber Risk Study in Shipboard OT Systems

Ruchitha Dumbala, Priyanga Rajaram, Mark Goh Voon Vei, Jianying Zhou

iTrust (Centre for Research in Cyber Security), Singapore University of Technology and Design, Singapore

Abstract

In recent times, the number of cyberattacks in the maritime industry has been increasing as hackers try to exploit the vulnerabilities in the shipboard OT (Operational Technology) systems. As vessels increasingly connect to the Internet to improve the efficiency of their operations and communications, OT systems become more vulnerable to cyber-attacks, which disrupt their operations and may cause catastrophic consequences. This study mainly focuses on the major shipboard OT systems: Communication Systems, Propulsion, Machinery, and Power Control Systems, Navigation Systems, and Cargo Management Systems. The cyber risks and attack scenarios associated with these OT systems are investigated.

Keywords: Operation technology; Shipboard systems; Cyber risks; Attack scenarios; Vulnerabilities; Maritime cybersecurity

1. Introduction

With the increasing worldwide demand for transportation of goods by sea, technologies have been developing rapidly on the crease. Advancements in technologies being a boon, still lack proper adherence to vital cybersecurity policies. Lack of good cybersecurity in the maritime industry can have potential effects on the safety of the vessel, crew, and cargo. It is crucial to protect the systems, hardware, sensors, network from being tampered with, disrupted, and accessed without authorization. Securing the computer system is very important as it contains personally identifiable information, intellectual properties, sensitive data, governmental information. Sometimes faulty system configurations open doors for the attacker to easily exploit the vulnerability.

A lot of maritime cyber incidents are being reported, one among them is the NotPetya attack, the most catastrophic cyberattack of all time that caused economical damage to Maersk shipping company in millions of dollars (Greenberg, 2018). Ransomware attacks are on rising, where the crucial parts of the system are encrypted, and the vessel is held hostage until the said ransom is paid. A number of GPS spoofing incidents have been taking place, one of them being the GPS spoofing incident at the people's Republic of China, which observed several GPS spoofing incidents in and around coastal areas and ports (Safety4sea, 2020). As OT systems are a major part of the vessel's operation, it is essential to investigate the attack surface of the systems under risk and the possible cyber risks that might be a threat to the systems. Investigating the cyber risks associated with the

OT (Operational Technology) systems is an important step to be done before proposing appropriate guidelines and policies to safeguard the vessel.

We initially studied the existing cyber risk management guidelines from different sources, which helped us to decide on the OT systems to be considered for our study. From the existing guidelines we are able to identify four major OT systems which were more vulnerable: Communication Systems, Propulsion, Machinery, and Power Control Systems, Navigation Systems, and Cargo Management Systems.

The main objective of our work is to study the cyber risks associated with these OT systems and their possible attack surfaces that could be targeted by the attackers. Also, the team visited an oil tanker vessel's bridge, propulsion systems, engine control room, and cargo control room which gave us a better look at each of the OT systems considered in this work and get a good understanding of the OT systems and their operations.

Figure 1 A picture of ship's bridge taken from vessel visit

2. CYBER INCIDENTS

Due to numerous security gaps, cyber-attacks on the maritime industry's OT systems have increased in recent years. Below is a list of the incidents that have occurred in the last few years which demonstrates the need for cybersecurity in vessels.

- In 2020, one of the USA's tugboats was targeted. The attack was done by spoofing the tug operator's identity and sending a phishing email with a voicemail-themed attachment (Macola, 2020).
- In 2020, CMA CGM fell victim to cyberattacks that impacted their servers. They suspect that it might be because of malware, but the nature of the attack is unknown . (Hand, 2020)
- In 2020, Garmin fell victim to the WastedLocker ransomware which encrypted its servers that caused an outage and demanded a ransom of $10 million (Mission Secure, 2020)
- In 2020, the People's Republic of China observed several GPS spoofing incidents in and around coastal areas and ports (Connectivity, 2020).
- In 2019, Norsk Hydro fell victim to the LockerGoga ransomware which disables the computer system's network adapter, disconnects it from the network and tamper the admin and user credentials, and logs out of the machine. The ransomware brought their network down costing them the damage of $71 million (Mission Secure, 2020)
- In 2019, a New York-bound ship informed the US coast guard that they are experiencing certain problems with their shipboard network, expecting that it was due to a cyberattack. It was later found that the ship's network was infected with malware (Lemos, 2019).
- In 2018 Naval Dome Ethical hackers successfully deleted the radar targets from the ship's bridge radar screen, effectively blindfolding the ship (Wingrove, 2018).
- In 2018, the China Ocean Shipping Company (COSCO) was affected by the SamSam

ransomware. The SamSam ransomware intrudes into the network, by which the hackers can get administrative privileges and run malicious executables. The amount of damage is not disclosed (Mission Secure, 2020).

- In 2017, the systems in Maersk fell victim to ransomware. The Notpetya malware had encrypted all the essential files and demanded ransom. This became a very big threat to its sailing ships around the world and cost them damage in billions of dollars (Greenberg, 2018).
- In 2017, a large GPS spoofing attack was carried out in Russia. Many ships were affected, luckily none of the ships were damaged. Navigation systems showed that these ships are in the middle of Gelendzhik airport, a few kilometers from the shore of the Black Sea (Hambling, 2017).
- In early 2015, McAfee discovered a vulnerability that allowed it to create ransomware. This vulnerability made it possible to take full control of the propulsion and navigation systems. It was possible to infect the ship via an unsecured network connection (Kevin D Jones, 2016).
- In 2015, the USCG officially reported a first case where malware was mistakenly downloaded to a mobile offshore drilling unit and affected the DP system (Rinnan, 2016).
- In 2012, hackers broke through the systems of the Australian Customer Service and Border Protection agencies, so they could check the containers of ships the agency suspects were illegal, and so they were reacting accordingly (Kochetkova, 2015)
- In August 2011, hackers hacked into the cargo system of the Iranian shipping company. They were able to change the cargo number, delivery dates, delivery locations, etc. As a result, some containers were lost along the way to hackers (Kochetkova, 2015)

3. CYBER RISKS IN OT SYSTEMS

3.1 COMMUNICATION SYSTEMS

A reliable communication system helps the owners to communicate with their vessels, also enabling navigation, live surveillance, and real-time vessel monitoring. Vessels require reliable communication systems to communicate with their main offices and family. Ships must be able to send and receive maritime information and alerts in case of an emergency/distress. As systems are more interconnected and internet usage is a risk, there is an increased threat to the safety of the ship when a cyber incident arises.

3.1.1 Satellite Communication System

Maritime satellite communications play a major role in the maritime communication chain. Satcom technologies enable the vessels and crew to stay connected to the internet, no matter how far the vessel is from the land. VSAT (Very Small Aperture Terminal) systems must provide maximum system availability under any condition. Satellite communications can be the entry point for a variety of cyberattacks, thus we must protect them.

Usage of VSAT modems is vulnerable if the default username and password credentials are not changed. Some of their web interfaces support insecure protocols like telnet, HTTP which might lead to cross-site scripting attacks. Phishing emails from unknown sources must be handled carefully, otherwise, malware like ransomware and cryptocurrency miners can be delivered to the system, because of which the vessel might be held hostage until the said ransom is paid (Wingrove, 2019) (Wingrove, 2020).

3.1.2 Integrated Communication System

The shipboard integrated communication system is developed to optimize the availability and inter-connectivity of systems. Centralized management of different communication systems and devices is set up to provide high operation efficiency and to provide faster incident response. Some of the key features include satellite and radio communication devices, intercom, WAN, LAN, and so on. As these systems are more interconnected, the cyber risks associated with them have a huge impact on the safety of the ship.

The satellite terminals can be taken under control if the defaults passwords of the terminal administration interface are not changed. This allows the hackers to modify firmware, access critical networks, and inject malware. Once the hackers gain access to the admin area, they can change passwords, copy files, modify files due to which access to FTP is also possible. Also, hackers can control and alter the system configurations if the modem can be reached by command line access (Robinson, 2020).

3.1.3 Voice Over Internet Protocol (VOIP)

VOIP helps the crew to make or receive calls within the ship, to and from their main offices and family. A dedicated and secure communication is needed to provide prompt and definite commands to safeguard the crew and the vessel.

VOIP phones are vulnerable to DoS attacks where the attacker bombards the VOIP server with Session Initiation Protocol (SIP) messages which will disrupt or halt the traffic. If the crew is not able to make calls through VOIP during an emergency, then it is a threat to the safety of the ship. Encrypting the voice and data traffic is very important as malicious eavesdropping might lead to the disclosure of confidential information. On the other hand, attackers can pretend to be talking from a reputable source and trigger the victim to give out confidential information. The telecom phones must be kept safe from malware and viruses as they might create backdoors that hackers can exploit in the future (McCraw, 2020).

3.1.4 Wireless Local Area Network

A Wireless LAN is a wireless network setup where two more devices are connected to form a local area network. It is used to provide internet connectivity to the devices in the ship and for other communication purposes.

Usually, WiFi access points are set up with default usernames and passwords when they are shipped. If default credentials are not changed, it is very easy for an attacker to log in to the web interface and take control of the modem, tamper with the firmware and launch scripting attacks. Malicious eavesdropping, on the other hand, is one of the big threats if the network is unencrypted or is weakly encrypted as the attacker can easily listen in or decode the information relayed in the network. The WiFi Protected Access 2 or WiFi Protected Access 3 protocol must be used to encrypt the wireless network traffic as they utilize Advanced Encryption Standards which is way better and secure than other standards (WebTitan, 2018).

3.2 Propulsion, Machinery, and Power Control Systems

Vessel's machineries are an important topic in the case of security. Vessel's systems are operated by a number of electronic devices, and it is possible that cyberattacks can be launched on them via input ports if any. This threatens ship control, mainly when they are more integrated and remote condition monitoring is done.

Most of the devices in the ship communicate with each other through a protocol known as

NMEA, a digital language sanctioned by an industry association known as the National Marine Electronics Association (NMEA). NMEA is a serial network where the communication between two or more systems can be done simultaneously (Cassidy, 1999). The disadvantage of using NMEA is that they have no encryption and lack message authentication (Munro, 2018).

3.2.1 Engine Governor System

Engine governor is a crucial component of the ship, which is used to control the mean speed of the engine under varying load states (Sethi, 2020). The knock control Ariadne is the controller which is responsible for governing the fuel/air properties, whereas the dual fuel controller is used for controlling the speed of the engine and to send vital information to other systems in the ship (Hyra, 2019). NMEA protocol is used to communicate with other systems in the ship.

If the attacker has access to the NMEA network, then he can manipulate the Dual Fuel Controller to provide the wrong control. An attacker can manipulate the dual fuel controller to provide the wrong amount of oil to the engine, which might drop the engine's productivity. Hackers could compromise the knocking controller and tamper with the NMEA messages, causing a drop in the engine's efficiency.

3.2.2 Fuel Oil System

Fuel Oil System is used for ship propulsion and to generate power by utilizing the energy acquired from burning the oil (Wankhede, 2018). The fuel oil system consists of various systems such as fuel oil transfer system, fuel oil supply system, and fuel oil treatment system (Hyra, 2019) (Babicz, 2015).

The fuel system is directly connected to the NMEA network and it is possible to tamper with the messages flowing in and out of the system. For example, the fuel level indicator can be manipulated to show the wrong fuel level in the indicator panel, which might result in issues such as overloading the containers or delay in reaching the destination.

3.2.3 Alarm Monitoring and Control System

The alarm monitoring and control system monitors and controls all the alarms implemented on the ship. It connects the alarms associated with each of the systems in the ship and emits visual or audio signals in the event of emergency or failure (Wankhede, 2020)

The alarm system is connected to the NMEA network, which is not secure. Thus, it is possible that a hacker can tamper with the commands sent to the alarm system resulting in alarm failure or the rise of a fake alarm. The ship will be in danger if any emergency event or distress is not highlighted by ringing the alarm.

3.2.4 Power Management System

The goal of this system is to provide an uninterrupted power supply to all the components in the vessel. It consists of the main switchboard, emergency switchboard, and voltage indicators. Containers such as fuel tankers and air-conditioned tankers must be transported by controlling certain properties like temperature, pressure, and level of content. They must be controlled properly, if not the container contents might get spoiled or even cause an explosion of fuel tankers (Hyra, 2019).

The power management system is connected to the NMEA network. In case the power management system is compromised and if the power distribution is not done properly, then it

might damage the container's content as it may require an uninterrupted power supply throughout the voyage. Also, if any USB port is present in the system, then malware can be injected that would lead to disruption of normal operation and unauthorized access to system resources.

3.2.5 Emergency Generators and Batteries

The purpose of an emergency generator is to provide backup power to the crucial device in the ship in case the main generator fails or if a power outage occurs unexpectedly. Both the batteries and the emergency generator can be used in case of an emergency (Wankhede, 2020). The emergency switchboard and main switchboard is present in the power management system panel where voltage and frequency are monitored. As mentioned earlier, the power management system is connected to the NMEA network which is highly vulnerable to cyberattacks (Hyra, 2019) (Electro Technical Officer, n.d.) (Kaushik, 2020).

Cyberattacks that cause power management systems to fail will affect the automatic start of the emergency generators. If an attacker compromises the power management system, then the switchboards cannot be operated and controlled properly. Thus, if the emergency generator is not switched on when the relay senses that the voltage is low or when there is a power outage, delay in switching on these emergency generators might cause the contents in the cargo containers to spoil, for example, refrigerated or reefer containers carry temperature-sensitive goods, and they need constant electricity throughout the voyage.

3.3 Navigation Systems

With modern-day facilities and automation, the ship now has many advanced navigation equipment systems that provide accurate travel data.

Navigation is a computing system that supports navigation. Navigation systems may be complete onboard a vessel controlled by the system or located elsewhere, with the use of radio or other signals sent to control the vessel. In maritime navigation, it is necessary to know the accurate position, speed, and heading of the vessel to ensure that the vessel reaches its destination in the safest and timely manner.

3.3.1 Electronic Chart Display and Information System (ECDIS)

ECDIS is a development in the navigational chart system. With the use of the electronic chart system, it has become easier for a ship's navigating crew to pinpoint locations and attain directions. ECDIS displays navigational points, radar information, weather, ice conditions, speed, position, and planned route of the ship.

The virus enters the system while a crew member injects a USB device into the USB port. An attacker obtains unauthorized access to the internet and overloads the network to perform a Denial-of-Service attack that takes the ECDIS offline and leaves the vessel without a means of safe navigation. Spoofing attacks can take place by spoofing incoming plan text messages to the ECIDS from the NMEA network, which changes the display of the ECDIS and may result in ship collision. By compromising the local area network, the attacker can steal Electronic Navigational Charts (ENCs) and gain access to other data (Dyryavyy, 2015) (Hyra, 2019).

3.3.2 Radio Detection and Ranging System

The radar is one of the most used equipment systems onboard ships. It is mandatory equipment of navigation used in identifying,

tracking, and positioning vessels among other things to safely navigate a ship from one point to another.

Initially, Naval Dome's ethical hackers sent a virus-laden email via the ship's satellite link to the captain's computer, which regularly connects to ECDIS for chart updates. During the next chart update, the virus transferred itself to ECDIS where it immediately installed itself and got to work. After doing that, the virus transferred to the radar through the local Ethernet switch. This malware hacking attack alters the radar display by deleting the targets displayed on the screen, essentially blinding the ship (Wingrove, 2018). Due to vulnerabilities in the Server Message Block (SMB) service, an attacker can perform a Man in the Middle (MITM) attack and execute code without authentication (Boris Svilicic, 2020).

3.3.3 Automatic Identification System (AIS)

AIS displays other vessels in the vicinity. It is fitted on ships for the identification of ships and navigational marks. AIS helps in obtaining detailed information of any ship such as name, speed, position, direction, rate of turn, destination, and physical dimensions such as length, breadth, tonnage, beam, and draft to the nearby ships and to the coastal authorities.

The AIS software has no built-in security or authentication. In a spoofing attack, a fake terrestrial tower is created that transmits AIS data to integrated AIS terminals. Naturally, this could trigger a CPA alert which drives a vessel off-course by causing it to hit an obstruction or run the vessel aground (Anon., 2016). An attacker could launch a replay attack by executing a spoofing command to delay the transmission time and retry it over and over. This can effectively cause the AIS display to go away. There are a few specific instructions that only the port authorities can give for the transponder of the ship's automatic information system to operate on a certain frequency. A malicious attacker could spoof this type of command and practically switch the target's frequency to another that is empty. This frequency hopping attack causes the ship to stop sending and receiving messages on the correct frequency, effectively disappearing and being unable to communicate (Joseph DiRenzo, n.d.) (Hyra, 2019)

3.3.4 Global Positioning System (GPS)

GPS is a display system used to show the ship's location with the help of a global positioning satellite in the earth's orbit.

The spoofing attack attempts to trap a GPS receiver by transmitting fake GPS signals, which resemble normal signals. This makes the receiver believe that its position is somewhere other than where it is, as determined by the attacker. This attack makes ships unnecessarily idle at sea, so ship-to-ship and ship-to-land collisions are a possibility (Connectivity, 2020). Jamming is usually due to interference from signals on GNSS frequencies. When an attacker performs GPS jamming, AIS provides wrong positions, wrong information presented on ships ECDIS, misleading information presented on ships AIS (Grant, 2010).

3.3.5 Dynamic Positioning (DP) System

DP system is a computer-controlled system that automatically maintains a vessel’s position and heading by using its own propellers and thrusters.

Due to the poor software design of the DP system, an attacker can create a network storm on the GNSS receiver and perform a denial of service (DOS) attack. This attack makes the DP controller unavailable. Spoofing involves

transmitting the false signals to GNSS which displays the wrong position on the DPS display. This Spoofing attack causes the ship to change its heading. An attacker gains unauthorized access to the DP system and can perform a backdoor attack to download data and make changes to the system (Rinnan, 2016).

3.3.6 Global Maritime Distress and Safety System (GMDSS)

The goal of GMDSS is to virtually guarantee that vessels will be able to communicate with an onshore station at any time, from any location, in case of distress or to exchange safety-related information. GMDSS sends a distress signal via satellite or radio communication equipment. It is also used as a medium for sending or receiving maritime safety information and general communication channel.

Due to the lack of confidentiality in the VHF, GMDSS is vulnerable to cyber-attacks because malicious firmware, if installed, could allow attackers to gain control of the devices on board, deliver false information by spoofing and disrupting communications. While sending a distress signal, if sensitive information is being sent in plain text, it may be possible for an attacker to intercept or manipulate messages by executing an Eavesdropping attack. With faster and cheaper Internet access, the risk of documents or malware being downloaded to the devices onboard will increase. Therefore, this group of networked systems is vulnerable to DOS attacks resulting in loss of communication (Nettitude, n.d.) (Dennis Bothur, 2017).

3.3.7 Voyage Data Recorder

Voyage Data Recorder behaves like a "black box", continuously saves all necessary information about the ship. Records the various data relating to the position, movement, physical status, command, and control of a ship over the period, which can be used for reconstruction of the voyage details and vital information during an accident investigation.

Malware enters the system while a crew member injects a USB device into the USB port. Due to this malware, an attacker can log into the VDR system and steal data, destroy data. Vulnerabilities in services running on VDR allow attackers to execute code with administrator (root) privileges. This means that attackers can do everything within the VDR operating system, including deleting conversations from the bridge, deleting radar images, changing speed or position readings, essentially everything can be done with the root privileges (Hyra, 2019).

3.3.8 Integrated Navigation System (INS)

INS enhances the effectiveness and safety of ship navigation by integrating at least two navigational functions. It is a software platform for the fusion of data from the major ECDIS and radar systems with sensors for the additional navigation functions of the route.

Due to the low encryption of the protocol server in the INS and vulnerabilities in the SMB (Server Message Block) service, an attacker can carry out a Man in The Middle (MITM) attack and gain unauthorized access to the system. With this access, an attacker could execute the code in the INS system (Boris Svilicic, 2019).

3.4 Cargo Management Systems

Cargo management is made for an easier, faster, and more reliable way of controlling and tracking cargo. It consists of multiple smaller systems which cooperate. Depends on the ship they can be automatized. Often the status of cargo is synchronized over the internet.

3.4.1 Cargo Control System (CCR)

CCR or cargo office of a tankship is where the person in charge (PIC) can monitor and control the loading and unloading of the ship's liquid cargo. The design and layout of an individual cargo control room are determined by the ship's design, owner's requirements, and the capabilities of the shipyard in which the ship is built.

A virus enters the onboard network via phishing emails with attached files, making it easy to download from the Internet or via a storage device. Any cargo control and monitor computer system connected to the network is locked out unless a ransom is paid. The unintentional or intentional introduction by a crew member of malware targeting malicious attacks is serious and much more likely to occur. Due to this malware, an attacker can access the system and steal important data. This attack causes the wrongful owner to pick up the cargo (N. Kala, 2019).

3.4.2 Ballast Water System

It is a compartment within a ship that holds water as ballast to provide stability. Using water in a tank allows for the easier adjustment of weight. It also allows for the ballast to be pumped out to temporarily reduce the draft of the vessel when it is required to enter shallower water.

The malware injected into the Bridge system causes the engine system to send a false command regarding the increase or decrease of the water level in the ballast compartment, which causes the vessel to sink. Phishing emails sent to computer systems will compromise the ICS network, which will alter the functioning of the management of sensors and actuators, causing the vessel to become unbalanced (Lagouvardou, 2018) (Hyra, 2019).

4. Summary of Cyber Risks

Our study identified the attack surfaces and cyber risks of Communication systems,

Table 1 Summary of attack surfaces and cyber risks

OT System	Attack Surface	Cyber Risks
Communication systems	VSAT modem, Wifi access point, insecure web interface, VOIP phones.	Tampering the modem settings, Tampering the firmware, Man in the middle attack, Login with default credentials, Eavesdropping, Cross-site scripting, Denial of Service attack.
Propulsion, Power control & Machinery	NMEA network, USB ports.	Man in the middle attack, Eavesdropping, Malware.
Navigation systems	USB, Local Area Network, Local Ethernet Switch, Server Message Block Service, GPS receiver, Very High Frequency radio, Protocol server, NMEA network, AIS software	Denial of Service attack, Spoofing, Virus, Phishing, Malware, Man-in-the-Middle (MITM) attack, replay attack, Frequency hopping attack, Jamming, Backdoors, Eavesdropping, Remote code execution.
Cargo management systems	Computer Systems, USB, ICS Network, Pumps, Valves	Ransomware, Malware, Phishing, Virus

Propulsion, Machinery and Power control systems, Navigation systems, Cargo management systems. The summary of attack surfaces and cyber risks of OT systems are shown in Table 1.

5. Conclusion

Increased connectivity and networking of integrated on-board OT systems has been an essential part of the operation and management of ships and of the safety and security of crew, cargo, and ships themselves. While it has brought many advantages, this digitalization and connectivity to the internet also increase the risk of cybersecurity attacks and threats, as we have outlined above. Undoubtedly, it is vital to deploy well-established and tested systems in the vessel. Thus, it is very crucial to identify the vulnerabilities in the system to prevent cyberattacks. In our work, we have researched the major cyber risks associated with shipboard OT systems. Identifying the attack surfaces and the cyber risks provides a clear view of possible threats, which will be beneficial while we produce our own cyber risk management guidelines in future.

6. Future Works

As we have investigated the cyber risks, the next step is to establish guidelines that will help protect these OT systems. We will study and harmonize the existing cyber risk management guidelines and, along with our study, thereby produce Singapore's own guidelines that will help safeguard these systems from cyberattacks. The guidelines will help maritime authorities and vessel owners to investigate and determine the cyber hygiene and readiness of the vessels. The guidelines will also consider the balance of risks versus costs in implementing mitigating actions of cyber risks identified.

Acknowledgements

This work was supported in part by the Singapore University of Technology and Design and in part by the Singapore Maritime Institute, Singapore under the grant number SMI-2020-MA-04.

REFERENCES

Anon., 2016. Automatic Identification Systems (AIS), its Benefits and Threats. [Online]
Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/faq-automatic-identification-systems-ais-benefits-and-threats [Accessed 28 October 2020].

Anon., n.d. Fuel oil system. [Online]
Available at: https://www.wartsila.com/encyclopedia/term/fuel-oil-system [Accessed 20 October 2020].

Anon., n.d. THE GUIDELINES ON CYBERSECURITY ONBOARD SHIPS. [Online]
Available at: https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf
[Accessed 2 November 2020].

Babicz, J., 2015. Wartsila Encyclopedia Of Ship Technology. 2nd ed. Finland: Wartsila Corporation.

Boris Svilicic, I. R. A. J. a. D. Z., 2019. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering, p. 11.

Boris Svilicic, I. R. V. F. c. a. D. M. ´. c., 2020. Towards a Cyber Secure Shipboard. THE JOURNAL OF NAVIGATION, Volume 73, p. 12.

Cassidy, F., 1999. NMEA 2000 Explained - The Latest Word. [Online] Available at: https://www.nmea.org/Assets/2000-explained-white-paper.pdf
[Accessed 18 October 2020].

Connectivity, 2020. Understanding GPS spoofing in shipping: How to stay protected. [Online] Available at: https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/
[Accessed 27 October 2020].

Dennis Bothur, G. Z. C. V., 2017. A critical analysis of security vulnerabilities and countermeasures. s.l., AUSTRALIAN INFORMATION SECURITY MANAGEMENT CONFERENCE.
Dyryavyy, Y., 2015. Can You Hack An Ecdis?. [Online] Available at: https://www.pilotmag.co.uk/can-you-hack-an-ecdis-yevgen-dyryavyy/
[Accessed 26 October 2020].

Electro Technical Officer, n.d. All about Emergency Generator on ship. [Online] Available at: https://electrotechnical-officer.com/all-about-emergency-generator-on-ship/ [Accessed 26 October 2020].

Grant, D. A., 2010. GPS Jamming and its impact on maritime navigation. [Online] Available at: https://www.gla-rad.org/content/uploads/2018/01/gps-jamming-and-its-impact-on-maritime-navigation-presentation.pdf
[Accessed 2 November 2020].

Greenberg, A., 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. [Online] Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 07 October 2020].

Hambling, D., 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon. [Online] Available at: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 3 November 2020].

Hand, M., 2020. CMA CGM latest shipping victim of a cyber attack. [Online] Available at: https://www.seatrade-maritime.com/containers/cma-cgm-latest-shipping-victim-cyber-attack
[Accessed 9 October 2020].

Hyra, B., 2019. Analyzing the Attack Surface of Ships, Denmark: s.n.

Joseph DiRenzo, D. G. S. R., n.d. The Little-known Challenge of Maritime Cyber Security. [Online] Available at: http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberSecurityCorfu7-5-15.pptx.pdf
[Accessed 3 November 2020].

Kaushik, M., 2020. Ways of starting and testing emergency generator. [Online] Available at: https://www.marineinsight.com/tech/generator/ways-of-starting-and-testing-emergency-generator/
[Accessed 26 October 2020].

Kochetkova, K., 2015. Maritime industry is easy meat for cyber criminals. [Online] Available at: https://www.kaspersky.com/blog/maritime-cyber-security/8796/?ref=555601-91802X1545674X0299c634135b24a95a598a642f1cfb7c&affmt=2&affmn=1
[Accessed 29 October 2020].

Lagouvardou, S., 2018. Maritime Cyber Security: concepts, problems and models, s.l.: s.n.

Lemos, R., 2019. Coast Guard Warns Shipping Firms of Maritime Cyberattacks. [Online] Available at: https://www.darkreading.com/vulnerabilities---threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks/d/d-id/1335198 [Accessed 8 October 2020].

Macola, I. G., 2020. US Tugboat cyber-attack: the experts respond. [Online] Available at: https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/ [Accessed 8 October 2020].

McCraw, C., 2020. 12 VoIP Security Vulnerabilities and How to Fix Them. [Online] Available at: https://getvoip.com/blog/2020/05/06/voip-security/ [Accessed 12 October 2020].

Mission Secure, 2020. Real-World Lessons Learned from Maritime Cybersecurity Incidents. [Online] Available at: https://www.missionsecure.com/blog/real-world-lessons-learned-from-maritime-cyber-attacks-incidents [Accessed 8 October 2020].

Mission Secure, 2020. The Cyber-attack on Garmin: Exposing GPS vulnerabilities. [Online] Available at: https://www.missionsecure.com/blog/the-cyber-attack-on-garmin-exposing-gps-vulnerabilities [Accessed 09 October 2020].

Munro, K., 2018. Hacking, tracking, stealing and sinking ships. [Online] Available at: https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/ [Accessed 20 October 2020].

N.Kala, M. B., 2019. Cyber Preparedness in Maritime Industry. International Journal of Scientific and Technical Advancements, 5(2), p. 28.

Nettitude, n.d. Marine and Offshore Cyber Briefing: Cyber Risks in Communication Systems. [Online] Available at: https://cdn2.hubspot.net/hubfs/3021880/NETT_2019_M&O_Cyber%20Risks%20in%20Communication%20Systems_0711.pdf [Accessed 28 October 2020].

Rinnan, O. C. &. A., 2016. Who Said That DP Does Not Rhyme With Cybersecurity?. s.l., DYNAMIC POSITIONING COMMITTEE.

Robinson, E., 2020. Hacked – a real life story of exploiting vessel VSAT. [Online] Available at: https://smartmaritimenetwork.com/2020/05/25/hacked-a-real-life-story-of-exploiting-vessel-vsat/ [Accessed 09 October 2020].

Safety4sea, 2020. Understanding GPS spoofing in shipping: How to stay protected. [Online] Available at: https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/ [Accessed 8 October 2020].

Sethi, S., 2020. Types of Governors for Engines Used On Ships. [Online] Available at: https://www.marineinsight.com/tech/types-of-governors-for-engines-used-on-ships/ [Accessed 20 October 2020].

Wankhede, A., 2018. Marine Heavy Fuel Oil (HFO) For Ships – Properties, Challenges and Treatment Methods. [Online] Available at: https://www.marineinsight.com/tech/marine-heavy-fuel-oil-hfo-for-ships-properties-challenges-and-treatment-methods/ [Accessed 21 October 2020].

Wankhede, A., 2020. Different Types of Alarms on Ships. [Online] Available at: https://www.marineinsight.com/marine-safety/different-types-of-alarms-on-ship/ [Accessed 22 October 2020].

Wankhede, A., 2020. How is Power Generated and Supplied on a Ship?. [Online]
Available at:
https://www.marineinsight.com/marine-electrical/how-is-power-generated-and-supplied-on-a-ship/
[Accessed 26 October 2020].

WebTitan, 2018. Most Common Wireless Network Attacks. [Online] Available at:
https://www.webtitan.com/blog/most-common-wireless-network-attacks/
[Accessed 12 October 2020].

Wingrove, M., 2018. 'Impregnable' radar breached in simulated cyber attack. [Online]
Available at: https://www.rivieramm.com/news-content-hub/news-content-hub/impregnable-radar-breached-in-simulated-cyber-attack-25158
[Accessed 2 November 2020].

Wingrove, M., 2019. How to ensure VSAT modems cannot be hacked. [Online]
Available at:
https://www.rivieramm.com/news-content-hub/news-content-hub/ensure-vsat-modems-cannot-be-hacked-57065
[Accessed 09 October 2020].

Wingrove, M., 2020. Secure VSAT to prevent cyber attacks. [Online]
Available at: https://www.rivieramm.com/news-content-hub/news-content-hub/secure-vsat-to-prevent-cyber-attacksnbsp-58986
[Accessed 09 October 2020].

Authors Biography

The authors are from iTrust (Centre for Research in Cyber Security), Singapore University of Technology and Design, Singapore. Ruchitha Dumbala and Priyanga Rajaram are Senior Research Assistants, Mark Goh Voon Vei is Senior Manager, and Jianying Zhou is Professor and Co-Center Director of iTrust.

Recognition of Structural Members Enables Plate Buckling Checks According to ABS / DNV Rules Directly in General FEA Programs

Oleg Ishchuk

COO @ SDC Verifier, Email: oleg@sdcverifier.com

Abstract

Plate buckling strength is an important aspect of offshore steel construction design. In this article, we will show how the problem of both general FEA analysis (strength evaluation, displacement, and deflection checks) and plate buckling check according to ABS or DNV rules is solved with the help of FEA and code-checking tools. The most complicated task in performing a plate buckling check for a big structure, like complete ship design, on a general Finite Element Analysis model is to define a big amount of plates and the dimensions of these plates to be verified. For the precise FEA analysis, the model has to have a fine mesh with small enough finite elements to guarantee the correct results. But at the same time, each plate field must be treated as one separate structural member for plate buckling checks. With the help of a specific tool, it is possible to break the boundaries of general FEA Analysis and enable the code checking directly in Simcenter 3D, Femap, Ansys, etc. by enabling the automatic recognition of structural items. The recognition of plates, stiffeners, and girders is based on mesh connectivity and can be performed on any structure which is built with 2D or, in some cases, even 3D elements. The structural members are defined automatically and mesh independently. This allows an engineer to have a model with fine mesh for precise results of the general finite element analysis and a list of structural members for code checking.

Keywords: Plate Buckling; FEA; Code Checking; Plate Buckling Factor

1. Introduction

Plates are commonly used in the design of ships, offshore structures, aircraft, civil, and other engineering structures. Each plate should be verified as it influences the strength and stability of the whole construction. There are two main failure modes of a plated structural item that can lead to sudden damage: material failure and structural instability, which is called buckling. Most plated structures are capable of carrying tensile loadings but may be poor in resisting compressive forces. Usually, buckling effects take place suddenly and may lead to severe or even catastrophic structural failure. That's why it is very important to understand the buckling capacities of the plates to avoid a collapse of the complete structure.

Buckling analysis of the structure with a general FEA solver may seem like a quick and easy solution since it provides a buckling load factor – a ratio of the buckling load to the currently applied load. As a result, you get a value of the factor that will cause buckling failure in case of multiplication the load value with it. But this analysis result would be only for a panel that will fail first, which does not guarantee that the rest of the structure is safe. This is where it becomes necessary to verify according to the industry standards. A lot of these documents already contain verification procedures or recommended practices for the plate buckling analysis. Here are some of the codes that are commonly used in the industry:

- DNV RP-C201 Buckling Strength of Plated Structures;
- DNV CN30 Buckling Strength Analysis of Bars and Frames, and Spherical Shells;
- ABS Plate Buckling and Ultimate Strength Assessment for Offshore Structures;
- Eurocode 3 – design of steel structures – Part 1-5: Plated structural elements.

In the case of code checks according to the standards, an engineer is able to perform the calculation of the value of utilization factor for every plate as a result. It is possible to do the calculation for each load or combination to ensure that the whole structure is safe. This procedure is usually not very simple, since a lot of factors, characteristics, and coefficients should be taken into account. With a certain knowledge, it's possible to do the check according to the standard by hand. But in this case, an engineer is able to verify one plate under one loading condition at a time. Though, a typical offshore structure or ship design consists of thousands or even millions of plates and hundreds of load combinations. This is when automation is a must.

When it comes to the code checking in CAE there are two ways:

- To run the general finite element analysis for the design, which is mandatory to understand the behavior of the structure and obtain the results stresses, displacements, forces, other outputs. And then to perform the Standard verification of important details with scripts, spreadsheets, or hand calculation.
- To use the general FEA analysis for the design and dedicated software for the code checking.

Both of these methods have certain drawbacks. Spreadsheet or hand calculation analysis is time-consuming and it's easy to miss a failure, since not always the most stressed, or longest plates are the most subjected to buckling. Using dedicated code checking software is more precise, but since it requires having each structural member defined, it is necessary to build another model for code checking. Discernibly, double modeling leads to an increase in the overall completion time of the project, since every update and modification has to be done twice.

2. Automatic Recognition

Since checks are done on structural items and not on finite elements, the best solutions for both execution time and accuracy of the results would be to use the extension for general FEA programs that is capable of the automatic recognition of the structural members mesh independently. SDC Verifier is software that follows this methodology. The best solution to avoid double work is to have the same environment for both General FEA and code checks.

Stiffened Panel Finder —is a tool to automatically

recognize sections, panels, plates, stiffeners, and girders, and dimensions of these structural members. The detection is based on mesh connectivity and can be performed on any structure which is built with 2D (plate or shell elements) for plate members, and both 1D (beams) or 2D finite elements for stiffeners and girders.

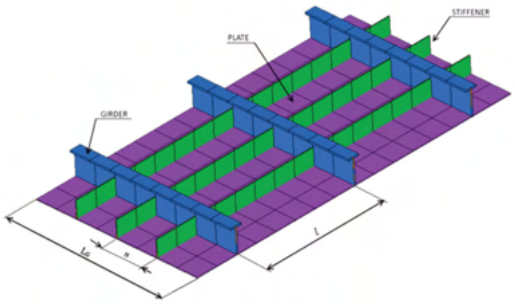


Figure 1 Recognized structural members

Detection is made automatically and meshes independently. This brings to an engineer the opportunity to have a model with fine mesh for precise results of the general finite element analysis and use the same model for calculation of Eurocode, ABS, or DNV plate buckling checks.

At the first stage, Sections are defined by the global or custom coordinates. All the elements that lay in one plane (of course, with a certain angle of deviation which could be defined by the user in settings) are defined as Sections. This allows detection of, for example, Frames, Decks, and Longitudinal sections of the ship. Hull is also automatically recognized as a custom section.

Figure 2 Frames of the ship automatically recognized by the coordinates.

The next step is to define the plates on these sections, plates are also recognized automatically with borders at sections intersection, stiffeners, girders, or any other members perpendicular to the sections. A user always has control over recognition to add/remove or split the members manually. But if the mesh is fine enough, there is no need for manual interaction with the recognized structural members. Recognition is completely mesh-independent, any plate of the studied FEA model can consist of hundreds or even thousands of finite elements for precise stress analysis, and it will still be defined as one structural member for plate buckling checks.

Automatic recognition of the plates defines the following parameters for the code check: length and widths of the plate, direction, amount of edges, material type, and thickness. The analysis is based on stresses in each finite element of the plate or on the plate average stress.

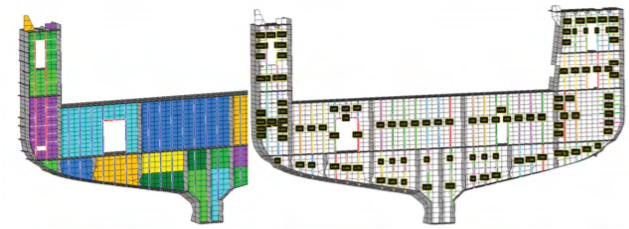


Figure 3 Plates and Stiffeners recognized on a section

3. Verification procedure from the user point of view

Despite the fact that material properties, forces, stresses are defined in the FEA program and plate dimensions and types are automatically recognized, some parameters still should be defined by the user. For example, DNV RP-C201 Plate/Stiffener Buckling (2010) requires user input for a characteristic called Resulting

Material Factor. During the analysis procedure buckling resistance will be divided by this factor. By default, this factor is 1.15 but an engineer may change this value taking into account the type of structure or consequences of failure.

It is also possible to define a thickness factor that allows to increase/decrease all plate thicknesses quickly without re-solving the model. For example, a thickness factor of 1.2 means a thickness increase of 20% which leads to a stress decrease.

An important decision has to be made about what stresses to use. It is possible to use plate average stress, this will result in one buckling factor result on each plate. A more conservative approach is to use stresses of every element for the analysis, in this case, the maximum buckling factor from all the elements of a plate would be presented as a resulting buckling factor of the whole plate.

Figure 4 Plate Average Stress options.

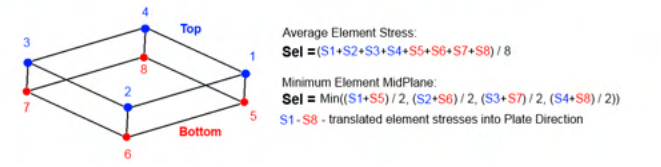


Figure 5 Elemental Stress options.

If the option to use plate average stress is turned off, then there are two options to define elemental stress: average element stress or minimum element midplane stress (which is maximum compressive stress)

Basically, the parameters and decisions described above are the only engineer's input in case of automatic code checking. The rest of the calculation is done by a code checking program: standard outputs of the FEA solver and parameters of the model are used as variables for formulas to define plate buckling factor as a result. The benefit of SDC Verifier as a code checking tool is also that all the formulas are open and refer to the standards, so it is easy to follow the calculation procedure, possible to find the source of the problem quickly, and even modify the existing formulas if customization of the checks is necessary. It is also possible to see the intermediate results values.

Software completely follows the verification procedure of the selected standard. At the first step of the code check plate length, width, and thickness are retrieved from the recognition, and compressive Stresses Sx, Sy, and Sxy are calculated in plate direction. Then the Slenderness and Buckling resistance for both X and Y directions are checked. Every formula is open and has a description, names of the intermediate variables. For example, the slenderness formula (used to calculate the buckling resistance in the X direction of the plate) from the DNV check is represented below:

```
Replacement = LambdaP (Plate Slenderness P)
Description: Formula (6.3)
0.525 * Plate.Width / Tplate * sqrt(Yield / Young)
```

Different types of variables are highlighted with different colors and description refers to the formula from the standard. In the final step, Buckling factors are calculated for X, Y, and XY (Shear) direction, as well as Maximum overall directional and combined Buckling Factors.

4. Results of the Automated Plate Buckling Checks

4.1 Result tables

As a result of this automated verification procedure, the user will get a Buckling factor for every plate of the whole structure in minutes rather than days spent with spreadsheets or hand calculations. Moreover, the calculation could is done for multiple load combinations and envelope groups of loads. This means that the results of the analysis, which are typically presented in detailed buckling factor tables for every section/plate, are automatically prepared for each loading condition.

A broad variety of tables are available, results can be presented over any load or selection. The extreme table type shows the maximum value for the complete selection and Expand table type presents the value for every item of this selection, so it can be quite extensive.

In addition to the buckling factor, the following parameters results can also be listed in the table:

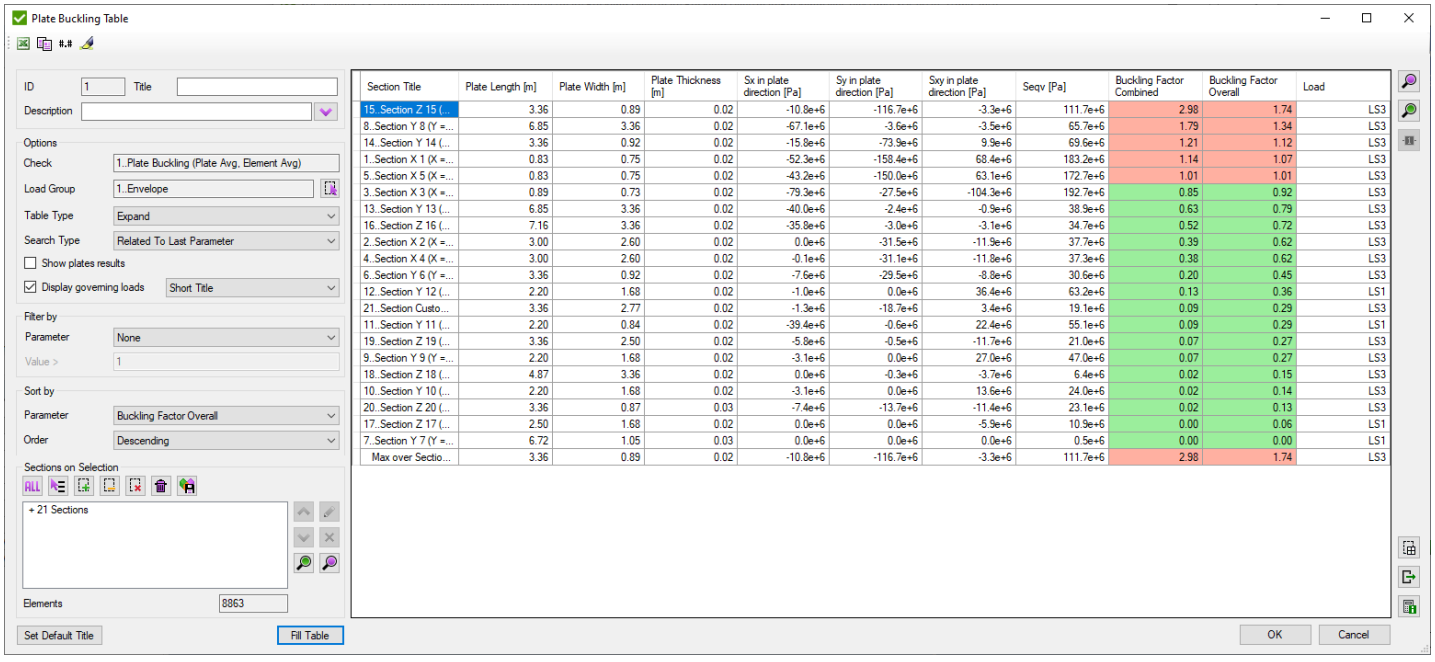
- Plate length;
- Plate Width;
- Plate Thickness;
- Sx in plate direction;
- Sy in plate direction;
- Sxy in plate directions;
- Equivalent Stress.

The interface of the tables allows presenting not only the final results but also the calculation details – all the formulas with intermediate resulting values of the parameters used for the calculation. This provides an engineer with an extra instrument to control the calculation and leaves much less room for an error.

4.2 Result plots

The graphical interface of the FEA programs is used to visualize the buckling factor or any other output (including the recognition details) values for any user-defined selection.

This provides a user with a full control of the view including the positioning of the model, plotting style, legend settings. Views are stored and can



Section Title	Plate Length [m]	Plate Width [m]	Plate Thickness [m]	Sx in plate direction [Pa]	Sy in plate direction [Pa]	Sxy in plate direction [Pa]	Seqv [Pa]	Buckling Factor Combined	Buckling Factor Overall	Load
15..Section Z 15 (...	3.36	0.89	0.02	-10.8e+6	-116.7e+6	-3.3e+6	111.7e+6	2.98	1.74	LS3
8..Section Y 8 (Y =...	6.85	3.36	0.02	-67.1e+6	-3.6e+6	-3.5e+6	65.7e+6	1.79	1.34	LS3
14..Section Y 14 (...	3.36	0.92	0.02	-15.8e+6	-73.9e+6	9.9e+6	69.6e+6	1.21	1.12	LS3
1..Section X 1 (X =...	0.83	0.75	0.02	-52.3e+6	-158.4e+6	68.4e+6	183.2e+6	1.14	1.07	LS3
5..Section X 5 (X =...	0.83	0.75	0.02	-43.2e+6	-150.0e+6	63.1e+6	172.7e+6	1.01	1.01	LS3
3..Section X 3 (X =...	0.89	0.73	0.02	-79.3e+6	-27.5e+6	-104.3e+6	192.7e+6	0.85	0.92	LS3
13..Section Y 13 (...	6.85	3.36	0.02	-40.0e+6	-2.4e+6	-0.9e+6	38.9e+6	0.63	0.79	LS3
16..Section Z 16 (...	7.16	3.36	0.02	-35.8e+6	-3.0e+6	-3.1e+6	34.7e+6	0.52	0.72	LS3
2..Section X 2 (X =...	3.00	2.60	0.02	0.0e+6	-31.5e+6	-11.9e+6	37.7e+6	0.39	0.62	LS3
4..Section X 4 (X =...	3.00	2.60	0.02	-0.1e+6	-31.1e+6	-11.8e+6	37.3e+6	0.38	0.62	LS3
6..Section Y 6 (Y =...	3.36	0.92	0.02	-7.6e+6	-29.5e+6	-8.8e+6	30.6e+6	0.20	0.45	LS3
12..Section Y 12 (...	2.20	1.68	0.02	-1.0e+6	0.0e+6	36.4e+6	63.2e+6	0.13	0.36	LS1
21..Section Custo...	3.36	2.77	0.02	-1.3e+6	-18.7e+6	3.4e+6	19.1e+6	0.09	0.29	LS3
11..Section Y 11 (...	2.20	0.84	0.02	-39.4e+6	-0.6e+6	22.4e+6	55.1e+6	0.09	0.29	LS1
19..Section Z 19 (...	3.36	2.50	0.02	-5.8e+6	-0.5e+6	-11.7e+6	21.0e+6	0.07	0.27	LS3
9..Section Y 9 (Y =...	2.20	1.68	0.02	-3.1e+6	0.0e+6	27.0e+6	47.0e+6	0.07	0.27	LS3
18..Section Z 18 (...	4.87	3.36	0.02	0.0e+6	-0.3e+6	-3.7e+6	6.4e+6	0.02	0.15	LS3
10..Section Y 10 (...	2.20	1.68	0.02	-3.1e+6	0.0e+6	13.6e+6	24.0e+6	0.02	0.14	LS3
20..Section Z 20 (...	3.36	0.87	0.03	-7.4e+6	-13.7e+6	-11.4e+6	23.1e+6	0.02	0.13	LS3
17..Section Z 17 (...	2.50	1.68	0.02	0.0e+6	0.0e+6	-5.9e+6	10.9e+6	0.00	0.06	LS1
7..Section Y 7 (Y =...	6.72	1.05	0.03	0.0e+6	0.0e+6	0.0e+6	0.5e+6	0.00	0.00	LS1
Max over Sectio...	3.36	0.89	0.02	-10.8e+6	-116.7e+6	-3.3e+6	111.7e+6	2.98	1.74	LS3

Figure 6 Overall Buckling Factor results in a table

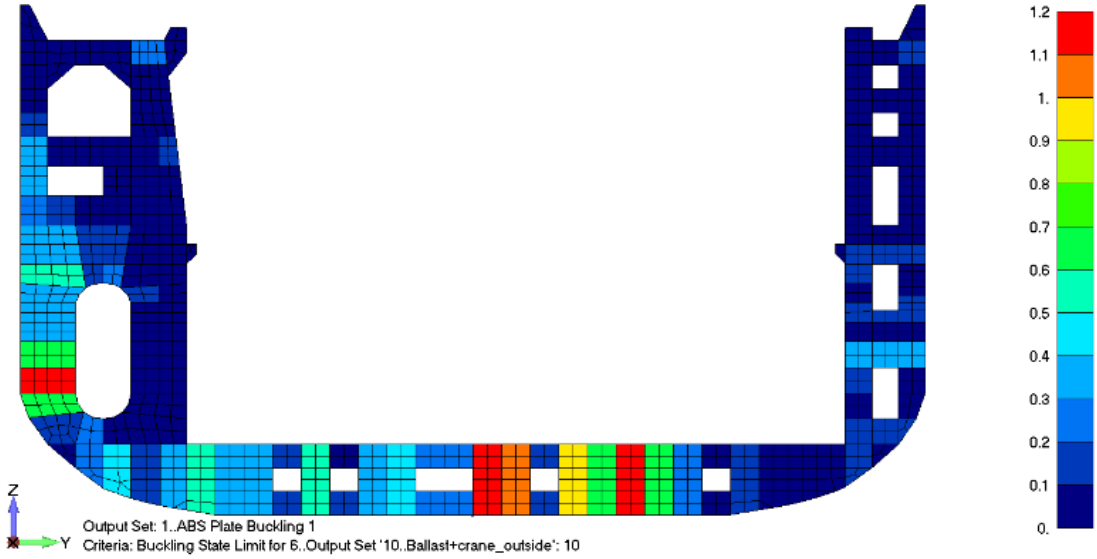


Figure 7 Buckling Factor results on a plot.

be used to present the results of general FEA analysis, as well as code checking results, for any load or selection.

4.3 Automatic reporting

Since the calculation core allows to get the results for individual loads and load combinations, and the code checking tool has an interface to present the results with tables and plots, it's easy to prepare an automated template-based structure for the report generation. Typically report contains the following parts:

- Model Setup – information about materials, properties, loads and boundary conditions, the basis of calculation, formulas used for the analysis (automatically added because of the open interface of the code-checking software);
- Results – automatically sorted by load, or by selection results of finite element analysis and verification according to standards;
- Summary – a short explanation of the main results and comparison with the allowable values.

Automation of the reporting process helps to save time on the repetitive documentation routine. It also reduces the deadline pressure: since the report structure is set, there is no need to create a new report in case of modifications or design changes. The engineer has only to update the model, run the calculation, and regenerate the report.

5. Conclusions

The code checking approach described in this article brings to marine designers and naval architects the understanding of alternatives for the usual code checking workflow and describes the ways to save time on routine and repetitive tasks by automating the verification for a complete model in a single CAE environment.

In addition to the time-saving benefits, usage of code checking extensions for the General FEA programs allows to:

- Check the quality of modeling, with the help of recognition tools.
- Understand the behavior of a studied structure. By analyzing all possible loading

conditions and defining the governing ones.

- Analyze the critical parameters for the checks.
- Quickly improve the design. By using the thickness factors and modifying the plate dimensions. Or with the help of powerful editors in the general FEA tools and instant update of the simulation data code-checking extension.
- Compare different design approaches of loading conditions in one user-friendly CAE environment.

References

Timoshenko, S. P. and Gere, J. Theory of Elastic Stability, 2nd edition, McGraw-Hill, 1961

Recommended Practice. Det Norske Veritas. DNV-RP-C201 Buckling Strength of Plated Structures. October 2010.

Authors Biography

Oleg Ishchuk, the Chief Operating Officer at SDC Verifier. With more than 10 years of experience in mechanical engineering: structural verification of Ship-to-Shore cranes, lifting appliances, floating structures, vessels, and other equipment. He is an expert in structural verification according to multiple industry rules in Oil and Gas, Offshore and Maritime, Civil, Heavy Lifting, Machinery, and other industries, focusing on Fatigue, Plate Buckling, and Member checks.

Cybersecurity Requirements for IMO 2021

Mark Warner

Director, Inmarsat Maritime, Mark.Warner@inmarsat.com

Abstract

Global maritime satellite service provider Inmarsat offers a comprehensive assessment of new International Maritime Organization obligations to protect ship cybersecurity which enter into force in 2021, and their implications for industry stakeholders. By IMO resolution, ship Safety Management Systems must be documented as having included a cyber risk assessment no later than its first annual audit after 1 January 2021, under revisions to the International Safety Management Code.

Developed under the Inmarsat Research Programme, this paper summarises the maritime industry's exposure to cyber threats, identifies the ship-specific vulnerabilities that have driven regulators to act, and explores the precedents from outside and inside shipping for IMO rule development. It cites a survey of over 2,500 risk managers conducted by reinsurance group Allianz as ranking cybersecurity as the second-highest risk for shipping in 2019, behind natural disasters.

The paper also highlights the way threats continue to adapt and evolve, reporting a fourfold increase in cyberattacks on maritime targets that coincides with the industry's move to home-based working through Covid-19. Insights include details of real cyberattacks on ships, covering their source, their target, their initial impact, and their resolution.

Cybersecurity requirements for IMO 2021 provide guidance on Fleet Secure Endpoint, Inmarsat's multi-layered cybersecurity protection, and reporting tool, also outlining IT Best Practices for IMO compliance and the value of Maritime Cyber Security Awareness training developed for Stapleton International by MLA College.

1. Introduction

Developments in connectivity and the transfer of data in greater volumes between ship and shore continue to bring significant gains for fleet management efficiency and crew welfare, but they also increase the vulnerability of critical systems on board vessels to cyber attacks.

A 2019 IHS Markit/BIMCO report* recorded 58% of respondents to a survey of stakeholders as confirming that cyber security guidelines had been incorporated into their company or fleet by 2018. The increase over the 37% giving this answer in 2017 explained a sharp drop in the number of maritime companies reporting themselves as victims of cyber-attacks according to authors – 22% compared to 34%.

However, the enduring feature of cyber threats is

their ability to adapt and evolve, with new lines of attack developed as barriers, are put in place, and strategies to expose vulnerabilities constantly emerging. A June 2020 White Paper** from the British Ports Association and cyber risk management specialists Astaara suggests that reliance on remote working during the COVID-19 crisis coincided with a fourfold increase in maritime cyber attacks from February onwards, for example.

In fact, cybersecurity was ranked as the second-highest risk for shipping in 2019, behind natural disasters, according to a survey of over 2,500 risk managers conducted by Allianz.

Given that, according to IBM, companies take on average about 197 days to identify and 69 days to contain a cyber breach, it is clear that an attack on a vessel's critical systems could threaten the safety of a ship as well as the business of shipping. The fact that a 2019 Data Breach Investigations Report from Verizon indicates that nearly one-third of all data breaches involve phishing provides one indicator that, where cyber vulnerabilities exist, the 'human element' can badly expose them.

The U.S. Coast Guard has already advised ship owners that basic cybersecurity precautions should include: segmenting networks so that infections cannot spread easily; checking external hardware such as USB memory devices for viruses before connecting to sensitive systems; and ensuring that each user on a network is properly defined, with individual passwords and permissions.

From 2021, the Convention for the Safety of Life at Sea that covers 99% of the world's commercial shipping will formalize the approach to cybersecurity permissible for ships at sea.

By International Maritime Organization (IMO)

resolution, no later than a ship's first annual Document of Compliance audit after 1 January 2021, every Safety Management System must be documented as having included cyber risk management, in line with the International Safety Management Code.

The following report offers ship owners and managers guidance covering their responsibilities under the new IMO regime and explains how the cybersecurity solution Fleet Secure Endpoint provides a comprehensive tool to support them towards compliance.

* Safety at Sea and BIMCO cybersecurity white paper. Downloadable at: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cybersecurity-guidelines-2018.ashx

** Managing Ports' Cyber Risks: https://www.britishports.org.uk/system/files/documents/bpa_astaara_white_paper_0.pdf

SUPPLY CHAIN CYBER THREATS AND VULNERABILITIES

THREATS:

- Adversarial: e.g. insertion of counterfeits, tampering, theft, insertion of malicious software.
- Non-adversarial: e.g. natural/man-made disaster, poor quality products/services, poor practices.

VULNERABILITIES:

- Internal: e.g. information systems and components, organizational policy/processes.
- External: e.g. weaknesses to supply chain/ within entities in the supply chain, dependencies (power, communications, transportation, etc.).

2. Cyber Risk Management - The Threat to Ships

One description of cyber risk management used

by IMO sees it as "the process of identifying, analyzing, 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".

The description draws on wording developed by the National Institute of Standards and Technology (NIST) of the US Department of Commerce for Cyber Supply Chain Risk Management (C-SCRM). In full, NIST explains C-SCRM as the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of data-centric information technology (IT) systems and the operational technology (OT) systems monitoring events, processes, and devices. It is a process that covers a system's entire life cycle (design, development, distribution, deployment, acquisition, maintenance, and destruction), given that supply chain threats and vulnerabilities may (intentionally or unintentionally) compromise IT/OT at any stage.

Businesses most commonly experience the consequences of cyber threats as financial penalties, but this is not always the case, as perpetrators can include:

- Terrorism
- Hacktivists groups
- Nation-states
- Insider attacks
- Cybercriminals

While all of the above involve 'bad actors', many attacks are also automated and their source is not immediately apparent: they succeed by repeated or multiple probing for weaknesses in an organization's systems or individual by acts of carelessness by those having access to them.

In addition, cybersecurity can be vulnerable where 'threats' are non-adversarial (e.g. software maintenance, or any activity involving connectivity for a third party onboard).

Effective cyber risk management must therefore consider not only multiple cyber assailants but: diverse lines of attack (targeted and random); continuous efforts by assailants to update strategies including malicious coding; and vulnerabilities in hardware, software, and human behavior.

In 2017, NotPetya ransomware found a point of entry to the Maersk logistics network via its container terminals business. The widely reported incident cost the container giant over $300m in systems renewal, with the group's IT team having to reinstall 4,000 servers, 45,000 PCs, and 2,500 applications in 10 days. Also reported, although in less detail, has been a suspected malware attack that brought the Mediterranean Shipping Company website and portal to a standstill in April 2020.

2.1 Ship Threats and Vulnerabilities

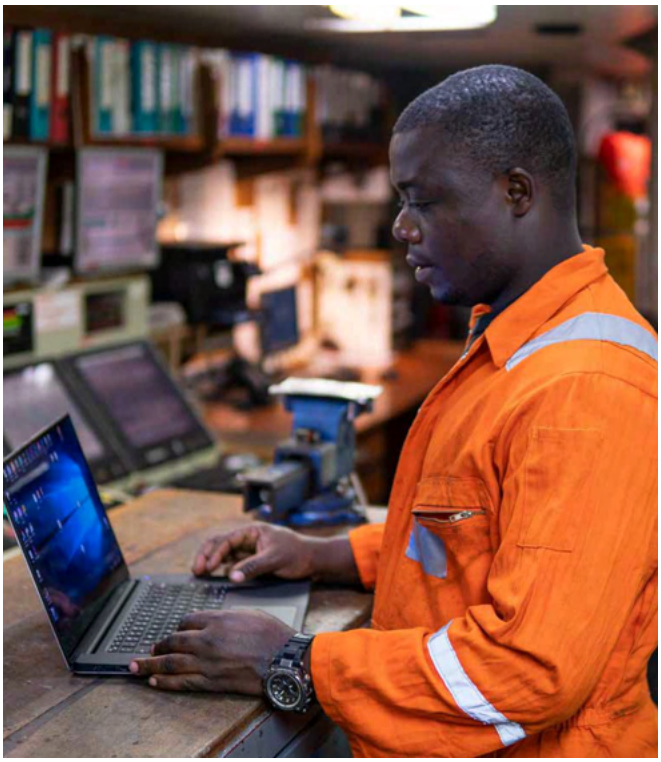
These incidents are in the public domain and involve the land-side systems managed by two of the most sophisticated shipping and logistics organizations in the world, both of which place a premium on the public profiles.

However, ships themselves increasingly play a fully connected data-centric role in the supply chain.

In doing so, common cyber vulnerabilities can be found onboard existing ships, and on some new-build ships. These may include:

- Obsolete and unsupported operating systems
- Outdated or missing anti-virus software and protection from malware

- Inadequate security configurations and best practices, including the use of default administrator accounts and passwords, and ineffective network management
- Shipboard computer networks which lack boundary protection measures and segmentation
- Safety-critical equipment or systems always connected with the shoreside
- Inadequate access controls for third parties including contractors and service providers



If these vulnerabilities are well-known, it is also widely recognized that incidents onboard are under-reported. Furthermore, a hallmark of successful cybercrime will be a lack of publicity. In fact, the full extent of the incidents affecting shipping is therefore hard to gauge. In one alleged incident, a ballast water management system cyber breach saw a ship heeled, with control only returned to the crew after a ransom was paid.

However, the owner apparently preferred to leave the matter unreported, subsequently denying the whole episode over concerns that the ship would not be accepted for charter.

It is nonetheless fair to point out that – for the connected ship – the vulnerabilities listed above are not simply exposed to the same spread of cyber threats as land-based counterparts: they are also subject to the General Data Protection Regulation (GDPR). Effective in EU jurisdictions from 2018, GDPR requires businesses to demonstrate sufficient control and protection over the data they own - especially if they subsequently have a breach. Failure to comply can bring fines of up to 4 percent of an organization's global turnover or £17.5m, whichever is higher.

With more devices on board, and more applications and media channels being used than ever before, some ships are doubling their data usage every six months according to an Inmarsat analysis of its Fleet Express customers. The need for cyber resilience has therefore never been greater.

2.2 Hardware, Software, and Personnel

Understandably, the ship at sea is not itself likely to be the focus for targeted Denial Distribution of Service (DDOS) attacks, whose targets tend to be corporate or more transactional. However, malware and Ransomware can be introduced easily enough to the unguarded ship network, via:

- Terminal hardware
- Software updates
- Misconfigured systems
- Inadequate integration
- Maintenance and design of cyber-related systems

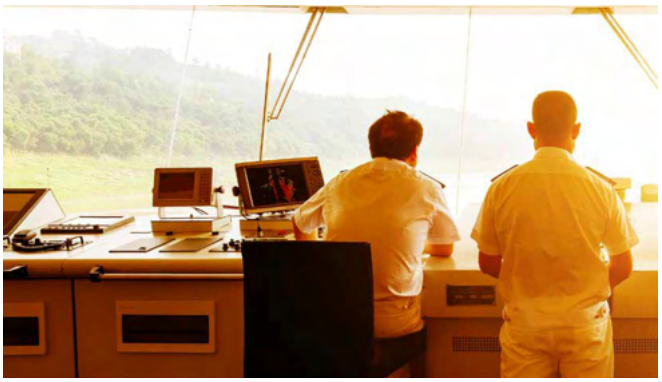
In addition, ship networks are vulnerable to cyber threats arising from:

- Email, Phishing, social media scams, etc.
- USB memory stick as a source of malware
- Downloaded malware
- Connection with infected devices – cell phone, laptop, tablet
- Unauthorized use of bandwidth, exposing a lack of network segregation

These second types of vulnerability relate to 'the human element', and specifically to weaknesses in cyber resilience brought by shortcomings in procedures, training, and awareness among personnel.

Even setting aside the operational headaches, cost of system renewal and expenditure on training that a cyber breach can bring, ships that fall victim to a cyber-attack can expect far-reaching implications that may include:

- Claims against interruption to operations, e.g., a virus affecting onboard systems cause costly delays in getting to the port, potentially leading to cargo claims/charter party disputes
- Loss of business-sensitive information could result in blackmail, with settlement no guarantee of closure
- Insurance cover: impact on premiums due to lack of cybersecurity measures
- Loss of reputation: corporate image tarnished by vulnerability to hackers
- Privacy impact: fined for failing to secure employee information.



3. The Basis for IMO2021

To be approved as IMO-compliant, after 1 January 2021 every ship's Safety Management System MUST include a Cyber Security Plan. However, some will be unfamiliar with the rationale driving 'IMO 2021'.

Regulators have aligned the provisions with International Safety Management Code (ISM Code) guidelines to ensure that companies and their employees, on ship and shore, observe the Convention of the Safety of Life at Sea (SOLAS). The ISM Code requires all identified risks to ships, personnel, and the environment to be assessed and appropriate safeguards to be established.

IMO sees it as the responsibility of the shipowner/manager to "Identify, Protect, Detect, Respond [to] and Recover [from]" cyber attacks through the preparation of cybersecurity planning that can be audited as part of a ship's Safety Management System. These functional elements can be explained as:

- Identify: Develop the understanding to manage cybersecurity risk. 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.
- Protect: Safeguard to ensure delivery of critical infrastructure services. Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- Detect: Develop and implement activities necessary to detect and identify the occurrence of a cyber event in a timely manner.
- Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or

services impaired in the event of a detected cybersecurity breach/cyber-event.

- Recover: Identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber-event. Maintain plans for resilience and to restore all that was impaired by the cybersecurity event.

Guidelines on Cyber Security Onboard Ships Version 2.0 produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, and IUMI describe ship cybersecurity as "an inherent part of the safety and security culture necessary for the safe and efficient operation of the ship". The guidelines are addressed to senior management ashore and onboard personnel alike.

The following section offers guidance on what 'IMO 2021' means in practice for owners

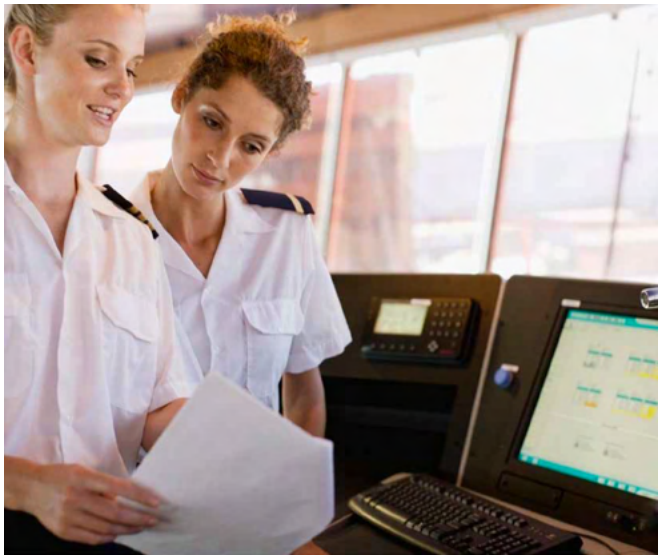
SYSTEMIC VULNERABILITIES

IMO highlights the following ship systems as vulnerable to cyber attack:

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
8. Communication systems

4. IMO 2021 In Practice

By IMO resolution (MSC.428(98)), no later than a ship's first annual Document of Compliance verification after 1 January 2021, any ship's Safety Management System (SMS) will need to take account of cyber risk management to secure Flag State approval, in accordance with the ISM Code.



BIMCO Cyber Security Onboard Ships Version 2.0 Guidelines note that chapter 8 of the International Ship and Port Security Code obliges ships to conduct security assessments, which should include all operations that are important to protect. They should address radio/telecommunication systems, including computer systems and networks and those controlling and monitoring ship to shore internet connectivity. BIMCO notes, in the context of the fast adoption of digitalized onboard OT systems, that systems "have not always been designed to be cyber resilient".

The objective of a ship's Safety Management System (SMS), meanwhile, is to provide for safe practices and a safe working environment by establishing appropriate mitigation measures based on an assessment of all identified risks to ships, personnel, and the environment. As cyber-enabled systems present operational risks, the justification for incorporating cyber risk management into Safety Management Systems is self-evident.

To verify that companies have adequately and appropriately implemented and incorporated appropriate cyber risk mitigation into their SMS,

internal and external audits are required in accordance with the ISM Code. Routine examinations would verify that a management system includes cyber risk management with a cursory review of the system's documentation.

Achieving and documenting compliance relies on ship owners and ships to having had their IT, operating technology systems, procedures, and crew training risk-assessed to demonstrate that they are prepared for cyber attacks and the actions that will be taken should systems be compromised.

The IMO resolution on cyber risk - MSC.428(98)

- references MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management offer an introduction to cyber threats in the maritime domain covering:
- IT and OT systems
- Intentional and unintentional threats
- Identify – Protect – Detect – Respond – Recover
- International best practices – ISO and EN standards

This is all-embracing, and the modular concept of the ISM Code is also flexible enough to offer a framework for continuous improvement that can accommodate cybersecurity in a company's SMS.

Even so, individual companies will clearly vary in terms of systems, personnel, procedures, and preparedness. The risks to a specific ship will also be unique and dependent upon the specific integration of cyber systems aboard.

It is nonetheless up to ship owners and operators to assess their cyber risks and to implement appropriate mitigating measures: each 'Document of Compliance' holder must consider their own cyber risks and implement necessary measures in their SMS.

Incorporating cyber risk into the SMS can take several months, depending on the complexity of the systems onboard the vessel involved. Meeting the 2021 deadline, or the first inspection thereafter will require a combination of technical mitigations, revised (or new) procedures, and staff/crew training to develop a practical and cost-effective route to compliance.

It is important to add that ISM does not prescribe a calendar schedule for assessing new risks, instead advising that they are accommodated as soon as possible. For this reason, the SMS should be considered by owners as a 'live' document that is regularly updated and improved as risks evolve.

4.1 Systems Inventory

Developing a process to identify, protect against, detect, respond to and recover from cyber-attacks is no box-ticking exercise: in the first instance, the shipowner/manager must establish an inventory of all critical hardware and software systems onboard each of its ships, listing the:

- IoT Systems
- Navigation
- Engine Control
- Cargo Control
- DP, Gas, Firefighting, etc.
- ICT – Business Computer System
- ICT – Crew Systems

This list needs to include:

Hardware

- Record make, model, version, function on all your hardware
- Individual hardware (and IP address) and patch panel, power

- Take note of possible attack surface/connection points among your hardware and work to secure them (USB, Ethernet, exposed wiring)

Software

- Record make and version of the applications used on a ship across all hardware. Firmware and software application versions, patch levels, malware protection

Existing documentation should be used as much as possible (especially Technical & Engineering details.

In terms of response and recovery, it is also the owner's/manager's responsibility to formalize the workarounds that address cybersecurity gaps, so that the ship can continue to operate in the event of a cyber attack or its aftermath, or risks can be mitigated. Workaround plans for critical systems and processes should be incorporated into the network and system design and described for Captains in a vessel's emergency manuals. These plans should include instructions and/or a checklist in the event of critical system failure, due to cyber incidents or unplanned system breakdown without a need to request and wait for help from the shore office.

The responsibility for verifying these steps when the ship's Document of Compliance is due for renewal also falls to the ship's owner/manager.

4.2 Risk Assessment Scope

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity or result in a loss of operation of the equipment, system, network, or even the ship. As explained elsewhere, these vulnerabilities and weaknesses broadly fall into one of the following categories:

1. Technical such as software defects or outdated or unpatched systems
2. Design such as access management, unmanaged network interconnections
3. Implementation errors for example misconfigured firewalls
4. Procedural or other user errors

4.3 Responsibilities

IMO 2021 requirements do not cover servers or staff onshore, but they clearly have a major impact on fleet management. For example, the individual managing the Fleet IT policy and documentation (usually, the 'Fleet ICT Manager') will would also normally be responsible for the owner/manager ISM documentation system for ships, for example.

Critically, under IMO 2021, at a minimum, a ship's SMS will identify the party ashore and onboard taking responsibility for cybersecurity (ICT Manager, Chief Security Officer, or any other).

In broad terms, that individual will take responsibility for:

- Having an understanding of the extent of cyber risks
- Managing crew awareness of and preparedness for threats to the vessel's systems
- Steps to secure ship systems to minimize the impact if a threat is actualized

Given that, in line with the ISO27001 standard, IMO 2021 also states that the owner's risk assessment should be auditable for the following attributes:

- The hardware installed
- The software in use
- Details of what is connected to the network
- How the above is protected

The Fleet ICT Manager will need to work with the Head of Crewing to ensure that Crew understands the importance of cyber security and have been trained either in the classroom or online. A record of the crew's performance in these training exercises should be kept on file by the HR/Crewing department.

RELATED CYBER SECURITY GUIDELINES

IMO's Guidelines on Maritime Cyber Risk Management refer to three specific guidelines as having been developed to help shipping get 'cyber ready':

1. Guidelines on Cyber Security Onboard Ships – BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL.

Guidance to ship owners and operators on procedures and actions to maintain the security of cyber systems in the company and onboard ships; designed to help owners understand, and manage:

- Limitation and control of network ports, protocols and services
- Configuring network devices such as firewalls, routers and switches
- Secure configuration of hardware and software
- Protecting web browsing and email
- Satellite and radio
- Communications
- Defences against malware
- Data recovery capability
- Wireless Access control
- Application software security (patch management)
- Secure network design
- Physical security
- Boundary defence

The BIMCO guide also includes procedural controls for crew, including training and awareness, software maintenance and upgrades, and anti-virus updates. However, the guidelines are not a basis for external auditing of a company's/ship's approach to cyber risk management.

2. **NIST framework**

Published in 2014 by the US National Institute of Standards and Technology, the NIST CSF guide focuses on the same five functional elements presented by the IMO for risk management - Identify, Protect, Detect, Respond, Recover, to assist organisations in:

- Describing their current cyber security posture
- Describing their target state for cyber security
- dentifying/prioritising opportunities for improvement within a repeatable process
- Assessing progress toward the target state
- Communicating among internal and external stakeholders about cyber security risk

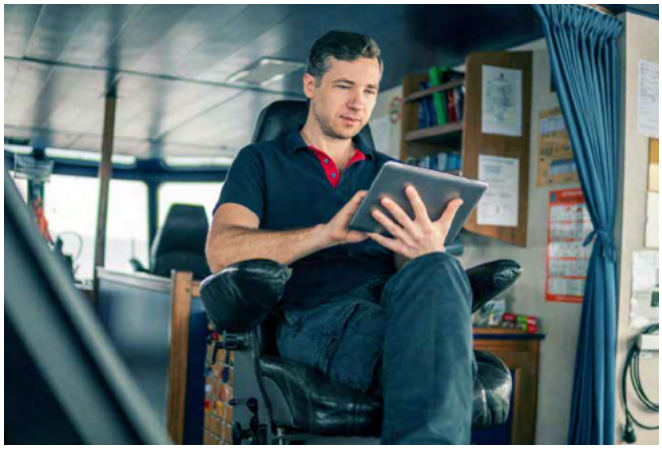
The NIST framework includes usable profile templates for use in risk assessment profiling at the individual vessel level. The resulting profile will help to identify and prioritise actions to align policy, business and technological approaches in order to manage and reduce risks. Sample profiles are publicly available: http://mariners.coastguard.dodlive.mil/2018/01/12/1-12-2018-release-of-offshore-operations-and- passenger-vessel-cybersecurity –fraework -profiles

3. ISO27001

The ISO27001-Annex A of cyber security objectives is published currently as ISO 27002. Here, cyber security controls are not specifically focused on Critical Infrastructure Protection or on the Maritime Industry, but with appropriate focus on cyber risk they may be applied by any organization. ISO27001 is also the only information security management system standard that can be independently certified with a level of authority.

5. IMO 2021 COMPLIANCE

Managing cyber risk onboard ship is considered a natural extension of current operational risk management practices incorporated into existing Safety Management Systems within the existing ISM Code.



The relevant MSC.428(98) - Maritime cyber risk management in safety management systems resolution, therefore:

- Affirms that an approved safety management system should consider cyber risk management in accordance with the objectives and functional requirements of the ISM Code.
- 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.

The owner/manager must be able to demonstrate to Port State Control or any other recognized authority the ship, its systems, and its crew are prepared for cyber risks and what to do about them in the same way that they would need to document any other safety issue.

Therefore, prepared answers are needed to the questions:

- What assets do we have (kind of hardware/ software and what is connected to the network)?
- What would we do if they do not work?
- How are assets protected?
- What would we do if they were compromised?
- Who has control ashore and onboard?

As well as being able to liaise with or identify the person responsible for cybersecurity on the ship, the Port State/Flag State/RO auditor should be able to check that the Safety Management System documents this and shows that the ship's owner or manager:

1. Has identified the systems on-board and outlined the relevant cyber risks
2. Has the ability to detect breaches in cybersecurity onboard
3. Has measures in place to protect systems and software onboard
4. Has response measures in place to deal with a cyber-attack, specifically related to system redundancy, training, and workaround plans

5.1 Responding to Cyber Attacks

The Cyber Security Plan should, at minimum, include:

- A process for initial incident triage
- Steps to quarantine all electronic traffic to and from ship or fleet. Procedures for alerting and requesting communication vendors to check traffic
- Procedures for keeping corporate IT security department abreast of the situation
- Procedures to secure/establish backup communications to the affected vessel(s)
- Steps to stabilize and isolate the infected system to guard against further spread
- Steps for gathering Intelligence and evidence from affected systems
- Procedures for executing recovery of critical systems remotely
- Arrangements for completely replacing the ICT system at the next safe port after the cyber event

5.2 Recovery from Cyber Attacks

Workaround plans are required to take account

of possible failures in critical shipboard systems, with the processes described in a vessel's emergency manuals so that the Captain can respond without the need to ask for help from/wait for shore-based colleagues. These plans should provide the Captain with instructions and/or a checklist on what to do.

In the case of cyber resilience, workarounds plans might include:

- Actions to restore crashed/ failed email clients or degraded/failed ship-shore communication links; use backup FleetBroadband for email/voice until recovery
- Actions to work around/recover failed PCs
- Usage of citadel telephone to send telex; testing of backup email ID from ship-to-shore and from shore-to-ship
- Fall back to paper charts in case of compromised ECDIS

In all cases, the Fleet ICT Manual inserted into the Ship's SMS/ISM Code documentation should provide full guidance ad document the Cyber Response Plan for all critical on-ship systems.

5.3 Training for Cyber Attacks

As the Plan is part of the Vessel's ISM it is also essential to periodically carry out drills to test any issues, train the crew, HSSE team, and any other stakeholders on how to respond to a cyber incident on board ship, and encourage a culture of continual improvement. This means ship owners and managers should give cybersecurity drills the same weight as they give any regular Incident Management Drill – whether for grounding, ship fire, or collision.

Under the new regime, cyber drills should be conducted across the fleet at least once a year to test response procedures and assess crew preparedness, procedures during a cyber incident onboard. It is essential that the Ship Manager's Incident Commander takes charge and demonstrates include:

- Fleet Secure Endpoint - a powerful multi-layered endpoint security solution for remote monitoring of onboard computers
- Fleet Secure Cyber Awareness - a mobile training app for the crew to gain up-to-date cyber security knowledge

The following section of this report offers guidance covering Fleet Secure Endpoint, with a specific focus on the digital tool's potential to offer direct support to ship operators/owners seeking to implement IMO 2021-ready cyber security SMS.

While not representing compliance itself, Fleet Secure Endpoint implementation provides ship network protection based on IMO's 'identify, detect, protect, respond, recover' pillars for cyber security planning. In offering a fully IMO-compliant reporting solution, it also supports operators/owners to achieve compliance at every stage in an orderly and straightforward manner.

THE COMPLIANCE CHECKLIST

1. As a ship owner/manager, to defend your IT set-up you MUST:

- Know what you have: all IT systems/systems controlled by IT - including Main Engines and Navigation Systems, etc.
- Defend what you have: to fight off basic threats to your organization, systems should be designed to guard against failure, using Software/Hardware/Ship's Systems redundancies.
- Defend what you have: to fight off basic threats to your organization, systems should be designed to guard against failure, using Software/Hardware/Ship's Systems redundancies.
- Be able to recover workarounds and recovery processes must be in place for ICT and Ship's systems, with crews trained and at least Yearly Incident Drills for Cyber Security.

2. However, IMO 2021 Compliance is NOT just about defending ICT against cyber threats. It is about Total IT Best Practice on a ship's.

- IT system AS WELL AS
- Technical, Navigation, Safety and Mechanical Systems.

3. Therefore, as an IMO 2021-compliant cyber secure ship owner/manager, you MUST:

- Know what they have – Establish and record all the systems (ICT and Technical) used on your ships (including make, model, version, software updates, supplier, etc.).
- Defend what they have - Ensure that steps are being taken to harden ICT and Technical systems against cyber threats.
- Be able to recover – update all documentation onboard to include guidance on what to do in case of IT or Technicalsystem failures on ship, including IT Policy in ISM Manuals, Training for Crew, Workarounds Process and Drills.

6. Fleet Secure Endpoint - An Introduction

Inmarsat's objective is to deliver cyber resilient digital services and mission-critical communications to its global maritime customers. It does so by:

- Embedding threat-based risk management into Inmarsat systems, products, and services
- Delivering operational resilience by identifying, managing, and responding to cyber threats with people, process and technology capabilities
- Fostering a culture where Inmarsat people embrace security and where threat-based security measures are embedded in their day-to-day working
- Sustaining a demonstrable framework for effective, efficient, and adaptable threat-based cyber risk management

Day-to-day protection of Inmarsat's Information Systems infrastructure is the responsibility of the Security Operations Team. Inmarsat has instituted an in-house 24/7 Cyber Security Operations capability that collaborates actively with the cybersecurity intelligence community as well as Cyber Security, our partners, and maritime customers to tackle cyber threats and manage incidents.

6.1 Security and Endpoints

Security devices such as Unified Threat Management/Next Generation Firewall sit at the ship network level, where they detect and protect against attacks commonly made from shore to ship and vice versa. However, while network monitoring will display a detailed view of the vessel's IT infrastructure, it will not have any jurisdiction over the endpoint, meaning that endpoints such as business-essential PCs and crew laptops remain at risk.

Traditional anti-virus solutions were not really designed to prevent the sort of sophisticated and targeted malware that has become the mainstay of today's maritime cyber threat landscape. They were conceived around a machine-centric view of security and worked by scanning and quarantining suspicious files to prevent them from being launched and were not geared to offer protection against attacks launched on a machine from its host network.

Conventional AV software requires constant updates of new signature files to remain current. Having only one security feature to protect the endpoint will rely heavily rely on a signature set by one security vendor and, in many cases, individual security vendors will not catch 100% of malware. To maintain integrity, a full system scan would also be required after every update, which would often slow the machine's performance to a crawl and frustrate end-users.

If no or lower forms of security is installed on the endpoint, then it is at risk of infection even if the ship network is protected by a security device.

For example, someone plugging a USB into the computer can infect it even without clicking anything. If a network security device is being used, then it may recognize the device is infected but cannot clean the infection.

With new variations of malware emerging almost daily, no single vendor was able to keep up and include all new signatures in their database. Cyber criminals' preference for the latest iterations shows they know this and actively exploit the lag between new malware being detected, a signature being developed, and an update is issued and installed.

Inmarsat Fleet Secure Endpoint (FSE) avoids many of these shortcomings as it was built from scratch with a network-centric view of security in mind but targets endpoints. Endpoint protection is a crucial step to ensuring layered protection and not just relying on firewalls, company policies, and network security devices to be the saving grace for security.

6.2 FSE Onboard

Fleet Secure Endpoint provides an extension of security to all endpoints on a vessel and delivers several security functions in a single managed service which protects everything from business essential PCs to crew laptops. FSE can be applied to multiple Inmarsat maritime services – Fleet Xpress, FleetBroadband, and Fleet One.

Fleet Secure Endpoint scans the network for security issues and records its findings, providing an auditable trail covering alerts and network status. Its reach extends to any new devices joining the network. Whilst FSE itself does not deliver IMO 2021 compliance, it provides the shipowner and ship manager with a cybersecurity solution that facilitates and supports compliance.

MORE THAN ANTI-VIRUS
Standard anti-virus is no longer adequate protection

	GENERIC ANTI-VIRUS (Bitdefender, Symantec, etc.)	ENDPOINT PROTECTION (ESET Protection)	FLEET SECURE ENDPOINT
Anti-Virus (Anti-Spyware, Anti-Phishing)	R	R	R
Web control		R	R
Two-way firewall		R	R
Botnet protection		R	R
Ransomware prevention		R	R
Multi-engine scanning			R
Network monitoring			R
Asset inventory (software, hardware, driver, etc.)			R
Endpoint health status alerting			R
Endpoint threat alerting			R

7. Fleet Secure Endpoint and Fleet Xpress - Supporting IMO2021 Compliance

Fleet Secure has been designed to align with IMO's five pillars for cyber resilience, namely: identity; detect; protect; respond; and recover, while its reporting function has been developed with IMO compliance in mind. In addition, an ISO 27001 audit of FSE conducted by DNV GL describes Fleet Secure Endpoint as a single product that can assist in achieving IMO 2021 compliance. Although Fleet Secure Endpoint works across all of Inmarsat's maritime services, to maximize protection and compliance FSE should be used in conjunction with Fleet Xpress, which provides reliable high-speed internet access with the ability to separate crew and business traffic and make it easier to respond and recover to attacks.

7.1 Identify

Fleet Secure highlights where errors and warnings have occurred in the vessel/fleet, which enables the designated security personnel to quickly ascertain potential weak spots that require further investigation. It does this using a powerful network scanning and monitoring module, called Teyla, that automatically detects devices on the local network and checks whether Fleet Secure Endpoint (FSE) is installed. If not endpoints will be marked as 'rogue nodes' and alerts are raised as an alert. The designated security officer can either allow or deny network access privileges to that device.

This oversight means someone on the vessels is always aware of what is connected to their network. To aid network audits, on machines where installed, FSE will also collect data on installed software, hardware, and system configuration.

7.2 Protect

FSE is built around ESET Endpoint Security, an award-winning enterprise-grade endpoint security product, and has special adaptations for use in a maritime setting. It not only detects and blocks files with known signatures from operating but monitors low-level system calls and actively analyses software for suspicious behavior in real-time.

- Botnet protection shuts down malicious connections to known botnets. Botnets hijack a machine without the owner's knowledge to carry out Distributed Denial of Service (DDOS) attacks. When activated, they consume processing power and cause spikes in bandwidth consumption.
- Multi-engine scanning broadens detection by using malware signature databases from multiple security vendors so that new fingerprints not known by all vendors are included during the inspection.
- Ransomware prevention detects and prevents malicious encryption attempts before they have a chance to initiate and encrypt the device.
- A two-way endpoint firewall blocks malicious incoming and outgoing network traffic.
- Anti-spyware terminates malicious applications designed to steal sensitive information.
- Anti-phishing blocks connections to sites known to extract confidential user information.
- Web control allows the system administrator granular control over the website's users can visit.
- Endpoint Threat alerting sends an email notification to the system administrator listing recently detected threats on vessel/s.

7.3 Respond

Knowing how to react during and after a cyber-incident is critical to a well-rounded cybersecurity strategy. It is necessary to envisage a wide range of potential scenarios and plan the steps needed, to contain their impact on vessel operation and safety, and secondly to restore impaired systems and recover data in a timely fashion.

FSE can assist the response stage in several ways. In contrast to off-the-shelf products, the service is enhanced by round-the-clock monitoring by a dedicated team of IT experts based in the Security Operating Centre, who check security events or other signs of unusual network activity on a vessel as and when they occur. They are supported by marine engineers with extensive knowledge of different hardware and software systems found on modern vessels.

Via the portal, the ship owner's in-house IT team can roll out updates in real-time to configurations quickly and remotely to all computers installed with FSE in the wake of an incident, in order to prevent an attack from spreading across the fleet and reduce exposure to similar attacks in the future.

Additionally, the shore-based portal retains a centralized log of all flagged security events and allows bespoke alerts to be created. For example, alerts can be set up to warn when a certain virus or class of virus is detected or certain software requires updating.

The asset management functionality incorporated into FSE gives offers a clear overview to designated security personnel and IT staff of which devices are onboard and which devices have FSE installed. It also provides detailed information on assets and the software environment available for responding to an incident and for analysis during the post-incident review.

- Alerting offers pro-active insight on what is happening onboard and helps react to incidents
- Alerts can be created to E-mail the user when events happen on board, such as virus detections or outdated software
- A single agent handles all Fleet Secure Endpoint related activities and multiple software packages are not needed, saving system resources
- A 24/7 Security Operations Centre takes action when needed

7.4 Recovery

If an infection is detected onboard, Fleet Secure Endpoint will automatically detect the infection and respond by blocking it, removing it, and finally reporting it. The built-in memory analysis will detect both known threats and new security vulnerabilities. If FSE recognizes a file to be malicious, it will be stored in a dedicated

quarantine location on the device. Quarantined files are stored in a location that ensures the malicious file cannot infect the system.

Once a security incident has been brought under control and the immediate threat has been neutralized, attention shifts to restoring and reconnecting systems needed for normal vessel operation. Work also begins on investigating the exact cause of the incident and taking measures to prevent a recurrence or similar event from taking place elsewhere in the fleet.

7.5 Reporting

FSE comes with extensive built-in reporting functionality which can help in this exercise. A full report can be created on the vessel, containing a record of all devices connected to the network, their hardware, and the software that is installed. This report can be given to port state control and/ or authorities to show them the vessel has been taking adequate steps to minimize cybersecurity risks on board. While FSE implementation does not achieve compliance, Fleet Secure Endpoint reporting is fully IMO compliant.

The Fleet Secure Endpoint Security report shows the following:

- Network-connected devices with Fleet Secure Endpoint installed, devices without FSE installed
- System specifications such as free disk space, CPU, and amount of memory
- Installed software and their version
- Security events such as neutralized viruses and blocked USB drives
- Acknowledgements of the Security Operations Centre team based on security events

Reports are generated in formats like PDF and can be printed on board so that the master of the vessel can circulate them among staff and easily integrated into a vessel's safety management manual, or show port inspectors that steps have taken steps to protect the vessel and its assets. Even if a vessel has not been the target of an attack, Inmarsat recommends that these reports are periodically reviewed to steer ongoing improvements to a vessel's cyber risk management plan. Any Cyber Review in the Change Management Process should

- Include ICT staff when making major changes in the ship's system
- Ensure Cyber Security in the end-to-end process when supplying new equipment

7.6 Manageability

Using the Fleet Secure web portal the ship operator/owner can remotely upload configurations to be implemented onboard so that Fleet Secure Endpoint can be configured remotely. The user can also configure alerts to reflect owner/operator preferences so that events such as virus detections or blocked network attacks are also flagged up.

In common with any proposed solution, Fleet Secure Endpoint will only assist in reaching IMO compliance when correctly implemented: this means the risk assessment needs to have been completed, while the FSE monthly report will be included in the Safety Management Manual.

FLEET SECURE ENDPOINT - THE COMPLIANCE CHECKLIST

1. As a ship owner/manager, to defend your IT set-up you MUST:

- Know what you have: all IT systems/systems controlled by IT - including Main Engines and Navigation Systems, etc.

- Defend what you have: to fight off basic threats to your organization, systems should be designed to guard against failure, using Software / Hardware / Ship's Systemsredundancies.
- Be able to recover: workarounds and recovery processes must be in place for ICT and Ship's systems, with crews trained and at least Yearly Incident Drills for Cyber Security.

2. However, IMO 2021 Compliance is NOT just about defending ICT against cyber threats. It is about Total IT Best Practice on a ship's

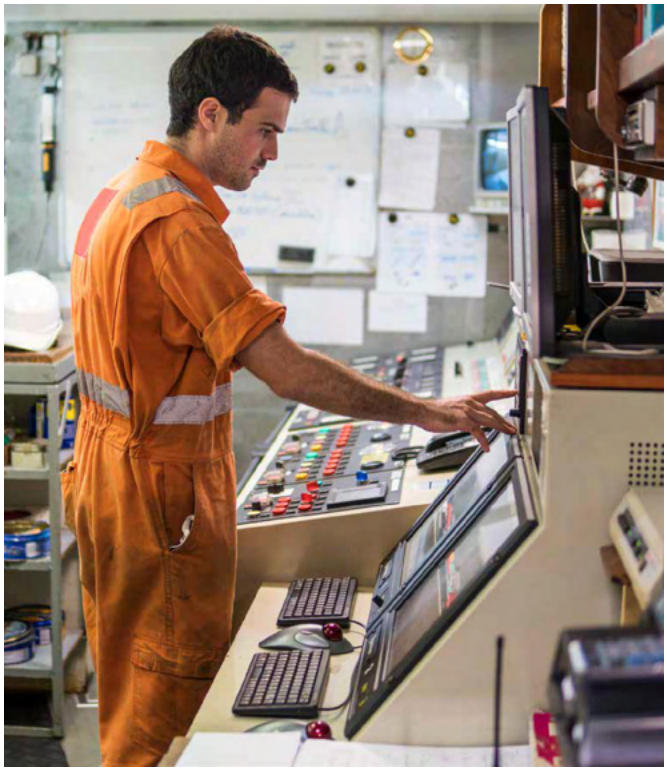
- IT system AS WELL AS
- Technical, Navigation, Safety and Mechanical Systems.

3. Therefore, as an IMO 2021-compliant cyber secure ship owner/manager, you MUST:

- Know what they have – Establish and record all the systems (ICT and Technical) used on your ships (including make, model, version, software updates, supplier, etc.).
- Defend what they have - Ensure that steps are being taken to harden ICT and Technical systems against cyber threats.
- Be able to recover – update all documentation onboard to include guidance on what to do in case of IT or Technicalsystem failures on ship, including IT Policy in ISM Manuals, Training for Crew, Workarounds Process and Drills.

4. FLEET Secure Endpoint helps you, as a ship owner/manager to:

- Step 1 Know What you have: FSE includes a module logging any new hardware added to your network.
- Step 2 Defend what you have: via strong AV, WebControl, Network Monitoring.
- Step 3 Recover – FSE's crew training module coversa significant part of the trainingneeds demanded for IMO 2021Compliance.



FSE KEY BENEFITS:

- No additional hardware is required. Protections are primarily introduced at the network level, with 'lightweight' installed software needs on the end-user machines to handle updates and communicate system status back to the server PC
- Multi-layered security. In addition to anti-virus, Fleet Secure Endpoint features anti-phishing, anti-spyware and botnet protection among other features
- Enhanced network oversight: FSE includes sophisticated remote network monitoring of endpoints
- Remote monitoring and auditing: Shore-based portal lets in-house IT teams keep track of all security events, set up alertsand remotely roll-out configuration updates
- Remote monitoring and auditing: Shore-based portal lets in-house IT teams keep track of all security events, set up alertsand remotely roll-out configuration updates

- 24/7 Security OperationsCentre: FSE is supported by a dedicated team of trained cyber security experts and marine engineers, with engineers having been onboard vessels and so fully aware of the environment
- Low bandwidth consumption: Averages only 7Mb data per vessel per week, with lower options available on request (for vessels that are at always-onconnection with no data limitthe data usage ishigher)
- Tailored for maritime: One server locatedon the vessel to manage all endpoints

8. Fleet Secure Endpoint - Installation and Use

Despite its superior scope and functionality, Fleet Secure Endpoint is as straightforward for the user's ICT team to install as conventional anti-virus software developed by Inmarsat to protect ship systems (AmosConnect AV and Globe AV).

8.1 Fleet Secure Endpoint Installation

For a standard vessel network and under normal circumstances, and taking account of safety guidance offered by vendors, the installation can be expected to be completed on clean computers in approximately two hours.

The clean computer provides the optimum case for any anti-virus software installation, however. Pre-existing anti-virus software can present challenges and the user's ICT team will need to remove it before Fleet Secure Endpoint is installed. Inmarsat provides user guides/scripts to support the removal of third-party anti-virus software.

Even so, it should be emphasized that there is no requirement for the ship network to stop working in order to install or operate Fleet Secure Endpoint. Fleet Secure Endpoint has a built-in firewall, where ports can be opened for for the most commonly used applications on board.

The Inmarsat Security Operations Centre offers oversight for internet-connected ships to support installation and the removal of old systems.

8.2 Fleet Secure Endpoint in Use

Once installed on a device, Fleet Secure Endpoint will start reporting to the web portal. The web portal can then be used to view elements such as (but not limited to):

- Installed software
- Running windows services
- How long the system has been running
- Device hardware, such as remaining hard drive space, type of processor, etc.
- Which operating system the device is using

The portal has two versions, namely ship, and shore. With the ship version, all activities performed onboard can be accessed, including holding download files for clients' manuals and mapping out of all endpoints onboard the vessel. However, the shoreside portal holds detailed information such as events and alerts for the fleet and also for each vessel. The IT team of the vessel or fleet will have access to the shoreside portal.

It is also possible to view the results of the network scans performed onboard and see which devices do or do not have Fleet Secure Endpoint installed. For the devices that have Fleet Secure Endpoint installed advanced logging is available, allowing users to see things such as (but not limited to):

- Firewall logs (when an attack or an event happens which triggers the firewall)
- Device control logs (when USBs were inserted, whether they were blocked)
- URL blocker logs (whether sites were blocked)

8.3 Dashboard and Alerting

The Fleet Secure Endpoint web portal can be used to view events that occur on the vessel and configure alerts based on those occurrences. Alerts will notify the user or multiple users via E-mail. The user can configure alerts for events such as (but not limited to):

- Virus threats (receive a notification if a virus is detected)
- Firewall events (receive a notification when an attack/event happens which triggers the firewall)
- When a new device has been detected on the network that does not have FSE installed
- Software version control (receive an alert when a new version of installed software is available)
- User intrusion detection (receive an alert when a failed login occurs)

Multiple OS Fleet Secure Endpoint supports multiple operating systems. For Windows operating systems, Vista and up is supported. OSX, Linux, and their mobile counterparts IOS and Android are also supported.

Fleet Secure Endpoint has distinguished itself from Endpoint Detection & Response (EDR) packages. While these solutions are highly effective, they demand a strict ship networking setup to 'signature' and check every file on the vessel, consuming huge amounts of data. FSE addresses attacks and infections without needing to signature each file, saving on costs and data usage. In fact, FSE frequency and control reporting times can be adjusted, with data usage as low as 5MB a month. Where ships have internet connectivity, Inmarsat recommends more frequent reporting of network status so that its security operation center can take swift action when malicious traffic is detected.

In addition, Fleet Secure Endpoint can be used onboard vessels using FleetBroadband as their connectivity solution. In this case, trench rules need to be set correctly and onboard firewalls (if any) must be updated to accommodate Fleet Secure Endpoint IPs and port numbers.

8.4 Fleet Secure Endpoint Use in Context

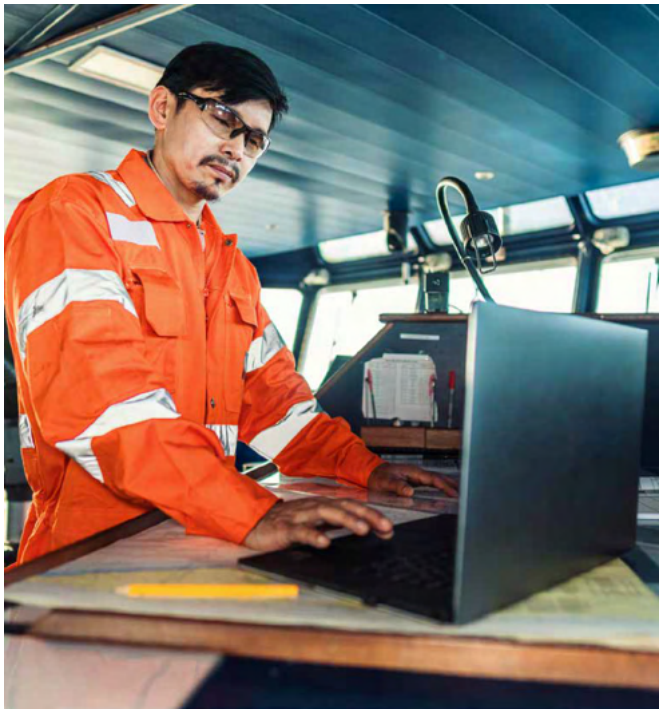
As noted earlier, Fleet Secure Endpoint installation provides a route towards IMO 2021 compliance, rather than offering a complete compliance solution. However, in summary, IMO 2021 can be achieved using Fleet Secure Endpoint and its cybersecurity reporting/response functionality covers all of the IMO 2021 guidelines into the ship's Safety Management Manual.

Scenario: a crew member opens a phishing email

The Fleet Secure Endpoint response:

- Scenario 1: If FSE is fully updated then it should have detected that virus.
- 1.1: The SOC is notified of this activity.
- Scenario 2: FSE is not updated,the virus is not detected, and the ransomware process is not stopped.
- 2.1: The SOC is notified of this activity.
- Scenario 3: The firewall in FSE introduces segmentation of the network so that the virus cannot spread to other PCs as they block the incoming attack.

Fleet Secure Endpoint handles all of these scenarios automatically. An option is also available to block out an endpoint from the network remotely.



9. Cybersecurity, Crew Training, and Awareness

Cyber attacks are constantly evolving and becoming more devious in their workings and, while technical countermeasures will stop the vast majority of attempted attacks, they are intrinsically reactive in their operation.

The remainder of the protection relies on staff vigilance, preparedness procedure and, understanding, weak cybersecurity in any one of these areas may undermine robustness elsewhere. Crew education is, therefore, an indispensable component in a well-rounded security strategy: a small investment in training and awareness can prove enormously valuable.

Alarmingly, a 2018 Futurenautics survey that recorded 47% of vessels as having come under cyber attack and 80% of cyber breaches as resulting from individual errors also saw 85% of crew reporting that they had never received any cyber training. Some estimates suggest that 50% of ship system disruptions are the result of USB 'abuse', where infected memory sticks or mobile devices (including secondhand phones) are plugged into the port. Other common cyber weaknesses include easily guessed passwords and responsiveness to phishing.

In bringing Cyber Risk Management into the ISM Code, MSC 428 (98) follows the September 2019 edition of the Tanker Management Self-Assessment (TMSA) scheme and the latest Ship Inspection Report Programme (SIRE) questionnaire to include cyber awareness training in IMO guidelines mandatory requirements.

Inmarsat has been one of the partners contributing to a Maritime Cyber Security Awareness training course developed for Stapleton International by MLA College, which is available to users of Fleet Secure Endpoint at a discounted rate. Using a combination of video modules, transcripts, and a concluding test, the course has been developed in accordance with BIMCO, IMO, ICS, and IACS guidelines and have been approved by the Institute of Maritime Engineers, Science and Technology and the University of Sunderland, UK. It is also in line with the provisions of the TSMA self-assessment.

Uniquely, the course is deliverable by an app for download through Google Play and AppStore to smartphones, tablets, and laptops, after which it can be accessed offline. Guidance based on the full extent of IMO Cyber Awareness expectation can therefore be learned during voyages without the need for scheduled classroom training during busy port stopovers, or even connectivity.

Focusing on the basics of cybersecurity for the maritime user, the course is suitable for all levels ashore and at sea, enabling seafarers to familiarise themselves with attacks they are likely to encounter in their day-to-day duties. It

also offers practical tips on how to avoid becoming a victim or endangering their vessel.

Each 30-minute training module covers:

- Digital threats using personal information
- Digital threats using IT devices
- The physical and human threat
- Final competency test and completion certificate

Subject to achieving a score of 80% from 20 randomized questions, seafarers receive a certificate valid for four months from the University of Sunderland and a certificate of Continuing Professional Development from the Institute of Marine Engineering, Science and Technology.

By completing this course, all personnel will be able to further understand the principles and actions they must adhere to, thus ensuring that they are fully compliant with the TMSA and IMO regulations. It will also help allay the fears of many within the sector and ensure that they remain cyber safe at sea.

10. Fleet Secure Endpoint - Real Case Studies

CASE 1

Vessel type: Undisclosed
Assailant: Multiple infections with a normal anti-virus installed

The customer was using Palo Alto cybersecurity software when the vessel was hit by multiple infections, including Trojans, Worms, and data exfiltration viruses infesting the system. The customer decided to install Fleet Secure Endpoint as part of a shipboard trial. Inmarsat's engineer found 79 infections that had not previously been detected.

Among the significant findings, the HTTP Filter detected users onboard unknowingly visiting websites serving malicious code. The connection was dropped, and the user was informed accordingly. Again, the FSE email filter detected infected attachments, including:

- CoinMiner.T trojan (A trojan that uses system resources to mine cryptocurrency for its distributor)
- TrojanDownloader.Agent.OJL trojan (a trojan capable of downloading and executing other malicious code)
- Agent.AQ trojan (A trojan agent template frequently used as a starting point for malicious code that can be modified to do whatever the malicious actor wants)

The FSE email filter disposed of these infections, preventing further infections.

CASE 2

Vessel type: Liquid Ethylene Gas Carrier
Assailant: Emotet trojan, causing vessel operations to stop

Emotet is well-known as a trojan in banking circles but was detected as infecting the majority of machines onboard a LEG Carrier, becoming active whenever a PC was switched on. The virus can intercept and exfiltrate data transmitted and saved when the user is browsing banking websites, resulting in leakage of sensitive data and malicious use of the user's banking details.

As part of a Fleet Xpress agreement, the ship was equipped with two Fleet Secure Endpoint security modules, installed across all PCs onboard:

- Advanced Memory Scanner – This detected Emotet in the memory, terminated, and blocked it from recurring.

- Heuristic Intrusion Prevent System (HIPS) – This detected the malicious code being executed and stopped the execution of this code.

The virus was successfully cleared from the memory on all infected devices.

CASE 3

Vessel type: Undisclosed
Assailant: Sohanad worm

A USB memory sticks infected with the NCB worm Sohanad was connected to an endpoint onboard ship. Sohanad spreads via removable media and shared folders: once it has infected any part of the network, it tries to replicate itself by infecting applications and files.

Two Fleet Secure Endpoint security modules were implemented:

- Real-time file system protection – Detected that files were being infected and automatically halted the process from accessing files so they could be investigated by the engine.
- Heuristic Intrusion Prevent System (HIPS) - Detected the malicious code that was causing the replication and stopped the execution of this code.

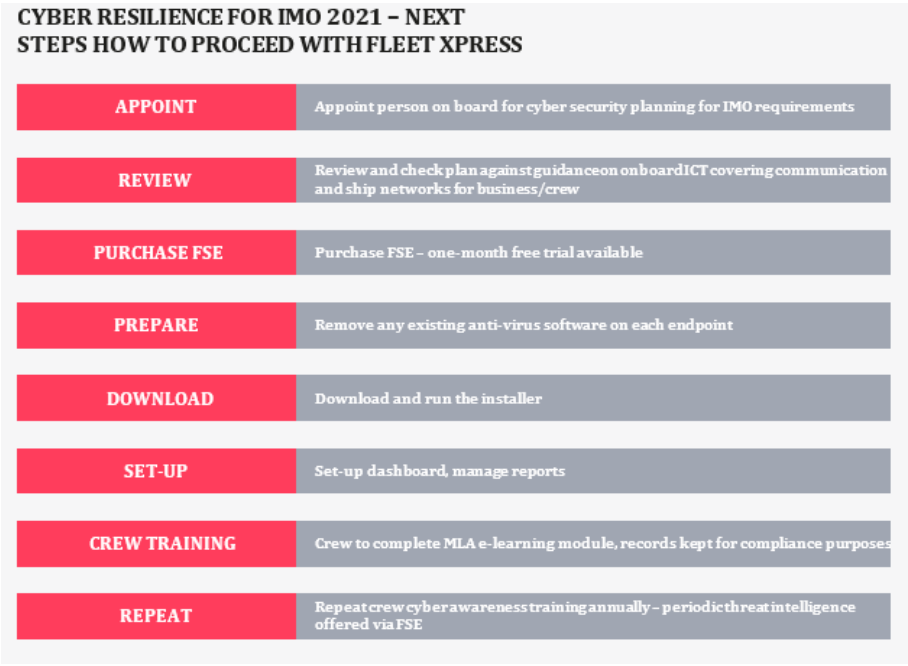
Fleet Secure Endpoint was able to stop the infection from continuing, cleaning 17.000 infections in the process.

CASE 4

Vessel type: Bulk carrier
Assailant: CoinMiner

The vessel in question had trialled Fleet Secure Endpoint. After the trial's conclusion, the ship ran for two months without FSE. On re-installation of FSE, all devices onboard that were tested were found to have been infected with a CoinMiner.
CoinMiners use a device's processing power to mine cryptocurrency for the attacker without the user's knowledge.
FSE was able to neutralize all threats.

11. NEXT STEPS – HOW TO PROCEED



Authors Biography

Mark Warner
Director, Inmarsat Maritime

Mark joined Inmarsat in September 2016 and has responsibility for maritime communications activities. With over 20 years of experience in the maritime industry, Warner has an extensive track record in digital platform development and programme creation for ship owners, managers, and suppliers. He has sector-specific experience in data analytics, E-commerce, lead generation and public relations, and social media.

A University of Plymouth alumnus, holding an MSc in International Shipping & Logistics and a BSc in Maritime Business & Law. Mark spent five years in the Royal Naval Reserve sailing on a variety of vessels including Frigates and Mine Sweepers.

For further information and questions, please contact the Inmarsat Maritime Security Services team: Maritime.Security@inmarsat.com

The Importance of Noise Management Early in the Design Process of Marine Installations

Daniel Alvarez, M.Sc. Acoustics

Vysus group

Abstract

Headaches, tiredness, stomach ulcers, hypertension, vertigo, nausea, a permanent whining, buzzing, hissing, or humming in the ears. Noise can also damage hearing permanently in the worst cases. Excessive noise reduces work efficiency and increases absenteeism. In extreme cases, noise can be fatal if there is so much noise that personnel cannot hear instructions or alarms. Good noise performance is critical to the business performance, safety, and environmental excellence of any asset. Good noise performance is largely a question of good management, coupled with the necessary technical expertise.

Noise management practice varies from high risk, zero cost "do nothing!" approach to a low risk, high cost "do everything possible!" Apart from the operational penalties of inadequate or non-existing noise management – harm to personnel, environmental damage and reduced performance – the immediate financial risks of the "do nothing" approach are increasing as authorities around the world become more acutely sensitive to the issue of noise in the welfare of workers and the environment. Permits and licenses may be revoked on the basis of poor noise performance and retroactive noise control can be extremely costly. However, the "do everything!" approach has an equally dramatic downside. Noise control measures can be intrusive; they can limit access to essential machinery, impact negatively on other aspects of health and safety and, in many cases, impose limitations on the performance of facilities and equipment. Between these two extremes lies successful noise management which minimizes the health and safety impact of noise, while maintaining the accessibility, operability, and performance of machinery and components. The best noise management does this in the most cost-efficient manner, focusing treatment only where it is needed. This requires an intimate understanding of not only where the noise comes from and how it spreads and fills workspaces, but also knowledge of the practices of personnel and how these affect their exposure to noise.

This document presents the different aspects of importance when conducting noise prediction in offshore assets and the consequences of executing noise studies at different phases of projects.

1. Introduction

Noise management during the design of offshore installations is often disregarded. Although employers are serious when it comes to taking responsibility for workers' welfare and environment, associated noise mitigation actions are often late and bring a considerable monetary

impact. In some cases, permits and licenses can be delayed or revoked on the basis of poor noise performance with disastrous consequences to projects.

Introducing noise and vibration matters during design represents a significant value. Good noise and vibration performance is largely a question of good management, coupled with the necessary technical expertise. This is critical to the business performance, safety, and environmental excellence of assets.

2. Understand the Targets

Facilities are subject to an array of legislative requirements from national and international authorities, classification bodies, and in some cases owners and operators. These requirements are designed to negotiate the tension between the needs of workers and the environment on the one hand and a reasonable and manageable level of mitigation on the other. Achieving targets in a cost-effective and minimally intrusive fashion is a substantial technical challenge, but before this challenge can be addressed, all the relevant legislation must be interpreted accurately and reconciled with the aims and ambitions of all the stakeholders in a facility.

An incorrect or inaccurate interpretation of legislative requirements may result in a cumbersome and unnecessarily exhaustive – and expensive – management program. By the same token, however, failure to understand the aims of legislation and limits can undermine the effectiveness of a noise management program and ultimately require retroactive treatment.

Understanding the targets is a crucial first step to optimal noise management, but once the targets are clearly interpreted and defined, they must then be achieved.

3. Start early, the earlier the better

It is much cheaper and easier to install noise control measures during construction than to retrofit them once an installation is operational. This is particularly true of measures that require shutdown and extensive fitting to install, but it is also the case with even simple strap-on or bolt-on treatments. Clearly, these problems are exacerbated if, as in the case with production platforms, FPSOs, and mobile drilling rigs, the installation operates offshore. Incorporating noise control measures directly in the design ensures that there is space and that the measure may be implemented without in any way compromising access and operability.

Incorporating noise management right from the start of the design offer the following benefits amongst others:

- Substantial difficulties can be avoided by relatively simple and minor modifications to the arrangement of equipment, accommodation, and so forth. Clearly, critical noise sources ought to be placed away from noise-sensitive areas, but careful consideration of noise transmission paths must be included to identify optimal arrangements.
- Evaluating machinery technologies during the design considering the noise factors would also represent a substantial distinction in the final product. Electric rather than diesel-driven technology, centrifugal rather than axial ventilation fans, water cooling systems rather than air-based would, amongst others, make a positive effect.
- It would also allow defining specific equipment noise and vibration requirements that can be checked during factory acceptance tests. This practice has triggered considerable actions by machinery vendors that use more and more resources to improve the vibroacoustic characteristics of their

products.

4. Reliable Prediction is the Key

Clearly, the key to successful noise management is reliable, accurate predictions. Understanding targets is a critical first step, but the negotiation between all the different methods available to the noise control engineer can only be as successful as the engineer's ability to predict the outcome of various combinations of measures. Even before any measures are considered, predictions are important to understand the magnitude of improvement required.

There are a vast number of noise sources on a typical offshore installation. Process machinery and equipment, turbines, motors, control and relief valves, and heating, ventilation and air-conditioning (HVAC) systems are some of the more obvious, but in quiet areas such as accommodation, even the sound of your neighbor snoring can be a nuisance. Understanding the behavior of noise sources will pave the way for different possibilities for noise control measures.

Once the noise has been generated it will spread. Noise travels through the air and particularly well through the steel substructure, whether excited by direct contact or through the air or – as in the majority of cases – both. Noise travels far and largely unabated through process pipes and HVAC ducts, both in the steel and in the liquid or gas flowing in them. It goes through walls and if it cannot get through a wall, it is uncannily good at finding ways around.

Sound is, fortunately, also absorbed on occasions and out in the open, all other things being equal, it diminishes in intensity the farther from the source you are. On an offshore installation, however, the situation is more complicated. There is little that absorbs, but much that reflects. Multiple reflections can "funnel" noise so that it diminishes much less than out in the open. A phenomenon called reverberance means that even relatively modest sources might generate fairly high noise levels at specific locations due to reflections.

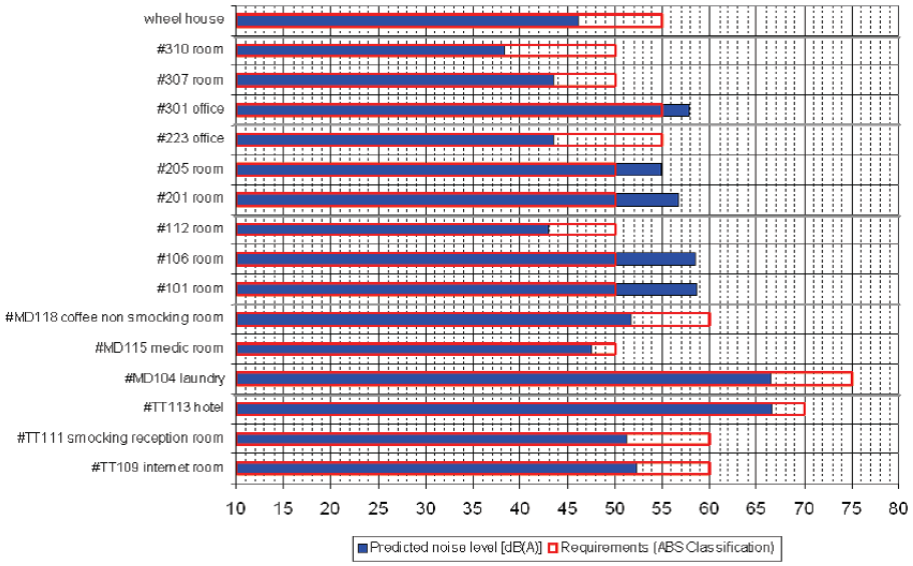


Figure 1 structure-borne noise prediction at different areas of a drilling rig (in blue) in comparison with the requirements (in red). Noise levels are given in dB(A), reference 20 µPa.

4.1 Prediction of Structure-borne Noise

Predicting noise accurately at particular locations, say for instance a cabin within the accommodation block of a production platform, involves differentiating airborne and structure-borne noise contributions. The latter refers to vibroacoustic energy propagated through the structure and radiated by construction elements, such as bulkheads, lining panels, etc., as sound into the noise-sensitive area.

Predicting structure-borne noise accurately on offshore assets requires knowledge about: a) the mean vibration that different machines can generate on steel structures – the transfer function between the force and generated vibration velocity – b) vibroacoustic behavior in the structure – material loss factor and the way how the energy gets damped or amplified in the specific arrangement – and c) the efficiency of construction elements to radiate sound in noise-sensitive areas. Figure 1 shows structure-borne noise contributions to overall noise levels in different spaces of a jack-up drilling rig according to a specific arrangement and in comparison with requirements.

Vibration equipment data is typically not delivered by machinery vendors as it depends on the foundation stiffness. Therefore, the accuracy of structure-borne noise predictions is typically built out of a combination of theoretical and practical experience. Computational models could for example be adjusted by comparing with data measured in the field. This drives towards tuned models for different steel constructions which allow the evaluation of control remedies and the consequences of applying them on different spaces of the installations.

Control remedies at the source would have a positive effect on the entire asset. Mitigating the input mobility of different equipment requires both sufficiently stiff foundations and often the use of carefully selected anti-vibration mounts for particular applications. Figure 2 at the top presents a finite element model of an engine foundation that allows evaluating the dynamic stiffness of the entire construction.

Control remedies at the transmission path are typically applied to the noise-sensitive area. This refers to, for example, applying floor coverings capable of increasing the damping of vibroacoustic energy and featured with low radiation efficiency. Figure 2 at the bottom presents floor coverings capable of providing structure-borne noise attenuation.

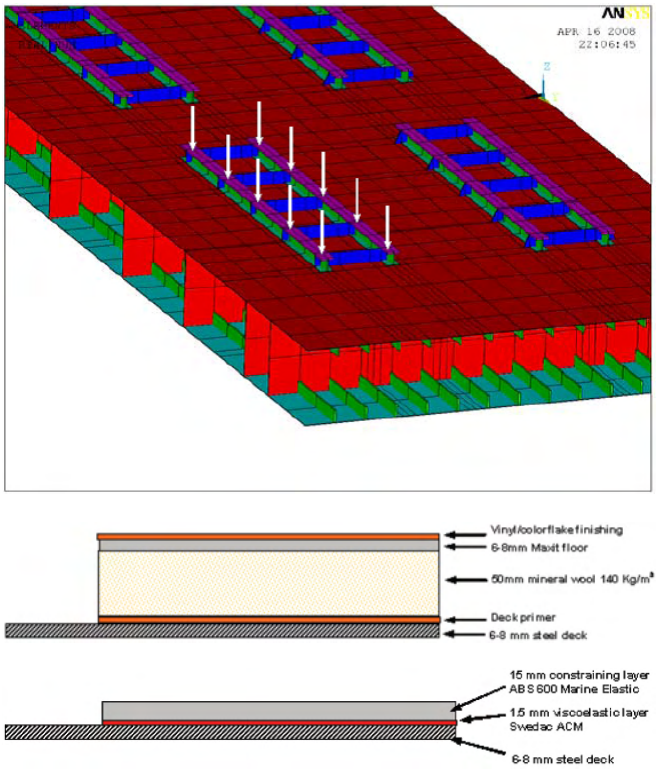


Figure 2 (Top) Finite element model for the evaluation of stiffness of engine foundation, (Bottom) floor coverings typically used for mitigation of structure-borne noise.

4.2 Noise in Machinery Spaces

The prediction of airborne noise propagation has more developed methods and procedures. As a consequence, commercial software can predict with relatively high accuracy the noise levels on e.g. the main deck of production platforms (see Figure 3 at the top). In addition, the fact that equipment vendors are more and more used to deliver sound power data of their products represents in general advantage on the modeling of noise propagation.

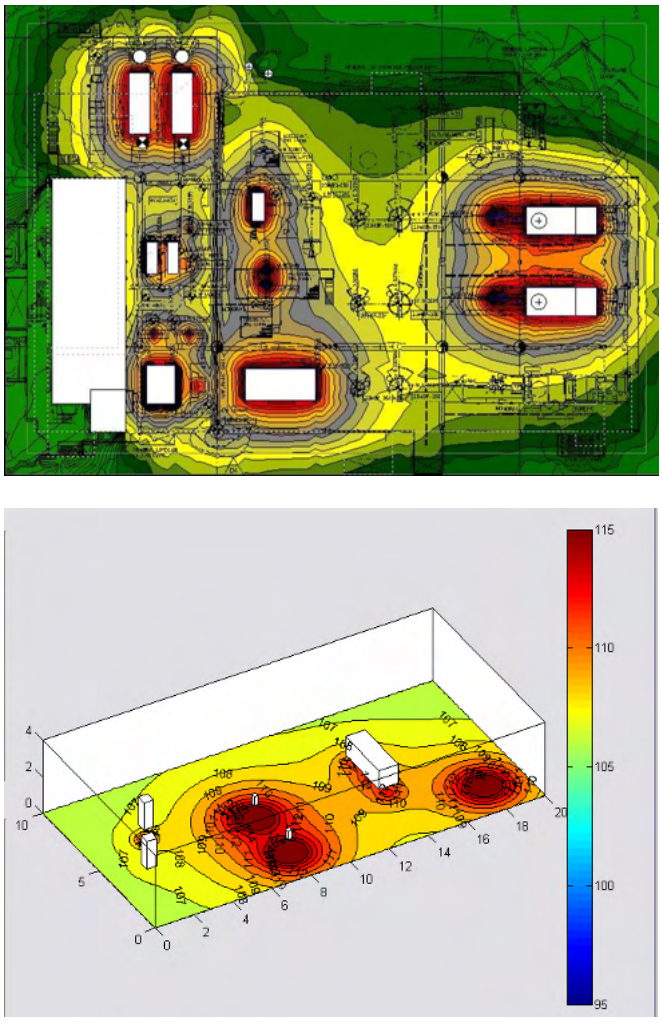


Figure 3 (Top) Outdoor noise contour map over an offshore facility. (Bottom) Indoor noise contour map in machinery space. The noise levels are given in dB(A), reference 20 μPa.

However, the expertise lays in how to introduce the different sources one can encounter on a production platform into a model. Compressors, turbines, pumps, valves, etc., radiate sound in different manners and the directional pattern is required in order to model them properly. In addition, the noise radiation of pipework connected to pressure control devices is typically forgotten and again should be properly introduced in the models.

At indoor machinery spaces, the sound field is composed of the direct sound radiated by machinery and the reverberant field which is determined by the characteristics of the boundaries (see Figure 3 at the bottom). Treating properly the boundaries with absorption material could represent some noise reduction. The effect will, however, be limited in close vicinity to the noise radiating machinery, in particular, if the sound-absorbing material is located relatively far away.

Insulation plans for machinery spaces should then consider not only fire and thermal insulation but also acoustic absorption, quite often aligned with the requirements.

Noise propagation models can be used to identify the areas where control remedies are required, evaluate the noise exposure of personnel working in the area, identify the areas where to introduce entry restrictions without the use of hearing protection, amongst others.

Control remedies include acoustic enclosures, curtains, acoustic lagging, etc. An acoustic enclosure is usually made of steel panels entirely covering the units for soundproofing (see Figure 4 at the top) For large units, doors and windows are implemented to allow maintenance and easy access. Typically, sound reduction of 10-20 dB may be achieved through the use of such

enclosure. Some units such as motors and pumps require an air passage for cooling purpose. It is then necessary to mount a vented enclosure and the sound reduction may consequently be reduced. In case both high noise attenuation and cooling are needed, a separate ventilation system for the enclosure equipped with appropriate silencers in the ducts could be implemented. For electrical motors, water cooling could be considered as an alternative.

An acoustic curtain is generally, a thick sound blocking curtain made in heavy PVC (see Figure 4 at the bottom). Velcro can assure a tight-fitting between the separate curtains which have to overlap and extend all the way to the floor to ensure that sound is not leaking between the separate curtains. If the curtains do not extend all the way to the ceiling, sound-absorbing baffles could be suspended in order that sound does not escape above the curtains from within the enclosed area. Acoustic curtains can provide approximately a 10 dB reduction.

Acoustic pipework lagging typically consists of a dense outer impervious wrap isolated from the pipework by a layer of mineral wool or glass fiber. This type of acoustic treatment is particularly relevant for mitigating valve noise and internal flow noise.

In indoor machinery spaces, the most commonly used sound-absorbing material is mineral wool (e.g. rock wool and glass wool). The mineral wool can be protected by a covering material. It is, however, very important that the cover does not ruin the sound-absorbing properties and if a perforated steel plate is used, it must have a degree of perforation higher than 30 %. If a painted cover is required, it must be done by the manufacturer, as commonly used painting ruins the absorption properties.

Figure 4 Examples of (Top) acoustic enclosure and (Bottom) acoustic heavy-duty curtains.

4.3 HVAC Noise

Ventilation fans are considered potential noise sources. Such devices produce noise that is related to the amount of work they do in order to move a given volume of air against the system resistance. Additionally, flow noise contributions may be generated during the transmission to the served room, typically at fire dampers, control dampers, and ventilation diffusers. Moreover, the noise attenuation is often included using absorption silencers and/or cabin units which consist basically of a plenum box and an air diffuser.

Noise issues during the design of HVAC systems are frequently disregarded. Techniques to predict HVAC noise are relatively well-established and the noise generation and attenuation data are nowadays quite reliable. Nevertheless, HVAC noise issues are often seen after the assets are already built and modifications are often not possible due to space restrictions.

Silencers are typically seen either upstream or downstream fans; rarely in both directions as it should be. For instance, a fan serving to extract air from an engine room should have a silencer upstream the fan in order not to affect the engine room considerably. In addition, a silencer downstream should be installed in order not to affect areas at the outlet, typically through a louver and often pointing towards noise-sensitive areas such as corridors and laydown areas. Acoustic louvers offer an alternative control remedy.

Absorption silencers and acoustic louvers work by the principle that when the sound gets in contact with the sound absorbing material – typically mineral wool – a fraction of the sound is absorbed in the material. The efficiency of these devices primarily depends on the dimensions, the type and thickness of sound-absorbing material, and the air gap between the baffles.

Introducing these HVAC control remedies in due time and based on reliable noise predictions will avoid expensive retrofitting.

4.4 Internal Sound Insulation

Accommodation blocks in offshore installations are noise-sensitive areas that have to be isolated as much as possible in order to provide comfort and quality time for employees on/off duty. In addition to all noise contributions, i.e. structure-borne, airborne, HVAC noise and other, noise generated inside must also be controlled. Noise transmission between cabins is often an issue as noise generated in adjacent rooms, such as TV, people talking, snoring, etc., can disturb sleeping and pleasantness.

Requirements to comply with offshore regulations indicate up to 45 dB weighted sound reduction index (R'w) between cabins, which requires careful selection and installation of partitions. Partition panels are tested in laboratories in order to indicate their acoustic insulation properties in material datasheets. However, the specified acoustic insulation is typically not met in-situ due the noise flanking transmission through e.g. the suspended ceiling system.

Understanding the acoustic performance of such materials provides an indispensable tool for the optimization of noise control measures and the selection of the appropriate building elements and installation methods. In addition, experience on laboratory and field measurements and the use of computational software can create a robust platform for the evaluation of sound insulation.

5. A Holistic Approach

The most effective noise control management is achieved through a dialogue between on the one hand contractors, responsible for layout and construction including noise control measures, and on the other hand vendors, who deliver the equipment that generates the noise and who have certain responsibilities with respect to limiting it.

The challenge for the noise control engineer is to find the optimal combination of noise control measures that can be incorporated in construction and layout and those that can be implemented by machinery vendors in response

to the noise requirements imposed on them. Unreasonable demands made on vendors can lead to over-engineered noise control of machinery, limiting access to critical equipment, increasing maintenance costs, and potentially harming performance. But if specified requirements are too lenient then too much is left for other noise control measures and similar problems may arise.

Clearly defined, achievable demands on vendors are an essential part of successful noise management. Evidently, this dialogue is meaningless once equipment has been ordered, but this is not the only reason it is wise to start early.

Various analytical, numerical, and experimental techniques have been developed, and in some cases computer coded, to assist the noise control engineer in estimating the noise intensities, acoustic performance of structures and materials, and effectiveness of noise treatments. The matter is not only to know how to use them but also to choose the right tool for specific applications. In addition, empirical methodologies could play an important role if properly applied.

Methodologies to evaluate sources, transmission paths, and receivers, combined with the experience on the type of installation will provide the most reliable predictions for successful noise management, the earlier the better.

References

[1] "Working Environment", NORSOK Standard S-002:2018

[2] "Machinery – Working Environment Analyses and Documentation", NORSOK Standard S-005 Rev.1, March 1999.

[3] "Good Noise Management Demands a Holistic Approach Early in the Design Process", Graeme Keith and Daniel Alvarez, Lloyd's Register ODS. Scandinavian Oil & Gas Magazine Vol.36 No. 5/6 2008.

[4] "Measurement of sound insulation of buildings and of building elements – Part 4: Field measurements of airborne sound insulation between rooms", ISO 140-4: 1998

Authors Biography

Mr. Alvarez is Team Leader and Principal Consultant in Noise & Vibration at Vysus Group, formerly Lloyd's Register Energy. Mr. Alvarez holds an M.Sc. in Engineering Acoustics from the Technical University of Denmark and 15 years of experience as a consultant in noise and vibration matters for maritime and oil & gas sectors. With Lloyd's Register from 2006, Mr. Alvarez has successfully managed numerous projects related to predictions, investigations, and measurements regarding machinery noise & vibration, occupational noise, and environmental noise.

The nature of Lloyd's Register led Mr. Alvarez to grow knowledge and expertise in other fields of engineering dynamics, particularly structural, rotor, and fluid dynamics.

About the Financial Implications of a Prescriptive Maintenance System

Mario Pierotti

AMS GROUP (Advanced Management Solutions)

Abstract

Since the late 80's many studies have been conducted to technically demonstrate the efficiency of a real predictive maintenance technique. When applied to the marine sector, naval architects and marine engineers are well aware of the value-added, and of the economic implications that additional data knowledge of marine assets brings. However, less literature has covered the subject from a financial perspective.

This paper draws a financial framework of the economic benefits of a prescriptive maintenance system, underlying core implications as risk assessment, cost reduction, and margin increase. This study concentrates on three main topics:

- Market trend analysis and review of the different avant-garde maintenance solutions offered.
- Asset Integrity Management: the control tower of the entire process
- Breakdown of the technology economic benefits, using financial metrics.

The narrative tone will be primarily financial, in the perspective of offering trustable support to corporate financial decision-makers in justifying such investments, analyzing the impact over metrics as CAPEX, ROI, IRR, PAYBACK, DOWNTIME, USEFUL LIFE.

Finally, the article provides a relevant conclusion concerning cost reduction.

A detailed bibliography is given at the end of the study, from trustable references as government agencies and big market players - PWC, McKinsey, Deloitte, IBM, GE.

1. Introduction

An advanced technology economically oriented to justify investments in marine assets must attain four main goals: to reduce the cost of operations, increase productivity, increase revenues and operating margin, and have a tangible ROI.

This paper will show how a prescriptive approach to maintenance strategy and its impact on the entire marine asset integrity management, could disrupt the marine industry while generating gains.

In a world where technology and automation are reshaping Industry in any area, a corporate

strategy must be prompt and able to achieve true competitive values.

"Internet of Things" cuts barriers between hardware and software linking all the economic assets in an ecosystem environment.

Maintenance innovation becomes a top priority for industry leaders, where the key concept is not only to predict machinery failures but mainly to support an asset integrity management information system built with the ultimate goal of boosting efficiency, reliability, and productivity.

To this purpose, Big Data analysis and diagnostic are crucial since the real gain lies in how this data is used for decision making.

Nowadays, it is commonly true that the need for smarter and integrate asset management is even more strong; and it regards every industry, from Aerospace to Manufacturing, Marine to Automotive, Transport to Construction.

In Marine Asset Management, "technical" aspects as equipment innovation, digitalization, machinery, and propulsion reliability are considered as the most involved in value creation, but recent findings have shown that major winners are Balance Sheet and Income Statement – thus financial aspects.

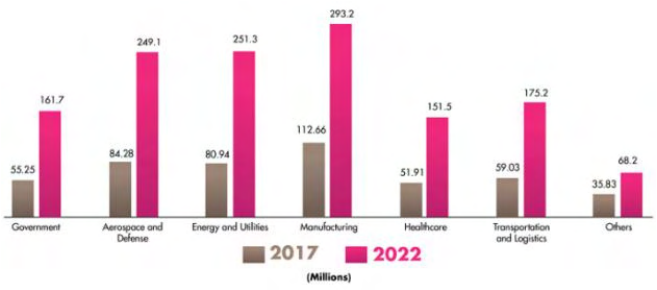


Figure 1 North America predictive maintenance market shares for 2017 till 2022 per industry.

In this article, the latest and most advanced maintenance management criteria are explored, highlighting why the audience should observe them from a financial perspective.

If the hardware is Engineering and the software is Data-analytic then the output is Financials.

2. Marine Asset Integrity Management System

During the life cycle of a fleet or a single ship, from the beginning to the end of its operational life, a dedicated Asset Integrity Management System acts as an umbrella, correlating every aspect of the fleet management under the same hat. Three main aspects could be summarized:

- Enhanced Maintenance Systems
- Operation
- Health – Safety & Environmental protection

The journey of data, and parallels the one of value creation, begins with the collection of condition-based data from Enhanced Maintenance to Operation, comprising Supply chain, Logistic and Inventory, and reaching Health – Safety & Environment.

The actual IoT environment takes the subject to a higher level where maintenance strategy is just a part of the ecosystem, the tip of the iceberg of Marine Asset Integrity Management.

The recent asset management challenge consists

of being able to identify the power of an advanced asset management structure. As well as to recognize the inevitable implications of a massive innovation change in maintenance management.

Speaking of maintenance strategy, traditionally, innovation means a technical improvement that focuses on improving the operation of the asset as machinery or a set of machinery.

The transformation from a preventive to a predictive and, finally, to a prescriptive approach involves the whole lifecycle of a fleet or a single ship, from Maintenance to Operations and Safety.

The revolution starts with maintenance management and expands to every field related to fleet management. An advanced predictive and prescriptive maintenance system plays indeed a crucial role in producing a large amount of data essential for decision making.

3. Smart Maintenance

In the field of Asset Integrity Management, the evolution of maintenance techniques ran parallel with the Internet and technology revolution, despite an important application delay.

From a primitive "run to failure" philosophy – "an outdated and inefficient way to conduct maintenance, when technology enables far more sophisticated and cost-effective methods and products themselves have become far more reliable due to superior Engineering [1]- studies evolved to a preventive/time-based mentality, but industry sectors were – and still partially, are – reluctant to maintenance innovation, regardless of the clear and proved benefits.

Hardware and software have reshaped the maintenance world, moving the focus from finding the right time to intervene – preventive – to data collection and predictive analysis – predictive. But still, "less than 1 % of the data generated are currently used for decision-making [2] McKinsey findings.

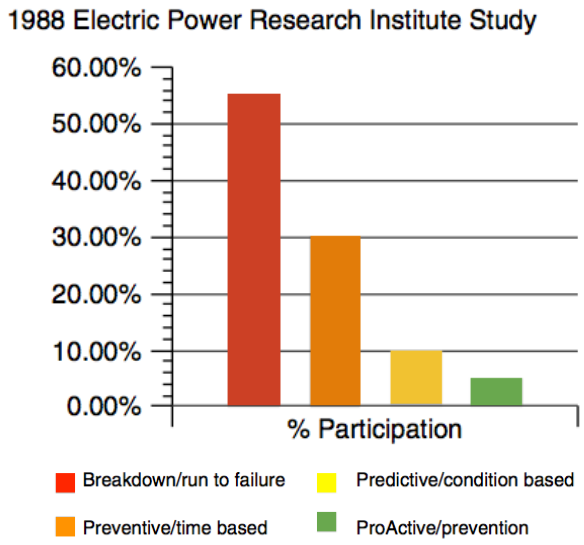


Figure 2 1988 Electric Power Research Institute Study

The latest connectivity revolution delivered by IoT, opened a breach into prevision and data analysis, correlating all plant's assets into an ecosystem, aiming to diagnose and generate information on actions to be taken - prescriptive.

Regarding predictive and prescriptive maintenance when applied in the marine sector, an advanced maintenance technology with a predictive and a prescriptive approach could pioneer the market. A one-of-a-kind system developed matching deep expertise in the marine industry with wide knowledge in engineering and technology.

Data handling and correlation are crucial steps in determining the uniqueness of maintenance technology. Data are the revolution bricks, a storm of bricks.

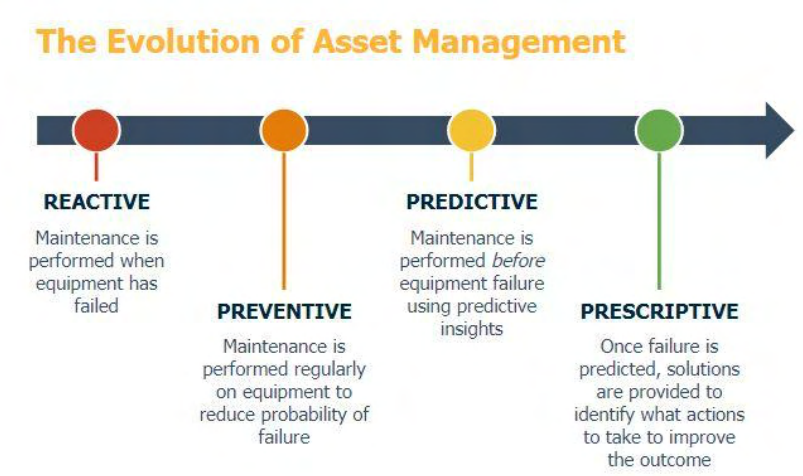


Figure 3 Maintenance Techniques Timeline

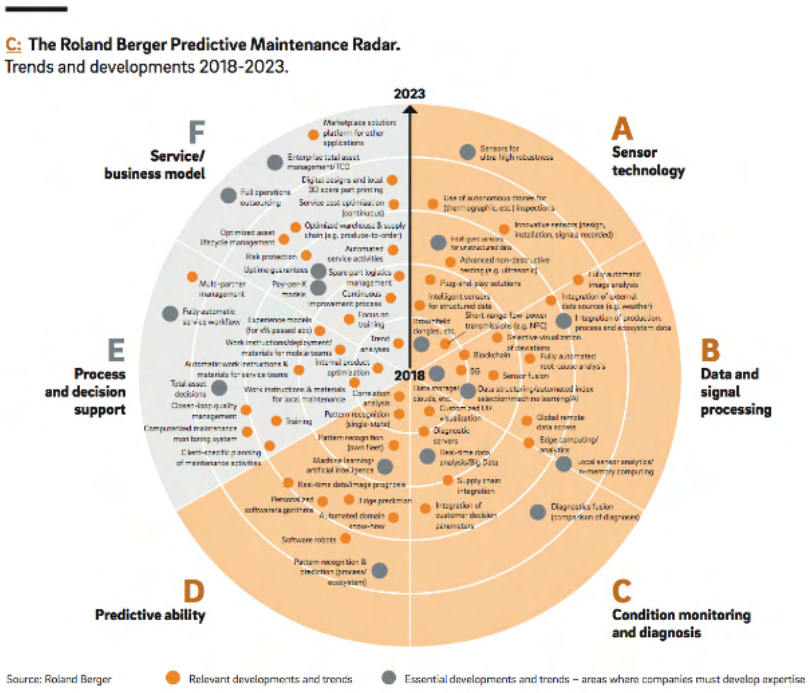


Figure 4 Predictive Maintenance Data Innovation Forecast

The maintenance system could represent a powerful tool that orchestrates the big mass of data in a way that makes them useful to fundamental decision making; Therefore, it applies algorithms to predict the best point in time to carry out maintenance before the actual occurrence happens or parameters drastically change.

Specifically, it gives you actionable instructions about how to solve predicted failures before their occurrence. Moreover, the system could survey a complex mechanical ecosystem and evaluate the intercorrelations between its machinery and equipment.

This paper aims at shifting the focus of the automated maintenance industry from a closed

and technicians' mindset to a wide managerial view. Giving that the implications economically affect different asset aspects, bringing benefits and cost reductions. Finance, more than giving an investment justification (in terms of ROI and payback time), has the capabilities to understand the overall business implications in terms of important metrics, such as CAPEX, downtime, performance, etc.

In Figure 5, 6, and 7, examples of the multidisciplinary nature of advanced predictive maintenance are illustrated. Firstly, a 2018 Industry survey shows a wide range of advanced maintenance applications.

Then findings, respectively from PWC and McKinsey articles, show some of the major drivers of maintenance innovation, ranging from safety to machinery lifetime.

The following chapter contains the core metrics regarding the proven financial benefits that a predictive and prescriptive approach brings. The scope is to provide valuable tools to financial managers, to understand the positive financial implications and the economic reasons for investment.

Maintenance value driver	*Average improvement*
Uptime improvement	9%
Cost reduction	12%
Reduction of safety, health, environment & quality risks	14%
Lifetime extension of aging asset	20%

Figure 6 Maintenance Value drivers from PWC

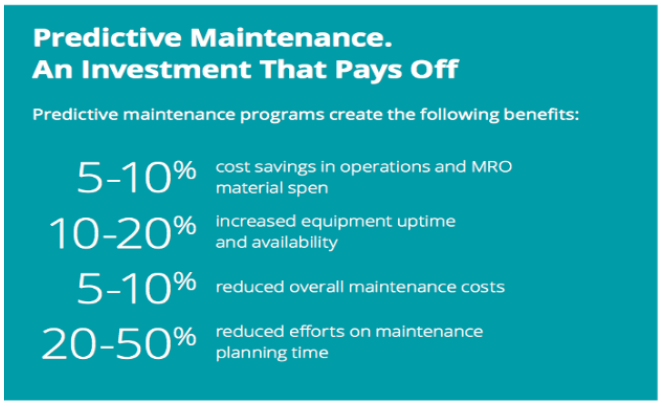


Figure 7 Maintenance Value drivers from McKinsey

4. Financial Implications

In the marine sector, if your business still follows a reactive or planned maintenance strategy, you

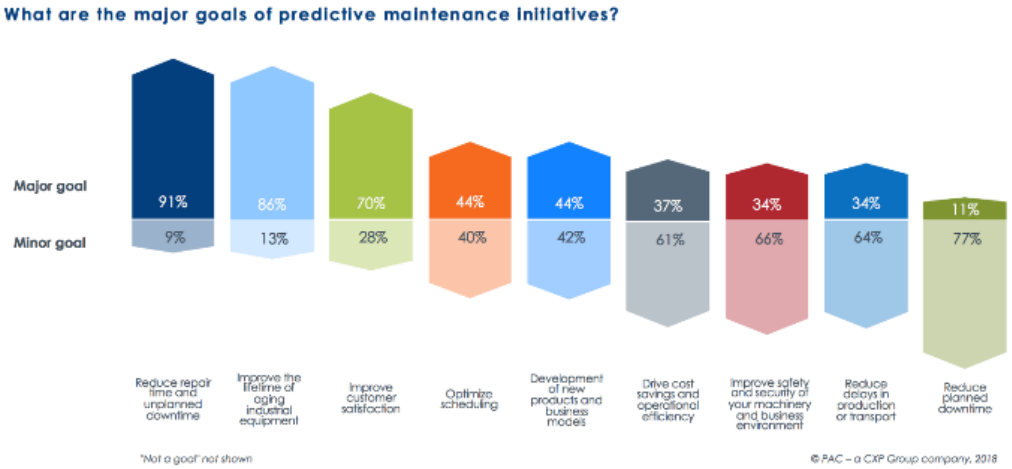


Figure 5 Which of the following are major, minor, or not a challenge for your company when it comes to existing maintenance and servicing processes for your assets?

are probably losing money every day.

In the paragraph, the entity of the losing impact will be shown as well as a strategy to stop losing and start gaining.

Several academic studies illustrate the benefits of predictive maintenance technologies, but unfortunately, they merely concern the technical side.

This research aggregates the multitude of qualitative and quantitative figures regarding financial benefits deriving from predictive asset management.

At first, an important consideration must be made concerning four fundamental concepts: **Cost of different maintenance strategies, Downtime, Capex, and ROI.**

Concerning the maintenance aspect, the US Department of Energy study "Operations & Maintenance Best Practices – A Guide to Achieving Operational Efficiency [3], set a cost of maintenance hierarchy considering the cost of maintenance in dollars per horsepower per year.

- Reactive - 18 $/hp/year
- Planned /preventive - 13 $/hp/year
- Advanced predictive/prescriptive - 6 $/hp/year

The impact is already huge, giving a yearly more than 50% cost reduction from a planned maintenance model.

More than that an important concept is hidden: the cost of a wider predictive and prescriptive maintenance not merely depends on the operative steps needed to conduct maintenance, but have an impact where there are direct or indirect effects on all activities within the marine asset integrity management process (spare parts management, integrated logistics, port activities, insurance, safety, and environment, etc.)

Besides, downtime is a factor that can highly benefit from an advanced approach.

Downtime means the time in which machinery (or a set of machinery being part of an ecosystem) is unavailable and can occur in two ways, either scheduled or unscheduled.

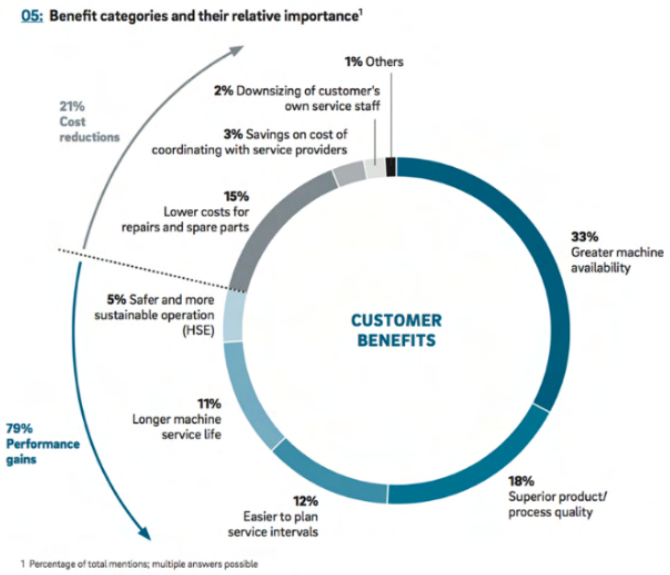


Figure 8 Benefit categories and their relevance

Deloitte, for example, focuses the attention on spare parts management highlighting the importance of downtime risk and its wide business implication.

"Spare-parts management presents a similar challenge that can feel like a constant balancing act. With limited budgets, maintenance professionals must evaluate which parts they will need and when to procure them. If the spare is not on hand or order when it is needed, the downtime of an asset can be anywhere from days to weeks—or even months—while waiting for the replacement part. This typically leads to the buildup of spares inventory, which not only ties up working capital but also increases the risk of excess and obsolescence that erodes the bottom line. [4]

Studies from IBM, Capgemini, PWC, and Arc Advisory Group, arrive at the same conclusion: using predictive maintenance over planned maintenance reduces at least 50% of random technical failure, 25% in yearly parts expense, at least 25% of the overall maintenance-related costs, up to 12% of the scheduled repairs and 10% to 15% in logistic costs. A prescriptive approach leads to even more impressive figures.

Capital Expenditures (CAPEX) has also a meaningful impact. Studies show how proper management of marine assets, in terms of advanced maintenance strategies and usage, can tangibly increase useful life. This impacts depreciation and amortization and ultimately the spending plans included in capital expenses. The lifecycle of machinery is reported to be reduced from 7% to 20% (in a switch from planned to predictive and even more to prescriptive).

Then, lifetime ROI is beneficially influenced by the maintenance approach adopted as presented in Figure 9.

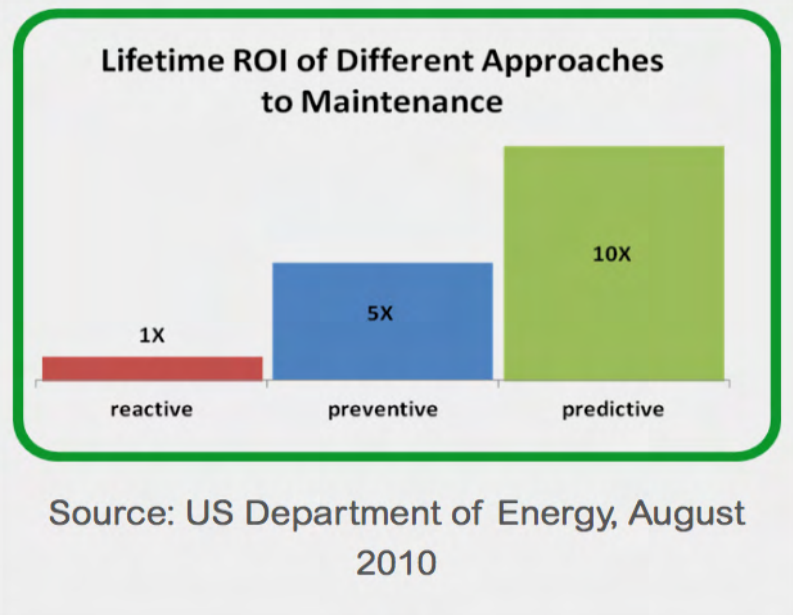


Figure 9 Lifetime ROI of different approaches to maintenance - US Department of Energy, 2010

The following table summarizes all the benefits found by trustable research and studies.

CATEGORY	INDUSTRY SEGMENT	VALUE / %	REFERENCE (YEAR)
Adv. Predictive vs Planned	General	-54%	US Dept of Energy (2010)
Downtime	General	-35%	US Dept of Energy (2010)
Downtime	Marine	-20%	General Electric (2016)
Downtime	Mining	-20%	General Electric (2018)
Downtime	Robotic	-50%	Harvard Business Review (2016)
Downtime	Oil & Gas	-36%	General Electric (2016)
Defect Rate	Cylinder Heads	-50%	IBM (2014)
Breakdowns	General	-73%	US Dept of Energy (2010)
Maintenance Repairs Operations Materials	General	-8%	Deloitte (2017)
Inventory Cost	Oil & Gas	-7,5%	GE (2016)
Safety Risk	General	-14%	PWC(2018)
Machinery Uptime	General	+25%	PWC(2018)
Lifetime Aging Asset	General	+20%	PWC(2018)
Production	General	+22,5%	US Dept of Energy (2010)
Production	Robotic	+25%	Harvard Business Review (2016)
Machinery Efficiency	General	+15%	Deloitte (2019)
CAPEX	General	-4%	McKinsey (2015)
ROI	General	x10	US Dept of Energy (2010)

5. CONCLUSION

An investment can be observed from both a technical and financial perspective. The former focuses on process optimization, while the latter evaluates economic factors such as cash flows (IN/OUT), risks, and time.

Several academic papers have been written to illustrate the benefits of predictive maintenance technology, especially concerning the technical side.

This research aggregates the multitude of quantitative and qualitative figures, regarding the benefits from a financial perspective.
In the research conducted, several systems that provide predictive solutions were found. What was harder to find out was a system able to provide advanced and quality solutions having a wider impact on the entire marine ecosystem, and a data journey able to deliver qualitative information useful for management decision making.

Most of the companies/startups on the market solely concentrate on data collection (in quantitative terms), with a vision limited to the machinery that needs maintenance.

However, exceptions could be found, there is an innovative system that applies an advanced predictive and prescriptive approach to maintenance. It has the Asset Integrity mindset as a fundamental business structure providing a solution that not only collects and analyzes structured data but moves forward, with automated diagnosis and specific prescription with direct consequences on the entire flow of activities of the marine asset integrity management process.

References

[1] IBM, "The Evolution of Maintenance Towards Prescriptive", 2017

[2] McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype", 2015.

[3] US Department of Energy, "Operations & Maintenance Best Practices – A Guide to Achieving Operational Efficiency", 2010

[4] Deloitte, "Predictive maintenance and the smart factory", 2017

Figure 1 – Bellias, M., 2021. The evolution of maintenance towards prescriptive, IBM [online] Business Operations. Available at: <https://www.ibm.com/blogs/internet-of-things/maintenance-evolution-prescriptive/>.

Figure 2 – John Piotrowski, 2007, "1988 Electric Power Research Institute Study", Shaft Alignment Handbook.

MCKINSEY GLOBAL INSTITUTE, 2015, "The Internet of Things: Mapping the Value Beyond the Hype".

ROLAND BERGER, 2018, "Predictive Maintenance – From Data Collection to Value Creation". Available at: https://www.rolandberger.com/de/Publications/Predictive-maintenance-–-from-data-collection-to-value-creation.html.

PWC, 2018, "Predictive Maintenance 4.0 Beyond the hype: PdM 4.0 delivers results". Available at: https://www.pwc.be/en/documents/20180926-pdm40-beyond-the-hype-report.pdf.

US Department of Energy, 2010, "Operations & Maintenance Best Practices – A Guide to Achieving Operational Efficiency". Available at: https://www1.eere.energy.gov/femp/pdfs/OM_5.pdf)

GENERAL ELECTRIC, 2018, "Digital Industrial Revolution with Predictive Maintenance". Available at: https://www.ge.com/uk/sites/www.ge.com.uk/files/PAC-Predictive-Maintenance-GE-Digital-Full-report-2018.pdf .

Figure 7 – "Benefit categories and their relative importance "

RONALD BERGER, 2017, "Predictive Maintenance Servicing tomorrow – and where we are really at today".

DELOITTE, 2017, "Asset Monitoring & Predictive Maintenance". Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-a-turnkey-iot-solution-for-manufacturing.pdf.

MCKINSEY, 2018, "How advanced analytics can benefit infrastructure capital planning". Available at: https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/how-advanced-analytics-can-benefit-infrastructure-capital-planning.

Authors Biography

Mario Pierotti
CEO OF AMS GROUP (Advanced Management Solutions)

Dr. Mario Pierotti is a Naval Architect and Marine Engineer with more than 30 years of experience in the Shipping and Oil & Gas sectors.

In brief his career: Ship designer, Technical and Fleet Manager, International Group Executive Vice President, Managing Director of various Companies. He is also an Engineering Consultant and expert in Asset Integrity Management.

Breaking the Innovation & Adoption Conundrum

Chye Poh Chua
ShipsFocus Group

Abstract

With the ubiquitous internet and its diversely proliferating applications, their usage, and corresponding economic benefits they generate, there is little necessity to explain the need to digitize in the mainly B2B maritime industry. The question is about how, and to do or not to do, for each stakeholder individually and the industry collectively, to transit from the current, and largely analogue and manual maritime and port operations to a digital system.

But, despite a countless number of projects over the years, success stories are still few and far in between. On the other hand, without having enough maritime and port stakeholders digitizing their operations; connecting digitally, and accumulating a good amount of data; there is little practical hope for more advanced applications like A.I. and other innovations; let alone the notion of an industry transformation. We share our experience and perspectives here about the causes for what we term as an 'innovation & adoption conundrum' that hinders digitization and innovation, and how we overcome such a conundrum, using our venture studio as an example.

Introduction

There are several broad reasons why maritime and port stakeholders fail either in delivering an innovation or digitization project or fail in getting a product or solution effectively adopted and achieve meaningful traction after a project completes. One of these is **not fully understanding and thus underestimating the conundrum** and resulting in not getting appropriately prepared prior to commencing a project. Another is the 'Emperor's new clothes' syndrome of **not wanting to acknowledge the conundrum** and preferring to go with the hype.

The conundrum explains broadly the causes and factors that hinder digitization and innovation projects and their adoption. These factors are also true and present for corporate ventures and their innovation teams as we have observed despite the hype.

Barriers to successful digitization or innovation – the Maritime Innovation & Adoption Conundrum

The 'Maritime Innovation & Adoption Conundrum' refers to a huge gulf between Tech on one side, and the Maritime Industry on the other side, preventing innovative or digitization development and their adoption. I generalize the causes into:

1) Skills Issues

On one side: Multi-disciplinary and holistic skills are rare due to the vast nature of the industry; most maritime jobs are specialized. On the other side, Tech tends to lack a deep enough domain understanding of maritime and port's many operational variations, exceptions, and nuances that are needed to effectively solve people's problems on the ground. On top of these, depending on the scope and scale of a project, there is also a special skill required in managing the 'Big Picture and Operational Precision Paradox'. Often, it is manifest in someone who can revel alternating between seeing the macro picture and toiling through the details & related operational rigor.

2) Trust Issues

Many industry people, particularly those at the frontline feel that IT has not delivered from their own past experiences: It has been a case of them serving the system than the other way round, of technology or system serving the people. This is particularly stark now with the many seamless and superb UI/UXs they have become accustomed to on their personal mobile applications. On the other hand, Tech people feel that shipping people are unwilling to spend time and commit their effort in discussing their problems and requirements – so there is a lack of trust between them.

3) Mismatch Issues

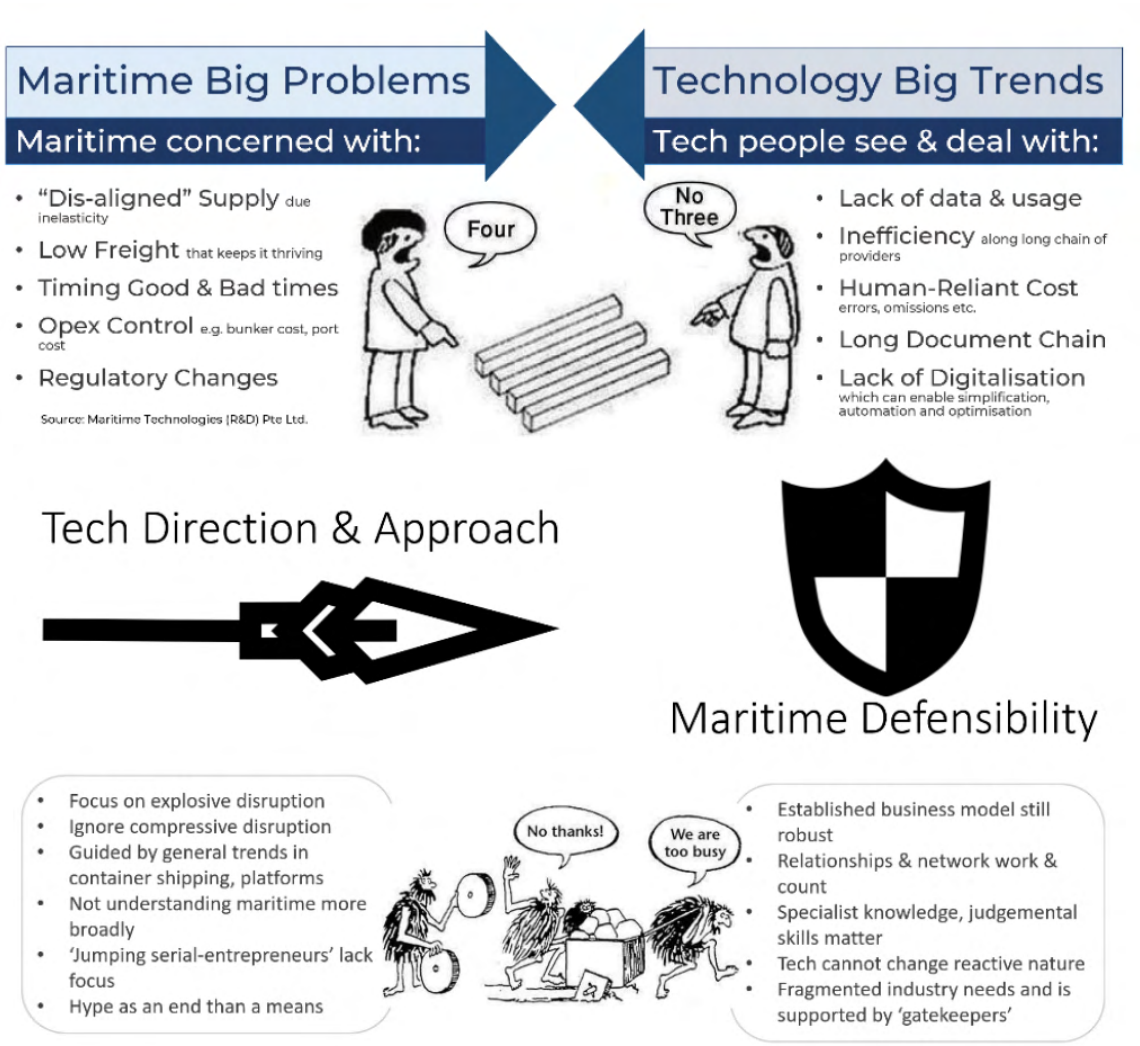
Even in instances where there is a lot of willingness from each side to come and work on a project together, the things that concern maritime people are often not the same things that Tech people look at solving. Both sides tend to have different perspectives, expectations, and priorities – this is even so in the case of a Corporate Innovation structure. They still need an expert third party to bridge the gap. To succeed in any digitization or innovation project, we will need to align such attitudinal differences and mismatches first.

Often the approach is taken also varies. Tech tends to take a directional approach that somehow creates a defensive response from the industry people. When that happens, the key inputs required for change must come from people who become gatekeepers now! Furthermore, many of the Tech understanding and approach is also based on container shipping which operates on different principles from other segments, thus missing out on learning in the other shipping segments including bulk.

4) Complexity Issues

Finally, it is the very **complex nature of maritime commerce itself.**

The nature of maritime commerce includes having numerous nodes, which can be extensively diversified; involving long chain; with distributed flows – whether it is workflow or dataflow; and with many tedious operations; often requiring remote management due to the movement of the mobile asset. Such basic nature creates challenges in Simplification;



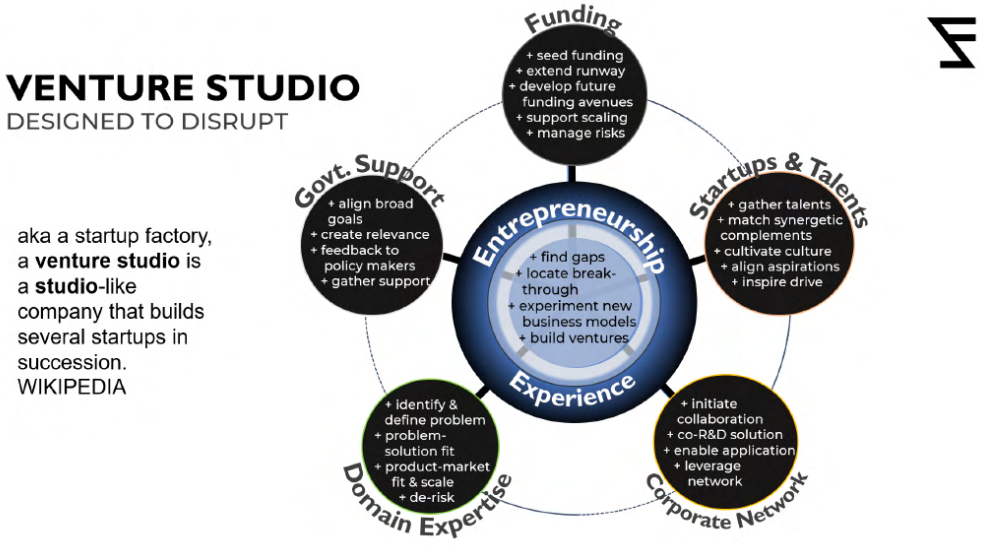
Standardization; Connectivity; Controllability; Efficiency and Predictability.

So, the very complex nature of maritime commerce hinders digitization. Ironically, these natural challenges are exactly what digitization aims to solve!

Solving the Conundrum – ShipsFocus venture studio model as a case study

When we started operations in April 2016, we decided to build a smaller twin ecosystem model, aspiring to research, address and overcome the conundrum. So, we ensured all the critical components of the larger ecosystem out there were present under one roof.

Using this model and the frameworks we developed, we have built over a dozen new tech applications that achieved commercial traction since we started. These include digital operational tools for ship operators chartering & operations, ship-agents, terminals; aggregated marine services, etc. all of which help



stakeholders reduce operations costs.

The adopters all enjoyed early stages and varied levels of three key components of a digital transformation as a result:

1. the overhauls of processes;
2. operations; and
3. relationships with customers.

Generally, there are four types of digital transformation:

1. business process;
2. business model;
3. domain; and
4. cultural or organizational.

Our model and frameworks aim to deliver in all four though we often see companies focused solely on the process or organizational transformation.

More importantly than anything else, as many of our targeted clients were MSMEs which make up the majority in maritime commerce, their digitization and adoption became a great equalizer to narrow the digital divide.

Some things the venture studio did better than the startup ecosystem

As the venture studio is a small replica (a twin model) of a startup ecosystem, over these years we were able to identify some key elements which the venture studio offers that made a critical difference from the larger ecosystem out there:

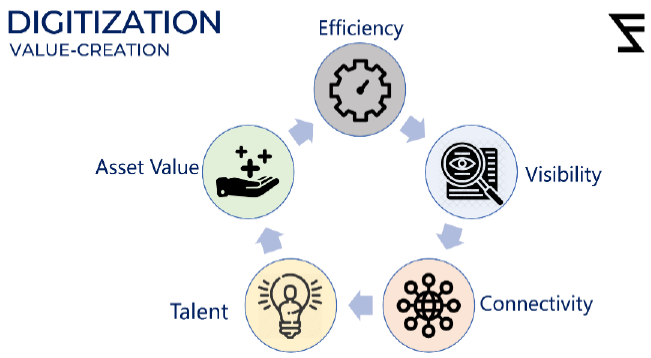
1. Proximity: of problem owner and solution builder coordinated by a project manager under one roof allows for daily scrums and uninterrupted iteration infused with instant user feedback.
2. Problem: Ability to put time and focus specifically on understanding and defining the Problem prior to thinking of its solutioning.
3. Solution: Nimbleness, flexibility, and empathy in creating and combining non-tech offerings as part of the solution and business model.
4. Interest: A genuine interest in the maritime domain means that the founders are determined and have the drive and commitment to stay the course despite facing multiple and continuous challenges as a startup on a prolonged period.

Benefits of Digitization

Whether it was from the onset or from a client's feedback, we noted various benefits that came with digital transformation:

1. Efficiency: It provides core business and operational functions like booking, scheduling to move away from manual processes, and automate key areas like recording, enabling frontline staff to focus more human-centric activities like relationship building; and business intelligence and analysis, enabling leaders to focus on wider business opportunities.
2. Visibility: It brings about unprecedented visibility and improves access to information which is the lifeblood in maritime commerce. Users now can search for collections quickly from anywhere at any time. Several users can access the same information and documents seamlessly at the same time.
3. Connectivity: It gives businesses instant connectivity and communication with customers and allows users to connect from anywhere at any time. Such connectivity is equivalent to building a tech moat around a business and enhances the stickiness of service.
4. Talent: The maritime industry faces a challenge in attracting and training of new talents, a cloud-based digital system doubles up as a knowledge repository which provides them access to the company key information and knowledge resources and creates a virtuous cycle: the more the staff use the system, the more data it will accumulate, and the system becomes more robust.
5. Company value: As the digital system enhances data processing, storage, and transmission, and as data flows and intermingles, they get accumulatively richer. The organizational value is no longer the traditional asset value. The unique database becomes a new intangible asset!

We are starting to see as companies and processes start to digitize, they also start to pay more attention to data. Even without their conscious motive, some of these companies are on a quiet data-centric transformation culturally.



Conclusion

In conclusion, through extensive R&D over the years, we are able to clearly identify; deeply understand, and effectively overcome each of the four broad issues which we termed as the maritime innovation & adoption conundrum. Operating ShipsFocus as a venture studio, enables us to effectively marry 'dream' and 'reality not just sporadically but on a consistent and efficient 5-step process of:

1) Ideation: imagine, create, and socialize the big picture (of the problem)
2) Business model: simplify, articulate, and develop the business model
3) Socialization: relate and socialize the big picture to gain buy-in
4) Architecting: embed physical, social, and tech infrastructure
5) Operationalization: operationalize the big picture through Systems, Processes, and People

As a result, we can do what many continue to grapple with in digitizing maritime commerce, particularly at the operations level where data are generated, captured, and enabled to flow digitally downstream, paving the way for accumulation and many exciting and new applications.

Authors Biography

Chua Chye Poh is the Founder and CEO of ShipsFocus, the world's first maritime venture studio based in Singapore. He is also a venture partner for a maritime fund at Wuest Ventures. Chye Poh holds a Master's degree in Business Administration from the University at Buffalo, State University of New York. His experience in ship operations & ship-broking spans over 30 years, and in the last 5 years in stitching together technology in maritime commerce. Having come from the industry, Chye Poh has not just a unique affinity but also strong empathy for maritime people and their multiple tedious operations, especially helping the many MSMEs digitalize and narrow the digital divide.

Hydrodynamic Study on Jetty by Using Simulating Waves Nearshore (SWAN)

Cathy Zhao

PETROLNG PTE LTD, Petrolngsg@gmail.com

Abstract

Nearshore Hydrodynamic Study is a key step to achieve the wave force on jetty and seawall design. This work focuses on the Hydrodynamic Study for the pontoons and seawalls using Simulating WAves Nearshore (SWAN). It also presents the wave and wind data overview, hydrodynamic study methodologies, and study results with recommendations for the future design of pontoons and seawalls. The CFD model covers a large domain of Singapore water, approximately 150 km in both the horizontal and vertical dimensions. The model extent is determined to enable an accurate description of the wind-wave generation, as well as to guarantee a thorough transformation of waves from the prevailing directions to the location of study. Finally, the design of seawall is recommended and the wave force on pontoons is advised for Civil Engineers.

Keywords: Nearshore Hydrodynamic Study, SWAN, CFD, Pontoon, Wave Force

1. Introduction

1.1 Background

During the past decades, the traditional wave simulation models in coastal engineering to computing waves in nearshore conditions are in the process to be replaced by models by the spectral energy balance on a regular grid. In third-generation versions of this model, the wave spectrum will be described to evolve free of any a priori limitations and all relevant physical processes represented explicitly in a discrete spectral formulation. That is the Simulating WAves Nearshore (SWAN) with the inclusion of ambient currents is illustrated in this work [14]. Conceptually it is an extension of deepwater third-generation wave models but the physical processes and the numerical techniques involved are more complicated for nearshore simulations. The SWAN wave model has been conceived to be a computationally feasible third-generation spectral wave model for waves in shallow water (including the surf zone) with ambient currents in a consulting environment with return times of less than 30 min on a desktop computer.

In general, coastal jetty projects were based on structural design and construction and without a sound assessment of their environmental impact [4]. The need and urgency of such projects were a consequence of the large sedimentary deficits that occurred mainly as a result of activities in the river systems, notably, the increase in dam

construction after World War II [3,4]. This has led to a large reduction of beaches in coastal areas and the destruction of many natural protections such as dunes [4]. With the ongoing climate change, the vulnerability of coastal zones has increased and, according to most forecasts, will tend to worsen further from the middle of the current century [4].

The objective of this work is to document the wind conditions for the Singapore water and to provide input data for the wave generation commissioned to PetroLNG Pte Limited in 2020 as the technical consultant to conduct hydrodynamic studies for jetty, as shown in Figure 1.1.

Figure 1.1 Location and layout of the The jetty

The protection of a boat canal at the nearshore area of Singapore water has been investigated using Computational Fluid Dynamics (CFD) by modeling in SWAN. To protect the entrance of the channel and shoreline with a future jetty, we have performed a hydrodynamics study with a parametric study on the effect of the seawall. Environmental forces affecting the proposed jettied inlet system are quantified using the SWAN, consisting of a spectral wave model and a depth-averaged circulation model with sediment transport calculations. The model simulation indicates the option with a full height of seawall will be helpful for the wave loading on the pontoons.

1.2 Terminology

Abbreviation	Description
CFSR	Climate Forecast System Reanalysis
EVA	Extreme value analysis
FUNWAVE	Full Nonlinear Boussinesq Wave Model
H_s (H_{m0})	Significant Wave Height (m)
T_p	Wave Peak Period (sec)
MOM	Method of Moments
NCEP	National Centers for Environmental Prediction
NOAA	National Oceanic and Atmospheric Administration
OCDI	The Overseas Coastal Area Development Institute of Japan
PIANC	World Association for Waterborne Transport Infrastructure
SWAN	Simulating Waves Nearshore Model
WEI	Weibull distribution function
N	NORTH
NNE	NORTH-NORTHEAST
NE	NORTHEAST
ENE	ENE
E	EAST
ESE	EAST-SOUTHEAST
SE	SOUTHEAST
SSE	SOUTH-SOUTHEAST
S	SOUTH
SSW	SOUTH-SOUTHWEST
SW	SOUTH WEST
W	WEST
WNW	WEST-NORTHWEST
NW	NORTHWEST
NNW	NORTH-NORTHWEST
WSW	WEST-SOUTHWEST
H	Wave height induced by passing ship
h	Water depth (m)
s	Distance from passing ship (m)
V	Speed of passing ship (m/s)
g	Acceleration of gravity (m/s2)
L	Wavelength (m)
T	Wave period (s)
k	Wave number
y	Vertical extent of the barrier below the still-water surface (m)
C_t	Transmission coefficient

2. Wind Conditions

2.1 Data Overview

The wind conditions for the Singapore water were obtained from the NOAA, NCEP, CFSR global wind data set Output from NOAA [1] NCEP CFSR is available at 0.5o grid resolution every hour on a global grid, covering a period of 38 years from January 1979 to December 2016. Figure 2.1 shows the location of the NOAA data-retrieving point. It is situated at (1˚N, 104.3˚E), about 64 km from the objective jetty. This position corresponds approximately to the center of the wave generation and transformation model.

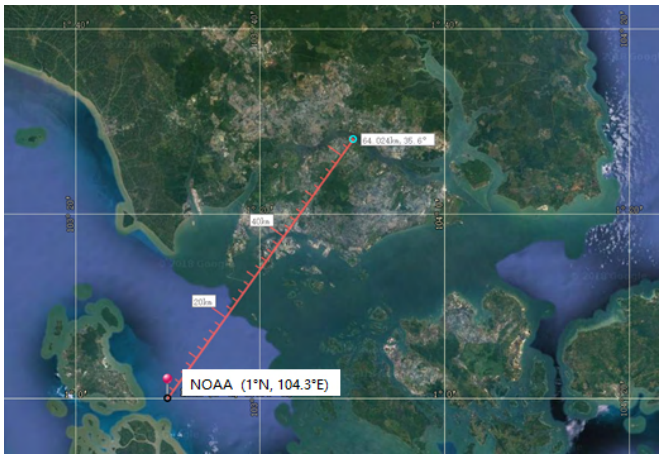


Figure 2.1 Location of the NOAA data-retrieving point (1˚N, 104.3˚E)

2.2 Wind Data

2.2.1 General Wind Condition

Based on the NOAA wind data set, an analysis of the wind conditions was undertaken. The wind rose and the wind speed – wind direction scatter table for the NOAA data-retrieving point (1˚N, 104.3˚E) are respectively shown in Figure 2.2, and Table 2.1.

From the data, it is clear that the wind the climate is dominated by moderate wind speeds from N, NNE, SE, and SSE in the vast majority of the time, and the wind speeds are below 6m/s in general.

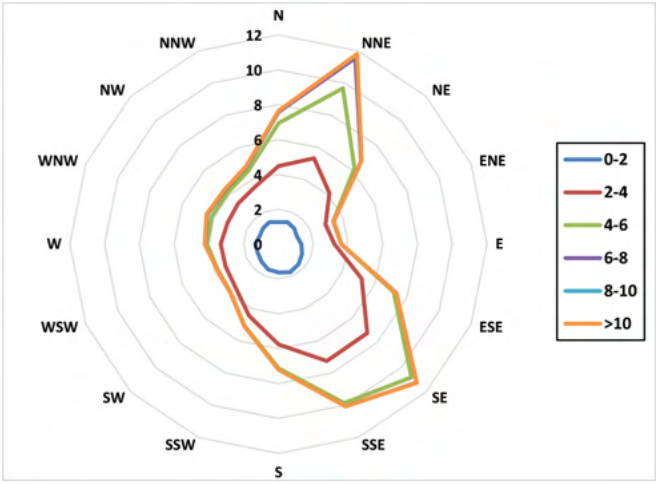


Figure 2.2 Offshore wind. The wind rose of all data points between 01-01-1979 and 31-12-2016 at the NOAA data-retrieving point (1˚N, 104.3˚E).

2.2.2 Extreme Wind Speed

Extreme value analysis (EVA) is conducted, based on the NOAA hindcast wind data, to derive the extreme wind speeds corresponding to different return periods and different wind directions. Weibull distribution function (WEI) and method of moments (MOM) are selected.

The extreme wind speeds for different return periods and different directions at the NOAA offshore point are summarized in Table 2.2

Table 2.1 Offshore wind. Wind scatter table for frequency of occurrence of all data points between 01-01-1979 and 31-12-2016 at the NOAA data-retrieving point (1°N, 104.3°E).

Directions	Wind Speed (m/s)						
	0-2	2-4	4-6	6-8	8-10	>10	Total
N (348.75-360-11.25)	1.26	3.22	2.43	0.62	0.07	0.01	7.65
NNE (11.25-22.5-33.75)	1.38	3.96	4.35	1.88	0.22	0.01	11.81
NE (33.75-45-56.25)	1.26	2.87	2.03	0.54	0.03	0.00	6.75
ENE (56.25-67.5-78.75)	1.14	1.76	0.47	0.03	0.00	0.00	3.44
E (78.75-90-101.25)	1.31	1.89	0.36	0.01	0.00	0.00	3.61
ESE (101.25-112.5-123.75)	1.46	3.68	1.98	0.16	0.00	0.00	7.33
SE (123.75-135-146.25)	1.62	5.58	3.59	0.42	0.01	0.00	11.24
SSE (146.25-157.5-168.75)	1.74	5.49	2.61	0.20	0.00	0.00	10.07
S (168.75-180-191.25)	1.62	4.12	1.35	0.08	0.00	0.00	7.20
SSW (191.25-202.5-213.75)	1.56	2.85	0.63	0.02	0.00	0.00	5.10
SW (213.75-225-236.25)	1.38	2.08	0.39	0.01	0.00	0.00	3.92
WSW (236.25-247.5-258.75)	1.29	2.00	0.49	0.03	0.00	0.00	3.82
W (258.75-270-281.25)	1.33	1.99	0.79	0.11	0.01	0.01	4.24
WNW (281.25-292.5-303.75)	1.17	2.00	0.98	0.29	0.03	0.00	4.48
NW (303.75-315-326.25)	1.28	2.01	0.87	0.21	0.03	0.01	4.41
NNW (326.25-337.5-348.75)	1.36	2.18	1.00	0.26	0.04	0.01	4.85
Total	22.25	47.79	24.44	4.96	0.46	0.03	100.00

Table 2.2 Offshore wind. Extreme wind speed for different return periods and different directions at the NOAA data-retrieving point (1°N, 104.3°E)

Direction	Extreme wind speed (m/s; 1-hr average)				
	1-year	5-year	10-year	50-year	100-year
Omnidirectional	8.3	10.4	11.6	12.7	15.2
N (348.75-360-11.25)	7.1	9.3	9.8	10.7	11.0
NNE (11.25-22.5-33.75)	8.3	10.4	11.6	12.1	12.8
NE (33.75-45-56.25)	7.1	8.9	9.5	9.7	10.0
ENE (56.25-67.5-78.75)	5.0	7.3	8.2	8.5	9.0
E (78.75-90-101.25)	4.7	6.6	7.1	7.3	7.5
ESE (101.25-112.5-123.75)	6.1	7.8	8.4	8.6	8.9
SE (123.75-135-146.25)	6.3	8.5	9.3	9.5	10.0
SSE (146.25-157.5-168.75)	6.1	7.7	8.7	9.1	9.8
S (168.75-180-191.25)	6.1	8.2	10.4	11.5	13.4
SSW (191.25-202.5-213.75)	5.3	7.3	8.3	8.7	9.3
SW (213.75-225-236.25)	5.4	7.8	10.2	11.3	13.2
WSW (236.25-247.5-258.75)	4.9	7.3	7.9	8.1	8.3
W (258.75-270-281.25)	5.6	9.0	10.2	12.7	15.2
WNW (281.25-292.5-303.75)	6.3	9.1	9.7	10.7	11.1
NW (303.75-315-326.25)	6.7	9.6	10.6	12.6	13.3
NNW (326.25-337.5-348.75)	6.4	10.2	11.6	12.1	12.8

3. Wave Generation and Propagation Model

3.1 General

As part of the hydraulic studies undertaken to support the design of the jetty, extreme wave conditions at the project location should be established.

The extreme wave conditions at the project location were established in the following 3 steps.

- Step 1: Derive the wave generation and transformation process using the Singapore regional wave model, taking into account the extreme wind conditions as described in Chapter 2;
- Step 2: Extract the extreme waves near the project location from Step 1, and derive the boundary conditions for the local wave agitation model in consideration of the ship waves induced by the passing ships;
- Step 3: Derive the extreme wave conditions at the project location using the local wave agitation model, combined with the wave transmission analysis as described in Chapter 4.

The regional wave model used in deriving the wave generation and transformation process is the Simulating Waves Nearshore (SWAN) model. To obtain the extreme wave conditions, the extreme wind speeds from different wind directions were prescribed as the driving force for the regional wave model. The model setup and output are further elaborated in Section 3.2 and 3.3. The calculation of the ship waves and the derivation of boundary conditions for the local wave agitation model are respectively described in Section 3.4 and 3.5.

3.2 Model Setup

3.2.1 SWAN

The Simulating Waves Nearshore (SWAN) model is a third-generation wave model, developed at Delft University of Technology, that computes random, short-crested wind-generated waves in coastal regions and inland waters. The model is based on the wave action balance equation (or energy balance in the absence of currents) with sources and sinks.

The following wave propagation processes are represented in SWAN:

- Rectilinear propagation through geographic space;
- Refraction due to spatial variations in the bottom and current;
- Shoaling due to spatial variation in the bottom and current;
- Blocking and reflections by opposing currents;
- Transmission through, blockage by, or reflection against sub-grid obstacles.
- The following wave generation and dissipation processes are represented in SWAN:
- Generation by the wind;
- Dissipation by white-capping;
- Dissipation by depth-induced wave breaking;
- Dissipation by bottom friction;
- Wave-wave interactions (quadruplets and triads);
- Obstacles.

3.2.2 Computational mesh

The extent, bathymetry, and computation mesh of the Singapore regional wave model for wave generation and transformation simulation are shown in Figure 3.1.

The model covers a large domain of Singapore water, approximately 145 km in both the horizontal and vertical dimensions. The model

extent is determined to enable an accurate description of the wind-wave generation, as well as to guarantee a thorough transformation of waves from the prevailing directions to the project location.

The grid cell size at the seaward end is approximately 1.5 km and decreases to just under 20 m close to the jetty with a detailed mesh to resolve the project area.

The model bathymetry was derived from three data sources:

- ETOPO global bathymetry data with a grid resolution of 30";
- Singaporean Nautical Charts;
- Survey data issued by the Client

All bathymetry data sets were converted to Chart Datum and were checked for a seamless transition ensuring that where the data sets join or overlap, no sudden steps are introduced in the model due to survey or conversion inaccuracies.

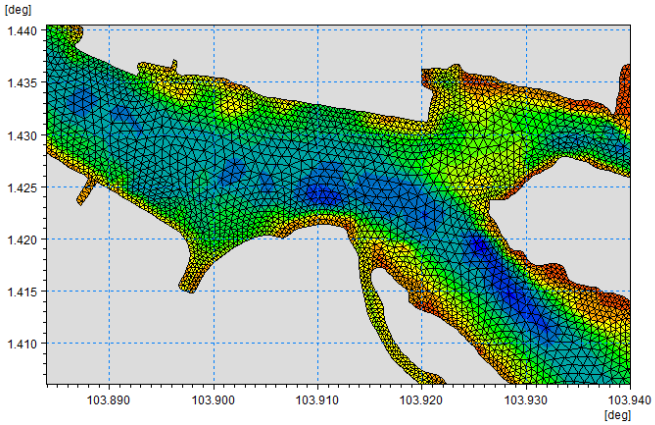


Figure 3.1 Model extent, bathymetry (m CD), and computational mesh for the Singapore regional wave model

3.2.3 Model specifications

The model was set up with a fully spectral, non-stationary formulation. This formulation is suitable for wave studies in a large domain, where the growth and decay of the wavefield have to be modeled time-dependent and varying in the domain.

The frequency discretization in this model was chosen as 27 bins with a minimum frequency of 0.04 Hz and a logarithmic frequency increment factor of 1.1, resulting in resolved wave periods in the interval 2.1 - 25 s (0.04-0.477 Hz). The directional discretization was defined from 337.5° to 202.5° sector with 20 bins resulting in a directional resolution of 11.25°.

The settings of the Singapore regional wave model are summarized in Table 3.1.

3.3 Simulation Results

Extreme coastal waves were extracted from the wind-wave simulation at pontoon near the project location, as shown in Table 3.2 summarizing the extreme wind-wave conditions

3.4 Ship Waves

As suggested by the client with an initial study on passing ships based on MPA [9], the passing ship displacement is 300 tons and the speed is 12 knots are used to compute the ship waves. With the given displacement, the formula recommended by World Association for Waterborne Transport Infrastructure (PIANC) [6] is used. The wave height, length, and period are expressed as follows:

$$H = h \cdot (s/h)^{-1/3} \cdot \left(V/\sqrt{gh}\right)^4 \quad [1]$$

$$L = 0.67(2\pi)\left(\frac{V^2}{g}\right) \quad [2]$$

$$T = \sqrt{\frac{2\pi L}{g} th \frac{2\pi h}{L}} \quad [3]$$

where,
H – wave height induced by passing ship (m);
h – water depth (m);
s – distance from passing ship (m);

V – speed of passing ship (m/s);
g – acceleration of gravity (m/s2);
L – wavelength (m);
T – wave period (s)

Speed of passing ship V was adopted as 12 kt, as stipulated in the 'Speed Limit in the East Johor Strait' issued by MPA in Mar 2005 [10]. Assuming the distance from passing ship s = 20 m, the ship waves were calculated as H = 0.76 m, T = 3.22 s.

Table 3.1 Summary of the Singapore regional wave model settings

Setting	Value
Mesh resolution	1.5 km on the offshore boundary; <20 m close to Punggol Point Jetty
Basic equations	Fully spectral
Discretization	27 frequencies with a minimum frequency of 0.04 Hz and a logarithmic frequency increment factor of 1.1 (0. 4 - 0.477 Hz; 2.1 -25 s); 20 directions from 337.5° to 202.5°
Time step	0.01 - 30 seconds
Wind forcing	Extreme wind speed from a different direction as listed in Table 2.2
Wave breaking	Included, Specified Gamma, γ=0.8

Table 3.2 Extreme wind-wave condition (kN)

Wind direction	Extreme wave conditions					
	1-year		10-year		100-year	
	H_{m0} (m)	T_p (s)	H_{m0} (m)	T_p (s)	H_{m0} (m)	T_p (s)
N (348.75-360-11.25)	0.26	2.85	0.38	3.15	0.47	3.16
NNE (11.25-22.5-33.75)	0.23	2.53	0.36	2.70	0.44	2.14
NE (33.75-45-56.25)	0.23	1.85	0.34	1.85	0.40	1.85
ENE (56.25-67.5-78.75)	0.22	2.33	0.34	1.85	0.42	1.85
E (78.75-90-101.25)	0.23	2.29	0.31	2.24	0.37	2.21
ESE (101.25-112.5-123.75)	0.25	2.38	0.35	2.38	0.42	2.39
SE (123.75-135-146.25)	0.25	2.38	0.36	2.42	0.43	2.44
SSE (146.25-157.5-168.75)	0.23	2.31	0.32	2.37	0.39	2.39
S (168.75-180-191.25)	0.21	2.34	0.31	2.35	0.40	2.44
SSW (191.25-202.5-213.75)	0.21	2.39	0.26	2.40	0.31	2.41
SW (213.75-225-236.25)	0.22	1.96	0.29	1.99	0.40	2.03
WSW (236.25-247.5-258.75)	0.24	2.01	0.36	2.01	0.42	2.02
W (258.75-270-281.25)	0.29	2.06	0.49	2.33	0.80	2.87
WNW (281.25-292.5-303.75)	0.32	2.21	0.52	2.41	0.65	2.58
NW (303.75-315-326.25)	0.33	2.24	0.58	2.64	0.81	3.16
NNW (326.25-337.5-348.75)	0.30	2.05	0.56	2.67	0.67	2.74

3.5 Composite Waves

The Overseas Coastal Area Development Institute of Japan (OCDI; 2009) recommends determining the composite waves of different wave groups using the following equations [5].

$$H_s = \sqrt{(H_1^2 + H_2^2 + \cdots + H_n^2)} \quad [4]$$

where,

Hs – significant wave height of the composite waves (m);

$H1$, $H2$, $\cdots$ Hn – significant wave height of wave groups (m)

$$T_{1/3} = k\sqrt{\frac{(H_{1/3})_I^2 + (H_{1/3})_{II}^2}{\frac{(H_{1/3})_I^2}{(T_{1/3})_I^2} + \frac{(H_{1/3})_{II}^2}{(T_{1/3})_{II}^2}}} \quad [5]$$

where,

$$k = 1.0 + \alpha(R_H/\mu)^{-0.121A\ln(R_H/\mu)};$$

$$\alpha = 0.08(\ln R_T)^2 - 0.15\ln R_T;$$

$$\mu = \begin{cases} 0.632 + 0.144\ln R_T & ; \quad 0.1 \le R_T \le 0.8 \\ 0.6 & ; \quad 0.8 \le R_T \le 1.0 \end{cases};$$

$$A = \begin{cases} 13.97 + 4.33\ln R_T & ; \quad 0.1 \le R_T \le 0.4 \\ 10.0 & ; \quad 0.4 \le R_T \le 1.0 \end{cases};$$

$$R_H = (H_{1/3})_I/(H_{1/3})_{II};$$

$$R_T = (T_{1/3})_I/(T_{1/3})_{II};$$

$(H_{1/3})_I, (H_{1/3})_{II}$ – Significant wave heights of wave groups I and II before superimposition (m);

$(T_{1/3})_I, (T_{1/3})_{II}$ – Significant wave periods of wave groups I and II before superimposition (s);

I, II – Respectively denote the wave group with shorter period and longer period

Based on the above equations, the composite extreme waves at P1 to P3, considering the wind waves as described in Section 3.3 and Ship waves as described in Section 3.4, were calculated and summarized in Table 3.3 for the 3 dominating directions: N, E, and W.

4. Wave Agitation Model

4.1 General

The wave agitation model was used to derive the extreme wave conditions at the project location, combined with the wave transmission analysis.

The wave agitation model was established with the Full Nonlinear Boussinesq Wave Model (FUNWAVE), developed at the University of Delaware. The model setup and simulation results are further elaborated in Section 4.2 and 4.3. The calculation of wave transmission and the derivation of design wave conditions are respectively described in Section 4.4 and 4.5.

Table 3.3 Extreme composite waves at P1

Wind direction	Extreme wave conditions					
	1-year		10-year		100-year	
	H_{m0} (m)	T_p (s)	H_{m0} (m)	T_p (s)	H_{m0} (m)	T_p (s)
N (348.75-360-11.25)	0.80	3.12	0.82	3.08	0.84	3.07
E (78.75-90-101.25)	0.79	3.05	0.80	2.92	0.80	2.90
W (258.75-270-281.25)	0.81	2.93	0.87	2.87	1.02	3.02

4.2 Model Setup

4.2.1 FUNWAVE

The Full Nonlinear Boussinesq Wave Model (FUNWAVE) [7], developed at University of Delaware, was applied for modelling wave penetration into and wave disturbance inside the The jetty.

FUNWAVE can be applied to the study of wave dynamics in ports and harbors and coastal areas. It is a time-domain, phase-resolving model capable of reproducing the combined effects of most wave phenomena including refraction, shoaling, diffraction, breaking, partial reflection and transmission, non-linear wave-wave interaction, frequency dispersion, and directional dispersion.

The model requires the following input:

- A digitized bathymetry;
- Basic model parameters describing the extent of the model area, the grid spacing of the computational model grid, the time step, and the duration of the simulation;
- Incident wave conditions described by flux time series on the boundaries of the model area or at internal generation lines;
- Porosities (reflection and transmission coefficients) to describe the reflection and transmission characteristics for all structures and natural obstructions (breakwaters, quay walls, beaches, etc) in the model area;
- Description of sponge layers, which are areas that absorb all wave energy propagating into the area (i.e. no reflection).

More information on the FUNWAVE model can be found at:
http://www1.udel.edu/kirby/programs/funwave/funwave.html

4.2.2 Model bathymetry

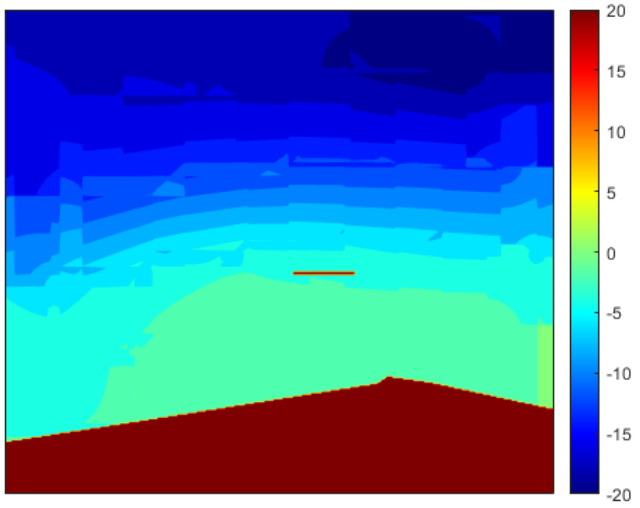
The extent, bathymetry, and computation mesh of the wave agitation model for wave penetration and disturbance simulation is shown in Figure 4.1. Two cases were studied: Case 1 – full seawall; Case 2 – half seawall.

The model covers the water area in the project location, approximately 360m and 320m in the horizontal and vertical dimensions. The model extent is roughly corresponding to the survey area where survey data is available.

The model uses rectangular grids with a uniform grid spacing of 1m. The model bathymetry was derived from the survey data.

4.2.3 Boundary conditions

From the wave generation and transformation study, extreme waves at the boundary of the wave agitation model were extracted. The boundary conditions for the wave agitation model were derived in the combination of the ship waves generated by the passing ships, as summarized in Table 3.3 shows directional irregular waves with corresponding wave height Hm0, wave period Tp, and mean wave direction were applied for defining the incident wave conditions for the wave agitation model.



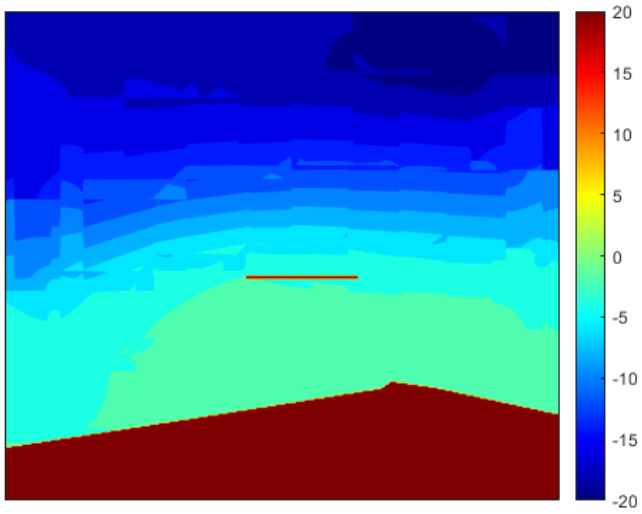


Figure 4.1 Model extent, bathymetry (m CD) & computational mesh for the wave agitation model (Top: Case 1; Bottom: Case 2).

4.3 Simulation Results

Examples of the simulation results were presented in Figure 4.2 to Figure 4.4, respectively for the cases of wind directions of N, E, and W.

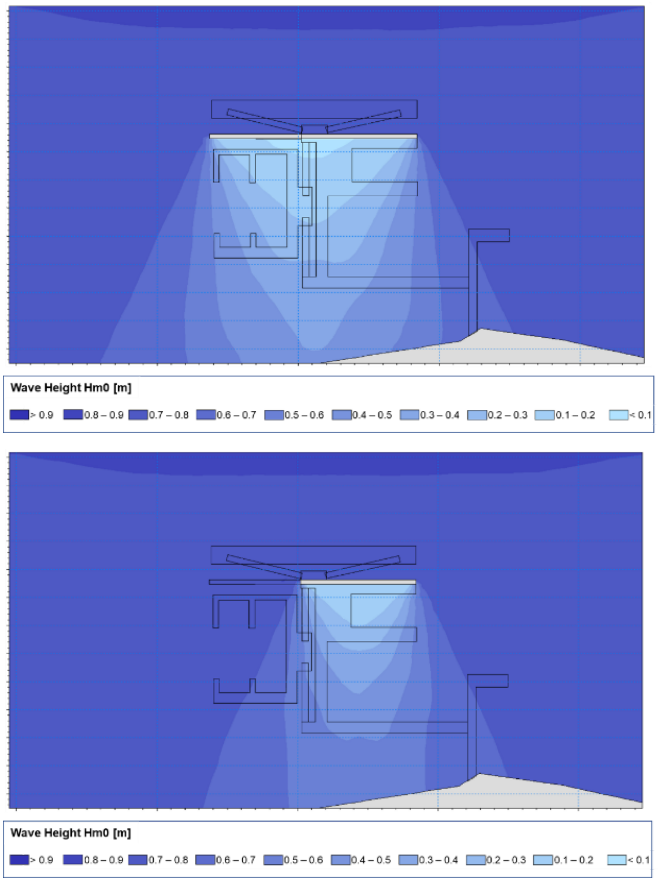
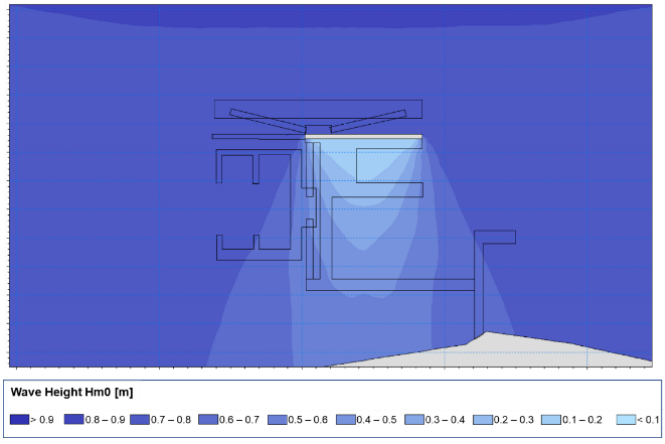


Figure 4.2 Diffraction wave map: Wind direction: N; Return period: 1 year (Top: Case 1; bottom: Case 2).



4.4 Wave Transmission

Coastal Engineering Manual (CEM; 2006) [8] recommends, for monochromatic waves and no overtopping, the resulting transmission coefficient can be calculated by:

$$C_t = \left[\frac{\frac{2k(d-y)}{\sinh 2kd} + \frac{\sinh 2k(d-y)}{\sinh 2kd}}{1 + \frac{2kd}{\sinh 2kd}}\right]^{\frac{1}{2}} \quad [6]$$

where,
d – water depth (m);
y – vertical extent of the barrier below the stillwater surface (m);
$k = 2\pi/L$ – wave number;
L – wavelength

At the seawall, $d \approx 6$ m below CD, $y = 1$ m below CD, $L \approx 16$ m, the wave transmission coefficient was calculated as $Ct = 0.37$.

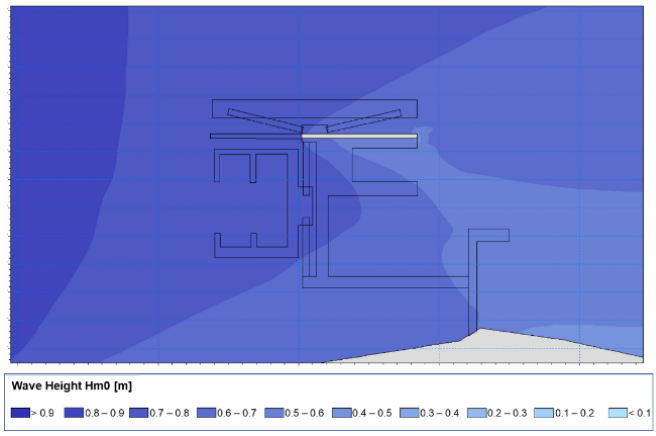


Figure 4.3 Diffraction wave map: Wind direction: E; Return period: 1 year (Top: Case 1; bottom: Case 2).

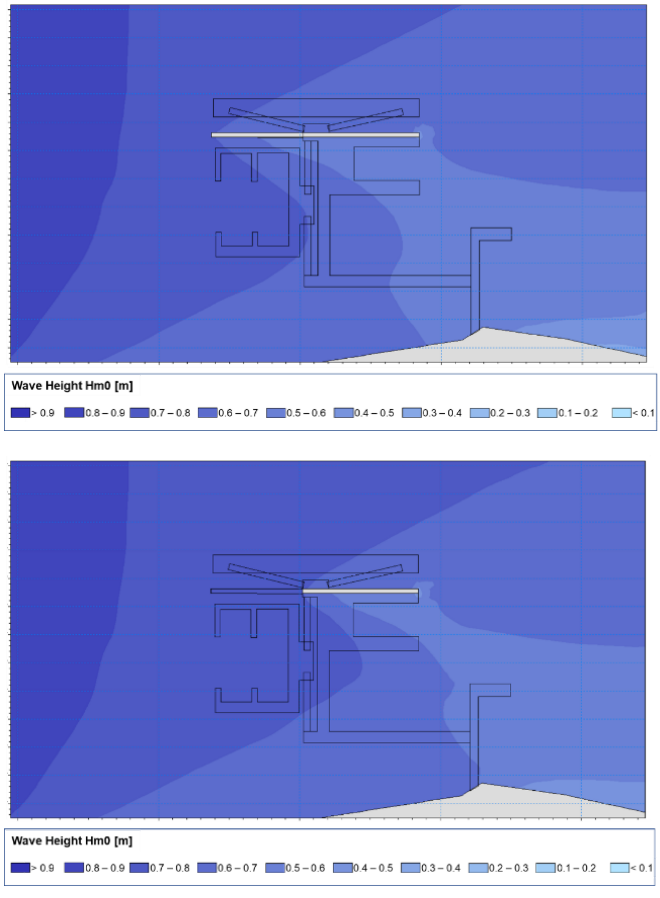


Figure 4.4 Diffraction wave map: Wind direction: W; Return period: 1 year (Top: Case 1; bottom: Case 2).

4.5 Design Wave Conditions

Design waves corresponding to different return periods were extracted from the wave agitation simulation at 13 locations. Table 4.1 through Table 4.6 summarize the design wave condition at B1 to B13 for Case 1 and Case 2.

5. Wave Force on Pontoon

5.1 General

The wave force acting on the pontoon is computed from the wave potential dynamics on both wave frequency force and wave drift force. The force under both case 1 and case 2 are calculated.

5.2 Wave Force on Pontoons

The wave frequency forces acting on the pontoons are summarized in Table 5.1.

6. Conclusions

This paper has performed an extensive literature review on the characteristic of nearshore Computational Fluid Dynamics (CFD) as compared with other fluid scenarios in the ocean. This leads to the using of SWAN as the a numerical tool for the wave study for the pontoon and the jetty.

The CFD study reviewed the wave condition over Singapore waters and creates the coastal wave model. Ship waves and composite waves are also investigated for the jetty including the past practice of the industry.

The wave load has also been calculated for the structural design of the pontoon. With regarding the pontoon wave load, which is the most critical parameter concerned by pontoon designer and also impact the pontoon fabrication case, it is

observed from CFD study that the wave load is only 30%~ 80% of half seawall under north wind environment. For east and west wind, the full seawall wave loads are 80% ~100% of half seawall.

Based on the results of the SWAN simulation, this study illustrated that the whole seawall will be helpful for the loading condition of the pontoons in the jetty.

Table 4.1 Design wave condition (Wind direction N; Case 1)

Point	Extreme wave conditions (combined with transmission)					
	1-year		10-year		100-year	
	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)
P1	0.78	3.19	0.82	3.21	0.85	3.21
P2	0.78	3.19	0.82	3.21	0.85	3.21
P3	0.37	3.20	0.39	3.22	0.41	3.23

Table 4.2 Design wave condition (Wind direction E; Case 1)

Point	Extreme wave conditions					
	1-year		10-year		100-year	
	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)
P1	0.78	3.19	0.82	3.23	0.87	3.23
P2	0.78	3. 19	0.81	3.21	0.85	3.23
P3	0.78	3. 18	0.80	3.20	0.84	3.24

Table 4.3 Design wave condition (Wind direction W; Case 1)

Point	Extreme wave conditions					
	1-year		10-year		100-year	
	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)
B1	0.76	2.94	0.81	2.90	0.97	3.02
B2	0.64	2.94	0.68	2.91	0.81	3.04
B3	0.73	2.94	0.78	2.90	0.93	3.02

Table 4.4 Design wave condition (Wind direction N; Case 2)

Point	Extreme wave conditions (combined with transmission)					
	1-year		10-year		100-year	
	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)
B1	0.79	3.20	0.83	3.22	0.86	3.22
B2	0.79	3.20	0.83	3.22	0.86	3.22
B3	0.79	3.20	0.82	3.22	0.85	3.23

Table 4.5 Design wave condition (Wind direction E; Case 2)

Point	Extreme wave conditions					
	1-year		10-year		100-year	
	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)
B1	0.65	3.04	0.68	2.96	0.69	2.93
B2	0.74	3.03	0.77	2.95	0.79	2.92
B3	0.60	3.03	0.63	2.95	0.65	2.92

Table 4.6 Design wave condition (Wind direction W; Case 2)

Point	Extreme wave conditions					
	1-year		10-year		100-year	
	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)	Hm0 (m)	Tp (s)
B1	0.77	2.94	0.82	2.90	0.98	3.02
B2	0.72	2.95	0.76	2.92	0.91	3.04
B3	0.75	2.94	0.80	2.90	0.97	3.02

Table 5.1 Wave Total Forces on Pontoons (Unit: kN)

Pontoon Numbers	North Env		East Env		West Env	
	Case 1	Case 2	Case 1	Case 2	Case 1	Case 2
1	42.1566	42.1566	30.498	30.753	38.2908	38.5764
2	10.3224	33.6702	14.1474	15.7182	17.2992	21.8892
3	15.0654	19.6248	14.6676	17.8194	27.5706	27.5706

Reference

[1] NOAA, https://polar.ncep.noaa.gov/waves/hindcasts/

[2] https://www.tudelft.nl/en/ceg/aboutfaculty/departments/hydraulicengineering/sections/environmentalfluid-mechanics/research/swan/

[3] Fundamentals of Ship Hydrodynamics: Fluid Mechanics, Ship Resistance and Propulsion, Lothar Birk, 2019

[4] Lihwa LinZeki, Demirbilek Zeki, Demirbilek Donald, WardDavid King, Wave and Hydrodynamic

[5] Chesapeake Bay, USA, Journal of Marine Science and Engineering 3(4):1474-1503, 2015

[6] OCDI (2009) Technical Standards and Commentaries for Port and Harbour Facilities in Japan. OCDI, Japan.

[7] Kriebel, D.; Seelig, W.; Judge, C. Development of a Unified Description of Ship-Generated Waves. In Proceedings of the U.S. Section PIANC Annual Meeting, Roundtable, and Technical Modeling for Engineering Design of Jetties at Tangier Island in Workshops (CD-ROM), PIANC USA, Alexandria, VA, USA, 2003.

[8] http://www1.udel.edu/kirby/programs/funwave/funwave.html

[9] U.S. Army Corps of Engineers. Coastal Engineering Manual. Engineer Manual 1110-2-1100, U.S. Army Corps of Engineers, Washington, D.C. 2006. (in 6 volumes).

[10] MPA, Maritime and Port Authority of Singapore Port Marine Circular NO. 8 OF 2005

Authors Biography

Cathy Zhao, Master's Degree of NUS. She is an expert in Computational Fluid Dynamics (CFD) for maritime, offshore, and subsea engineering. Currently, Cathy takes the lead of PetroLNG and actively competing projects for FSPO and coastal projects.

On the Application of Artificial Neural Network in Performing Relative Importance Analysis to FPSO Green Water

Shuo Wang(1), Xin Wang(2), Wai Lok Woo(3,2)

(1)Sembcorp Marine Ltd., 80 Tuas South Boulevard, Singapore 637051
(2)Newcastle University, NE1 7RU, England, UK
(3)Northumbria University, NE1 8ST, England, UK

Abstract

Artificial Neural Network (ANN) can be applied to assist the relative importance analysis, by either pre-processing the raw data and generate better inputs for traditional methods or derive the relative importance index directly from its connection weights. In this paper, both types of ANN approaches are tested and compared, using nonlinear data from the numerical analysis of green water on an FPSO. The pre-processing approach is found to be not only enhancing the efficiency of the traditional method but also expanding the applicable work scope; however, the second type of approach is generally not providing adequate estimation on the relative importance indices, and the reliability of such connection weight methods is thus questionable.

Keywords: Artificial Neural Network, Connection Weight Method, Green Water, Multi-layer Perceptron, Relative Importance

1. Introduction

Artificial Neural Network (ANN) is a type of artificial intelligence algorithm consisting of massive processors with various internal connections. In recent years, the innovative applications of ANN in the offshore and marine industry have been developing fast, assisting in various aspects of ship design, modeling, and analysis, accelerating the transformation of the industry towards a more digitalized and data-driven future.

Relative importance analysis is a commonly used technique for academic research and engineering practice, aiming to find out the relative contribution of each variable in a certain problem. The information is often useful in providing high-level guidance to the research plan, engineering design, and optimization work. Traditionally, relative importance can be evaluated using multiple linear regression (MLR), principal component analysis (PCA), partial derivative-based parametric study, as well as many other more complicated sensitivity study methods (Pianosi et al, 2016). However, all the

methods are generally suffering from high computational costs for large databases and poor quality of estimation for the sparse dataset.

In some past research works, ANN appeared to be a very useful tool in assisting relative importance analysis on many engineering problems, mainly applied in two types: data re-generating as a pre-processing step for traditional methods, and direct estimation using connection weights. Rahman et al. (2001) studied the sensitivity of the uplifting capacity of suction caissons to a few input parameters; by using MLP to re-generate the data, the parametric study was conducted in a much finer resolution than the original dataset. Tolon and Ural (2012) also performed a sensitivity analysis on the foundation area of wind turbine based on the trained ANN, and water depth was reported as the most important parameter; however, the detailed method of ANN application in this study was not elaborated. Benali, Nechnech, and Bouzid (2013) conducted some sensitivity analysis on the relative importance of various varieties to pile capacity using both PCA and Multi-layer Perceptron (MLP) neural network connection weights methods. Cheng et al. (2017) compared sensitivity study results on ship motion from three types of approaches: the traditional method on the original dataset, ANN connection weight method, and the traditional method on dataset re-generated by ANN; the ANN-EFAST method in the third type of approaches was reported to be cost-effective.

Comparing to the pre-processing approach, the second type of approach utilizing connection weights of the neural network provides much more savings on the computational cost and flexibility. However, some of the detailed results from this type of approach appeared to be not as accurate as they're expected or claimed. It can be found in Benali, Nechnech and Bouzid (2013)) that the relative importance indices calculated using ANN connection weights were not matching with PCA results; they had also reported that the relative importance results from connection weights were depending on the random initial weights of the particular ANN before training. In Cheng et al. (2017), relative importance results using modified Garson's method (mathematically same as Gedeon's method) also appeared to be very different from other methods. The discrepancy was explained by claiming Garson's algorithm as a 'local sensitivity study', thus different from other 'global sensitivity analysis' methods; however, there was no further convincing interpretation. Despite the numerous research work on the development and application of the connection weight approach with great passion and positive attitude, the comparisons of published results indicate the necessity of further research and investigation on this type of ANN application.

Floating offshore platforms moored in harsh ocean environments often encounter 'green water' incidents, which may also be referred to as 'shipping water', 'water on deck', or 'deck wetness'. When a green water incident occurs, the seawater exceeds the freeboard, runs up over the deck, and induces complicated nonlinear fluid-structure interaction. In extreme cases, the large or unexpected amount of green water can cause damage to deck plating, topside structures, and equipment, causing production downtime and threatening crew's safety. In previous studies on FPSO green water (Wang et al., 20171,2,3; Wang et al., 20181,2; Wang et al., 2019), the authors had developed and validated an effective and efficient numerical approach to estimate the green water on FPSO. To test the performance of ANN approaches in assisting relative importance analysis, two sets of nonlinear data are generated from the numerical model and used in this paper. The first set is the 3-hr most probable maximum relative wave

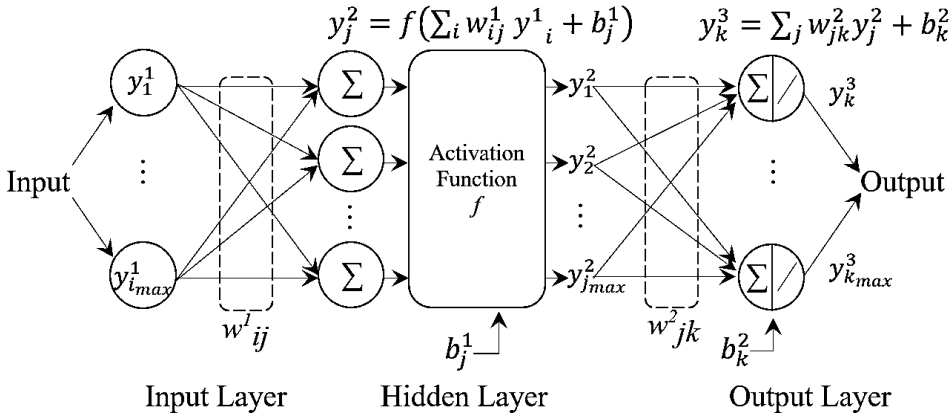


Figure 1 Typical Architecture of Multi-layer Perceptron Neural Network with 1 Hidden Layer

elevation at the midship of an FPSO in beam-sea condition; the second set is the level of green water risk using the data of the first set and the midship freeboard height. Both sets of data are generated from incident waves of various Hs and Tp.

2. Methodology

A type of feedforward backpropagate neural network called Multi-Layer Perceptron (MLP) is applied in this research to improve the efficiency and accuracy of numerical estimation in a few ways. Classic MLP neural network consists of 3 types of layers: the input layer reads the input data into the neural network; the hidden layer elements (called 'neurons') process the weighted sum of input data with activation functions; the activated signals are weighted-summed and processed again at output layer for the final result. The architecture of a typical MLP with 1 hidden layer is illustrated in Figure 1 below. The computation of the network follows a feedforward sequence from input to output.

2.1 Pre-processing Approach

The partial derivative approach marks the importance of the input variables to output by using the gradient of output to each input as an indicator. In practice, when the target data is not from a differentiable expression, the partial derivative can also be approximated numerically. Eq. (1) illustrates a common formulation of such method in estimating $\partial F/\partial x$ while x=xi and y=yi, in which F is a function of x and y, and Δx represents a small change on x.

$$\frac{\partial F(x,y)}{\partial x}\Big|_{(x_i,y_j)} \approx \frac{\Delta F}{\Delta x}\Big|_{(x_i,y_j)} = \frac{F(x_i+\Delta x, y_j) - F(x_i,y_j)}{\Delta x} \quad [1]$$

As the partial derivative result at any particular input sample only gives the local gradient, the overall condition needs to be represented by the sum or mean value of all partial derivative results throughout the target range of input. The relative importance result can then be determined by unifying all the indicators so that the sum of absolute results equals 100%. The relative importance of x to F(x, y) in Eq. (1) is expressed in Eq. (2) as an illustration.

$$RI_x = \frac{\int_x \int_y \frac{\partial F}{\partial x}\cdot dx\,dy}{\left|\int_x \int_y \frac{\partial F}{\partial x}\cdot dx\,dy\right| + \left|\int_x \int_y \frac{\partial F}{\partial y}\cdot dx\,dy\right|} \approx \frac{\sum_x \sum_y \frac{\Delta F}{\Delta x}}{\left|\sum_x \sum_y \frac{\Delta F}{\Delta x}\right| + \left|\sum_x \sum_y \frac{\Delta F}{\Delta y}\right|} \quad [2]$$

However, if the gradient is not monotonous, the positive and negative gradients will cancel each other, thus reducing the reliability of the indicator. To overcome such a problem, the indicator may also be taken from the sum or mean of the absolute value of the partial derivatives, as illustrated in Eq. (3).

$$RI_x \approx \frac{\sum_x \sum_y \left|\frac{\Delta F}{\Delta x}\right|}{\sum_x \sum_y \left|\frac{\Delta F}{\Delta x}\right| + \sum_x \sum_y \left|\frac{\Delta F}{\Delta y}\right|} \quad [3]$$

When applying the numerical partial derivative approach to estimate the relative importance of variables, the partial derivative needs to be calculated on a large number of samples to effectively cover the target input range, and the calculation shall be repeated for each variable. However, if the dataset is allocated in a uniform grid, the output values can be re-used in calculating the partial derivatives for different variables, thus significantly reducing the overall computational cost. Therefore, when the original data set from measurement or complicated calculation is not arranged in a uniform grid, MLP can be applied to obtain the data samples on the uniform grid via interpolation, thus accelerating the evaluation of relative importance significantly.

2.2 Connection Weights Approach

Besides the direct application in assisting the evaluation of relative importance in the traditional method, it is also claimed by some researchers that the connection weights in MLP can be interpreted to have relative importance directly. A few methods are listed below, based on the typical MLP ANN as illustrated in Figure 1, with 1 hidden layer.

Garson's Algorithm (Garson, 1991)

$$RI_{ik} = \frac{\sum_{j=1}^{j_{max}} \left(\frac{w_{ij}}{\sum_{p=1}^{i_{max}} w_{pj}} \cdot w_{jk} \right)}{\sum_{q=1}^{i_{max}} \left(\sum_{j=1}^{j_{max}} \left(\frac{w_{qj}}{\sum_{p=1}^{i_{max}} w_{pj}} \cdot w_{jk} \right) \right)} \quad [4]$$

Garson-Milne Method (Milne, 1995)

$$RI_{ik} = \frac{\sum_{j=1}^{j_{max}} \left(\frac{w_{ij}}{\sum_{p=1}^{i_{max}} |w_{pj}|} \cdot w_{jk} \right)}{\sum_{q=1}^{i_{max}} \left| \sum_{j=1}^{j_{max}} \left(\frac{w_{qj}}{\sum_{p=1}^{i_{max}} |w_{pj}|} \cdot w_{jk} \right) \right|} \quad [5]$$

Gedeon's Method (Gedeon, 1997)

$$RI_{ij} = \frac{|w_{ij}|}{\sum_{p=1}^{i_{max}} |w_{pj}|}; \quad RI_{jk} = \frac{|w_{jk}|}{\sum_{q=1}^{j_{max}} |w_{qk}|}; \quad [6]$$

$$RI_{ik} = \sum_{r=1}^{j_{max}} (RI_{ir} \cdot RI_{rk})$$

Olden's Connection Weights Method (Olden et al, 2004)

$$[RI_k] = \text{Unify}([w_{ij}] \times [w_{jk}]) \quad \text{or}$$

$$RI_{ik} = \frac{\sum_{j=1}^{j_{max}} (w_{ij} \cdot w_{jk})}{\sum_{q=1}^{i_{max}} \left| \sum_{j=1}^{j_{max}} (w_{qj} \cdot w_{jk}) \right|} \quad [7]$$

A derivation of Olden's method, inspired by Gedeon's method:

$$[RI_{ik}] = \text{Unify}([|w_{ij}|] \times [|w_{jk}|]) \quad \text{or}$$

$$RI_{ik} = \frac{\sum_{j=1}^{j_{max}} (|w_{ij}| \cdot |w_{jk}|)}{\sum_{q=1}^{i_{max}} \sum_{j=1}^{j_{max}} (|w_{qj}| \cdot |w_{jk}|)} \quad [8]$$

It is also worth mentioning that the Garson's algorithm is found to be modified in some literature (Goh, 1995; Olden and Jackson, 2002), and is different from the original version. As

shown in Eq. (9), the formulation is mathematically equivalent to the averaged contribution of the input variable to the entire hidden layer, without considering the hidden-to-output connection weights at all.

Modified Garson's Algorithm (Goh, 1995; Olden and Jackson, 2002)

$$RI_{ik}=\frac{\sum_{j=1}^{j_{max}}\left(\frac{|w_{ij}|\cdot|w_{jk}|}{\sum_{p=1}^{i_{max}}|w_{pj}|\cdot|w_{jk}|}\right)}{\sum_{q=1}^{i_{max}}\sum_{j=1}^{j_{max}}\left(\frac{|w_{qj}|\cdot|w_{jk}|}{\sum_{p=1}^{i_{max}}|w_{pj}|\cdot|w_{jk}|}\right)}=\frac{\sum_{j=1}^{j_{max}}\left(\frac{|w_{ij}|}{\sum_{p=1}^{i_{max}}|w_{pj}|}\right)}{\sum_{j=1}^{j_{max}}\left(\frac{\sum_{q=1}^{i_{max}}|w_{qj}|}{\sum_{p=1}^{i_{max}}|w_{pj}|}\right)}=\frac{\sum_{j=1}^{j_{max}}RI_{ij}}{j_{max}} \quad [9]$$

In this paper, a few ANN connection weight methods based on MLP are tested, including the Garson-Milne method (GM), Olden's native connection weights method (Olden), the derivation of Olden's method (Olden-Abs), and Gedeon's method (Gedeon).

2.3 FPSO Green Water Dataset

For FPSO green water assessment, most of the attention is usually focused on the relative wave elevation (RWE), which is the relative movement between the hull and the free surface of the disturbing wave, as shown in Eq. (10) below.

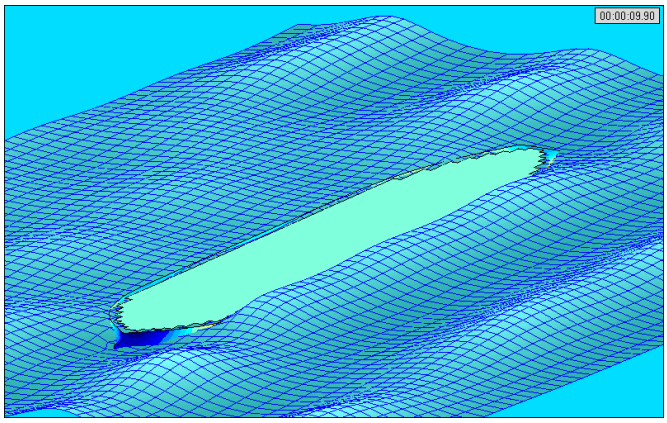
$$RWE=-z+\left(\zeta_0+\sum_{i=1}^{6}\zeta_i+\zeta_7\right) \quad [10]$$

where z is the vertical motion of the hull, ζ_0 is the incident wave, $\zeta_{1\text{-}6}$ is the radiated wave and ζ_7 is the diffracted wave.

With the RAO of the RWE and incident wave spectrum, the RWE response in an irregular incident wave can be evaluated and expressed statistically with the significant response, RWEsig, and zero up-crossing periods, Tz. The most probable maximum RWE response in a typical sea-state duration of 3 hours can then be expressed as shown in Eq. (11) below.

$$RWE_{MPM}=RWE_{sig}\cdot\sqrt{\frac{1}{2}\ln\left(\frac{3hr}{T_Z}\right)} \quad [11]$$

An FPSO model in beam sea condition is chosen to produce the dataset needed for the ANN application tests. The numerical simulation is based on linear potential theory and solved in the frequency domain using Commercial software ANSYS AQWA, and validated by comparing with lab test measurements, as presented in Figure 2. Numerous irregular incident waves are included in the simulation, to fully cover the following range Hs ϵ [1m, 19m], Tp ϵ [4s, 25s]. This range of incident wave parameters and resulting extreme response values may have largely exceeded the normal practical conditions, but the generated dataset is good enough for the testing purpose. RWE results at the portside midship of the FPSO are obtained from the simulation to derive RWEmpm which can be used directly as output for the training of a neural network.



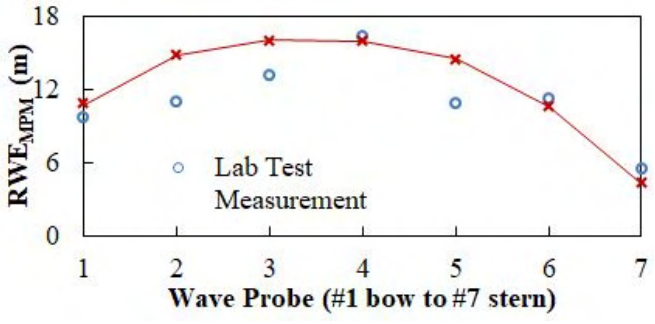


Figure 2 Validated Numerical Analysis of Green Water on an FPSO in Beam-Sea

In addition to the normal continuous type of output directly from numerical modeling, a discrete type of FPSO green water assessment result is also generated, by classifying the green water risk into 4 different levels based on the exceeding height of RWE over the freeboard, as proposed in Morris, Miller, and Buchner (2000). Both datasets are plotted in Figure 3 for illustration.

To further prepare the database for MLP training, the classified categories of zero /low /moderate /high risk of green water are further transformed into 4 binary digits: C036 = [1 0 0 0] as zero risk, C036 = [0 1 0 0] as low risk, C036 = [0 0 1 0] as moderate risk, and C036 = [0 0 0 1] as high risk. The trained MLP will generate the output as 4 real numbers; by setting the largest unit among the 4 from MLP to be 1, and the rest 3 units as 0, the original risk level data C036 of 4 binary digits can be effectively re-produced.

2.4 Training Approach of Neural Network

To test the two types of ANN approaches for relative importance analysis, the neural network needs to be trained with the dataset first. In this study, the MLP feedforward neural network with 1 hidden layer of 16 neurons is selected, and the training is performed with the typical back-propagation method, and with Bayesian Regularization to enhance the quality of the trained network. The dataset is randomly divided into two sets, to have 80% of the data being allocated to the training set and 20% to the testing set.

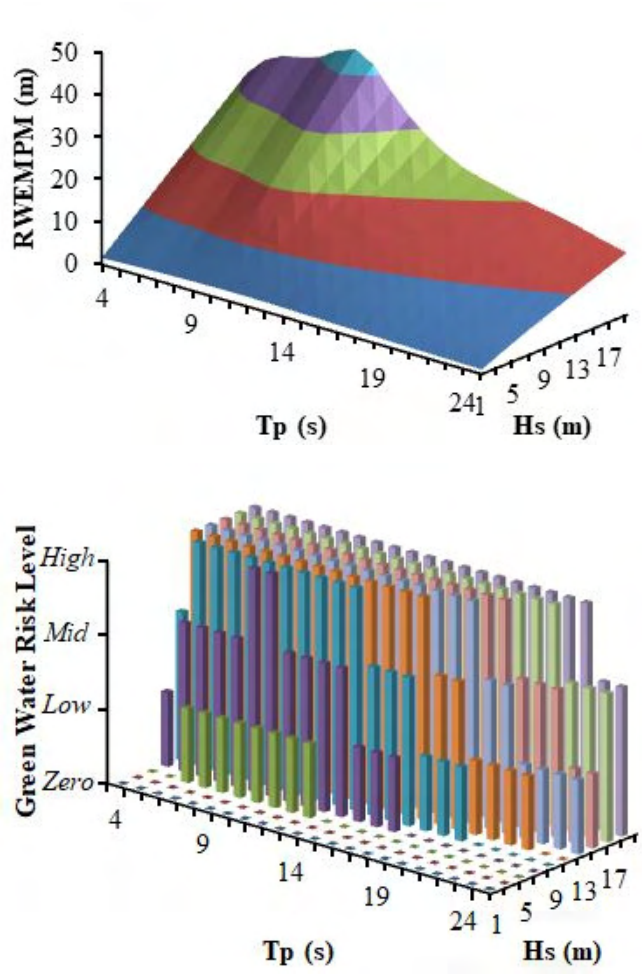


Figure 3 Numerically Generated Datasets of FPSO Green Water for Testing of ANN Approaches (upper: RWE_{MPM} ; lower: Green Water Risk Level)

In addition to the normal practice of neural network training practice, a novel training approach is further proposed to effectively and efficiently find the MLP with the typical quality of its type. A typical error level of the MLP is defined as shown in Eq. (12) below:

$$MSE_{critic} = \exp\left(\text{Mean}\left(\text{Ln}(MSE)\right) - \left(s + t_{inv}(p,i)/\sqrt{i}\right)\cdot\text{std}\left(\text{Ln}(MSE)\right)\right) \quad [12]$$

where MSE is the mean square error of the trained neural network, $t_{inv}(p, i)$, is the Student's t inverse cumulative distribution function for sample quantity of i and desired probability p for the sample mean to be below the population mean. The reliability of the estimated mode value can be controlled by adjusting p, and target performance level by adjusting s. In this study, p=0.95 and s=1 are used for the training process.

Figure 4 shows the flow chart for the proposed methodology to get an MLP with typical quality. The MLP is repeatedly trained with randomly generated initial connection weights, and the critical MSE from Eq. (12) is keeping updated with MSE from each trained MLP. When the MSE of an MLP is lower than MSEcritic, the neural network is considered as achieved its typical performance. In general, the MSE checking should be performed on testing error, so that the MLP is selected based on its capability of generalization; but the training error may also be checked at the same time.

3. Results and Discussion

As shown in Figure 5 below, the MLP trained from RWE_{MPM} dataset has obtained a very low error level and very high accuracy. 'However, for the MLP trained from the discrete dataset of green water risk level, the outputs produced by MLP are continuously distributed in a range, leading to a relatively 'poor' fitting to the binary output, as shown in Figure 6.

The accuracy rates of green water risk level assessment by the trained MLP are presented in Table 1, using numerical estimation as a benchmark. Despite the 'poor' fitting shown in Figure 6, the trained MLP appears to be successfully predicting the risk level of green water with high accuracy.

Since the overall performance of MLP appears to be reliable, the relative importance analysis can thus be conducted on the green water risk level assessment, using the differentiable MLP output.

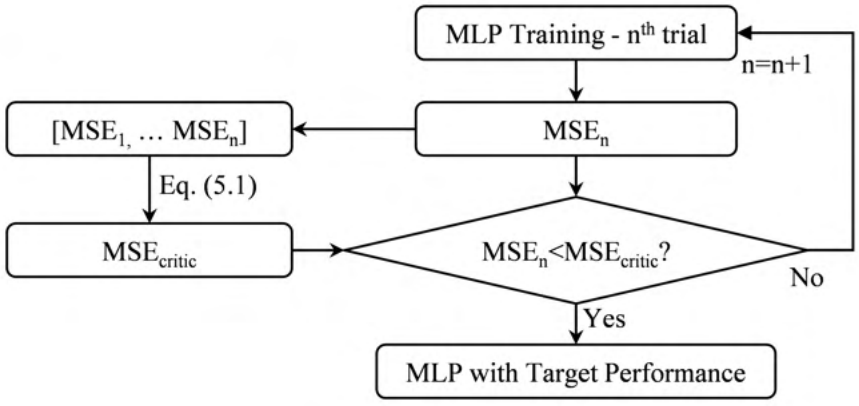


Figure 4 Flow Chart for Proposed MLP Training Scheme

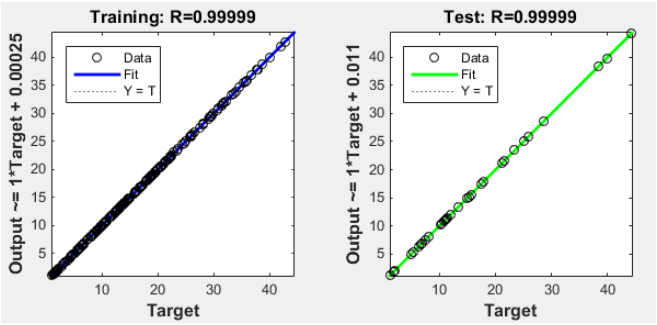


Figure 5 Fitting by MLP on RWEMPM Dataset

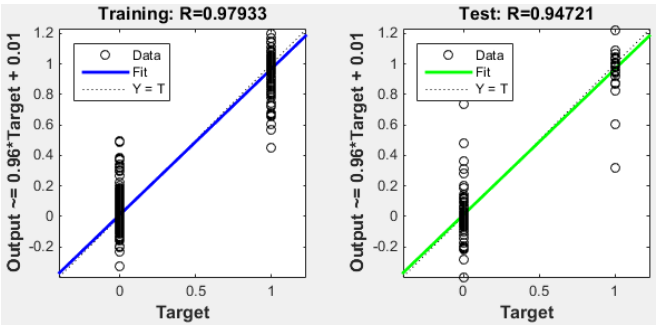


Figure 6 Fitting by MLP on Risk Level Dataset

3.1 ANN Pre-processing Approach

The relative importance analysis based on the partial derivatives is performed on RWE_{MPM} and C036 results, following Eq. (2) (expressed as 'PD') and Eq. (3) (expressed as 'PD-Abs'). The analysis is successfully assisted by the 1st type of ANN approach, in which the results are re-generated by ANN and allocated in a uniform grid to facilitate the RI indices estimation.

Besides, it is also interesting to see that, with the assistance of the ANN, the partial derivative method can also be applied to the discrete dataset, which is originally not differentiable. The application of ANN has not only improved the efficiency of the partial derivative method but also extended the type of data it can process.

3.2 ANN Connection Weight Approach

The relative importance analysis results for the input of Hs and Tp to the RWEmpm are presented in Figure 7, using the several selected connection weight methods. To avoid the possible effect of random initial weights, the MLP with typical performance is obtained using the method stated in Figure 4, and repeated 6 times, resulting in 6 sets of RI outputs from each method. The RI indices from the 1st type of ANN approach in Table 2 are also involved in the plot as a benchmark.

Based on the capability of indicating +/- sign in the RI results, the selected connection weight methods can be roughly categorized into two groups: Garson-Milne and Olden methods work on connection weights with original signs, and the resulting RI could be positive or negative to generally indicate the increase or decline relationship between output and input; Gedeon and Olden-Abs methods work on the absolute value of connection weights, resulting in only positive RI indices. The former group is comparable to the RI from the PD method, and the latter group is comparable to PD-Abs.

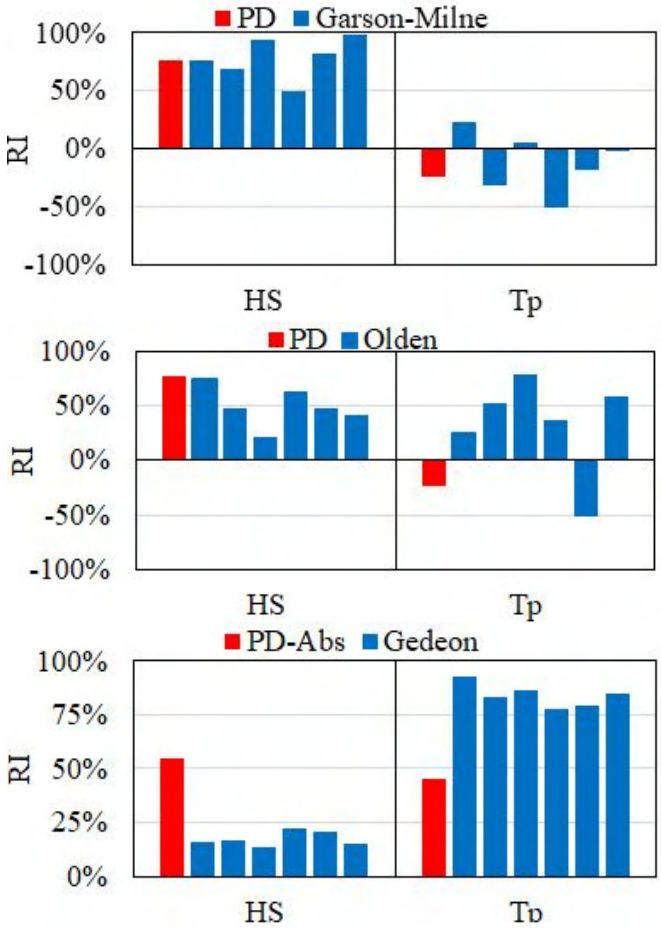
Comparison among 6 sets of RI output from each connection weight method shows that methods from the singed group, like the Garson-Milne method and Olden method, can't even produce self-consistent RI results. In contrast to the signed group, RI results produced from absolute group methods like Gedeon and Olden-Abs are observed to be generally self-consistent in this study. However, the results are very different from the benchmark generated using the absolute values of the partial derivative. Generally speaking, all the connection weight methods are surprisingly and unexpectedly not able to provide RI indices with sufficient quality.

Table 1 Accuracy Rate of Green Water Risk Level Assessment using MLP ANN

		Numerical Simulation			
		Zero Risk	Low	Moderate	High
MLP	Zero Risk	33.18%	0.00%	0.00%	0.00%
	Low	0.00%	11.36%	0.00%	0.00%
	Moderate	0.00%	0.00%	10.45%	0.45%
	High	0.00%	0.00%	0.91%	43.64%

Table 2 Relative Importance Results from 1st Type of ANN Approach

Relative Importance		PD		PD-ABS	
		H_S	T_P	H_S	T_P
RWE_{MPM}		0.7632	-0.2369	0.5441	0.4559
C_{036}	Zero	-0.7241	0.2759	0.6467	0.3533
	Low	0.0365	0.9635	0.6056	0.3944
	Moderate	0.4338	-0.5662	0.5796	0.4204
	High	0.6486	-0.3514	0.5615	0.4385



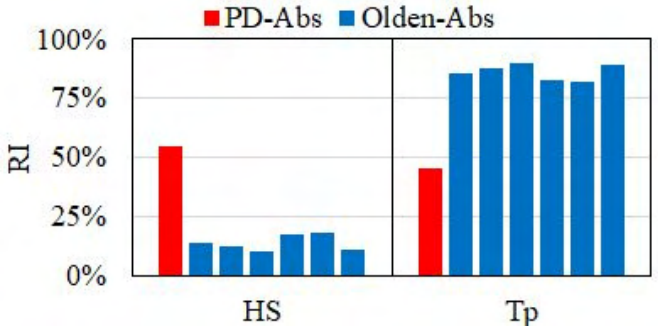


Figure 7 Comparison of RI from Connection Weight and Partial Derivative Methods

3.3 Further Investigation

By carefully comparing the methodologies of relative importance analysis based on partial derivatives and MLP connection weights, an interesting difference between the two types of approaches is noticed, that the range limit of input variables can be involved in the evaluation of averaged partial derivative, which is however not clearly described in the connection weight methods.

The RI analysis by partial derivative is only working on the results within the range of the given input. In practice, there is often a good

reason for the range limit of variables to be considered: value beyond the limit can be physically invalid, or outside the interest of the analysis. In certain situations, the range of input variables can significantly affect the relationship between input and output; the conclusion of relative importance analysis on different input ranges can vary widely.

On the other hand, the application of MLP does not provide a strict boundary to the learning results. The activation functions (linear, sigmoid, etc.) are purposely selected for MLP so that they would apply to the input variable of any real number. Therefore, even if the MLP is trained from a limited dataset, the output result for new input outside the original range of training samples shall exist mathematically, even if the range extension is against the physics concept. An example of a response surface extend to infinity by MLP is illustrated in Figure 8. When fitting the RWE database with Hs in [1m, 19m], Tp in [4s, 25s], the resulting MLP is representing a response surface of (-∞, +∞).

Regarding the relative importance analysis method using MLP connection weights, since the value of weights are valid for input variable of any real number, and the calculation does not require any information about the range of variable, the estimated result is expected to represent the characteristics of the entire surface, rather than the limited range of training samples or range of interest.

To test the above hypothesis, one of the trained MLP neural network is used to generate truncated response surface with various magnitudes of input range expansion, and the relative importance of input variables for each surface are evaluated with partial derivative methods. The results are summarized in Figure 9. The evaluated relative importance is observed to be affected by varying the input range. With the input range expanded towards infinity, RI results by PD and PD-Abs gradually converge to certain values, fitting towards the entire surface represented by the MLP neural network.

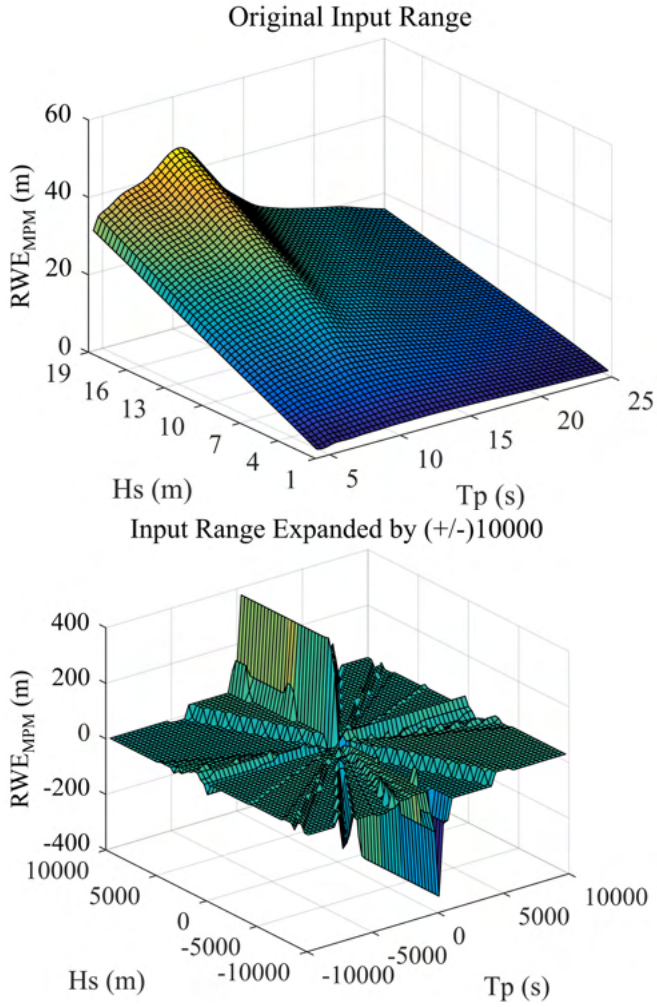
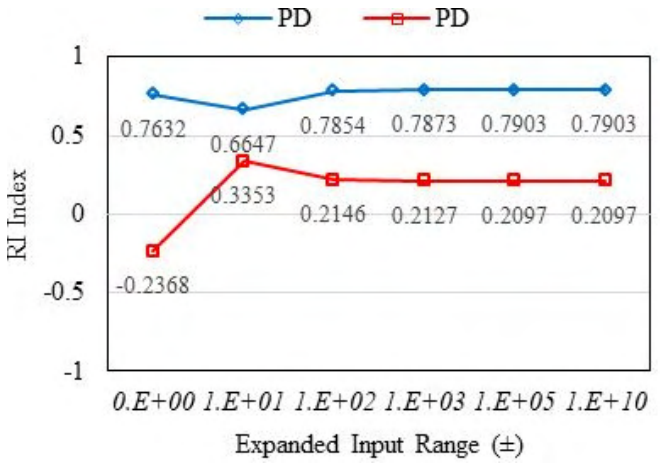


Figure 8 Response Surface from MLP with Extended Ranges of Inputs



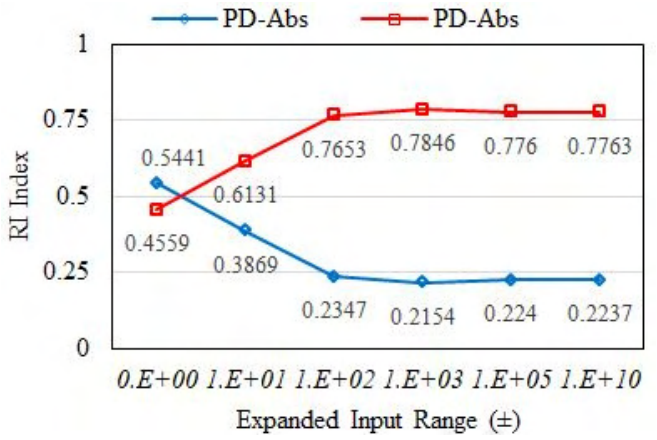
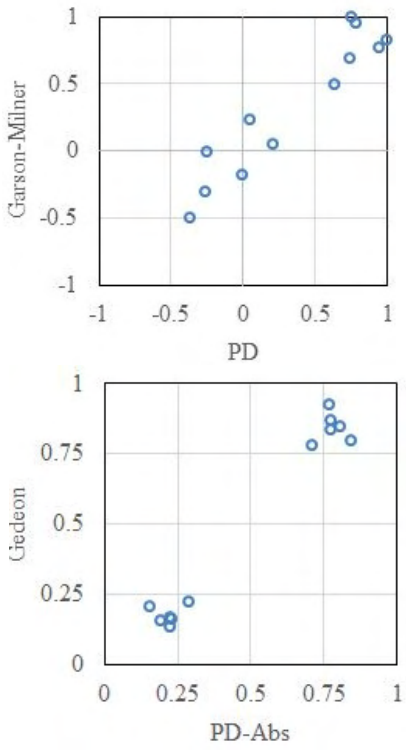


Figure 9 RI of RWE_{MPM} Response with Input Range Expanded by Various Magnitudes

By expanding the range limits of H_S and T_P on all the 6 MLPs with additional $\pm 10^{10}$, the RI results from PD and PD-Abs methods to different input ranges are compared to connection weight methods, as presented in Figure 10. As observed from the comparison, Garson-Milne, Gedeon, and Olden-Abs methods are showing clear agreement with partial derivative results; however, the RI results from the original Olden's method are still discrepant from the benchmark results.



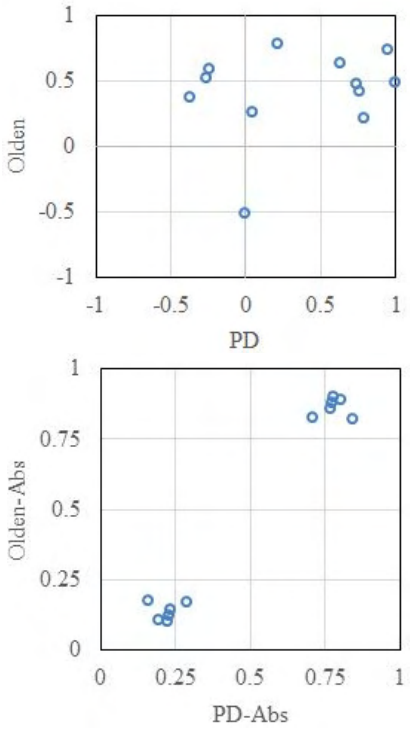


Figure 10 RI Comparison with Input Range Expanded by $\pm 10^{10}$

4. Conclusion and Recommendation

Two types of ANN approach for relative importance analysis are tested in this paper, using nonlinear data from the numerical analysis of green water on an FPSO. The pre-processing approach is found to be not only enhancing the efficiency of the traditional method but also expanding the applicable work scope. The second type of approach is generally not providing adequate estimation on the relative importance indices.

Further investigation has unveiled that the discrepancy is related to the range of data that each approach is working on. The connection weight methods are likely to be eventually working on the entire surface/hypersurface represented by the neural network, thus fail to reflect the characteristics of the limited data of interest.

To assist the relative importance analysis with

ANN, it is recommended to choose the pre-processing approach, and avoid any connection weight method at the moment. More rigorous studies and tests are needed to further develop the understanding of the connection weights inside the "black-box". Besides, since some methods like Gedeon and Olden-Abs appear to provide self-consistent results, some attempts might also be made to figure out if there is some more adequate manner to utilize such operation and indices.

Acknowledgement

The authors are grateful for the financial support by the Singapore Economic Development Board Industrial Postgraduate Programme and Sembcorp Marine Ltd, which enabled them to carry out the research in this paper.

Nomenclature

C_{036} Level	FPSO Green Water Risk
Hs	Significant Wave Height
MPM Response	Most Probable Maximum
MSE	Mean Squared Error
RAO	Linear Response Amplitude Operator
RI	Relative Importance Index
RWE	Relative Wave Elevation
sig	Significant Response
Tp	Wave Peak Period
Tz	Zero Up-crossing Period

Reference

Benali, A., Nechnech, A., and Bouzid, D.A., 2013. Principal Component Analysis and Neural Networks for Predicting the Pile Capacity Using SPT. IACSIT International Journal of Engineering and Technology, Vol. 5, No. 1.

Cheng, X., Chen, S., Diao, C., Liu, M., Li, G., and Zhang, H., 2017. Simplifying Neural Network Based Model for Ship Motion Prediction: A Comparative Study of Sensitivity Analysis. Proceedings of 36th International Conference on Ocean, Offshore and Arctic Engineering, Trondheim, Norway.

Garson, G.D., 1991. Interpreting Neural Network Connection Weights. Artificial Intelligence Expert, 6: 47-51.

Gedeon, T.D., 1997. Data Mining of Inputs: Analysing Magnitude and Functional Measures. International Journal of Neural Systems (1997), 8(2):209-17.

Goh, A.T.C., 1995. Back-propagation Neural Networks for Modelling Complex Systems. Artificial Intelligence in Engineering 9 (1995), 143-151.

Milne, L.K., 1995. Feature Selection Using Neural Networks with Contribution Measures. Proceedings Australian Conference on Artificial Intelligence AI'95, Canberra, 1995.

Morris, W.D.M., Millar, J., and Buchner, B., 2000. Green Water Susceptibility of North Sea FPSO/FSUs, IBC 15th Conference on Floating Production Systems.

Olden, J.D. and Jackson, D.A., 2002. Illuminating the 'Black Box': Understanding Variable Contributions in Artificial Neural Networks. Ecological Modelling 154 (2002), 135–150.

Olden, J.D., Joy, M.K., and Death, R.G., 2004. An Accurate Comparison of Methods for Quantifying Variable Importance in Artificial Neural Networks using Simulated Data. Ecological Modelling 178 (2004), 389–397.

Pianosi, F., Beven, K., Freer, J., Hall, J.W., Rougier, J., Stephenson, D.B. and Wagner, T. Sensitivity Analysis of Environmental Models: A Systematic Review with Practical Workflow. Environmental Modelling and Software 79 (2016), 214-232.

Rahman, M.S., Wang, J., Deng, W., and Carter, J.P., 2001. A Neural Network Model for the Uplift Capacity of Suction Caissons. Computers and Geotechnics 28 (2001), 269-287.

Tolon, M., and Ural, D.N., 2012. Geotechnical Considerations for Offshore Wind Turbines based on Neural Network. The 2012 World Congress on Advances in Civil, Environmental, and Materials Research (ACEM' 12), Seoul, Korea.

Wang, S., Wang, X. and Woo, W.L., 2017. Numerical Green Water Assessment for an FPSO with Consideration of Nonlinear Effects from Bilge Keel, Spread Mooring and Asymmetric Risers. Proceedings of 27th International Offshore and Polar Engineering Conference, San Francisco, CA, USA.

Wang, S., Wang, X. and Woo, W.L., 2017. Numerical Study on the Effects of Bilge Keel, Mooring and Riser Arrangement on FPSO Motion and Green Water Assessment. Proceedings of 10th International Workshop on Ship and Marine Hydrodynamics.

Wang, S., Wang, X. and Woo, W.L., 2018. A Comparison of Response-based Analysis and Environmental Contour Methods for FPSO Green Water Assessment. Proceedings of the 37th International Conference on Ocean, Offshore and Arctic Engineering (OMAE), Madrid, Spain.

Wang, S., Wang, X. and Woo, W.L., 2019. Effects of the Asymmetric Riser and Bilge Keel Arrangements on FPSO Green Water Assessment. Applied Ocean Research 86 (2019), 166-176

Wang, S., Wang, X. and Woo, W.L., 2018. On the Application of Simplified CFD Model in Assisting FPSO Green Water Assessment at Bow. Proceedings of 28th International Offshore and Polar Engineering Conference, Sapporo, Japan.

Wang, S., Wang, X., Woo, W.L. and Seow, T.H., 2017. Study on Green Water Prediction for FPSOs by a Practical Numerical Approach. Ocean Engineering, 143, 88-96

Authors Biography

Dr. Shuo Wang is currently working at Sembcorp Marine Ltd. as Assistant Manager. His working contents include hydrodynamic, mooring, and CFD analysis. He received his Doctoral degree from Newcastle University in Singapore, with the research on FPSO green water numerical analysis with ANN application, funded by the programme of EDB-SCM-IPP.

Dr Xin Wang is an Assistant Professor at Newcastle University in Singapore.He received his Doctoral degree in Ocean and Space Engineering from Yokohama National University, Japan. His research focuses on computational

methods for marine hydrodynamics (including LNG sloshing and nonlinear wave-body interactions) and ship energy efficiency optimization. Singapore. He received his Doctoral degree in Ocean and Space Engineering from Yokohama National University, Japan. His research focuses on computational methods for marine hydrodynamics (including LNG sloshing and nonlinear wave-body interactions) and ship energy efficiency optimization.

Dr. Wai Lok Woo is currently a Professor of Machine Learning at Northumbria University, UK. His research interests include the mathematical development of sensor signal processing and machine learning for anomaly detection and digital sustainability. He is the Associate Editor of several IEEE journals and is funded by the UK Research and Innovation Council.

From the Editor

Welcome to our very special commemorative issue of SNAMES Annual Journal to mark 40 years since our launch in the year 1981. The journal was created to satisfy the pressing need for an outlet that would publish articles dealing with a broad range of applied problems in the maritime industry.

Over the years, the journal has built a reputation for publishing outstanding work and so it seemed appropriate to us to commemorate the 40th by publishing a special issue with eleven of the influential papers this year. The anniversary is an opportunity to reflect not only on the past but also on the future. The year 2021 will be notable for the SNAMES Annual Journal apart from this 40th anniversary.

As the journal publishes articles on a broad range of topics, this year we focused on the themes **'Sustainable Development'** and **'Digital Innovation'**. The maritime industry is working continuously to reduce shipping's environmental impact and improve efficiency, optimize operation, reduce cost and achieve compliance through digital transformation. The COVID-19 pandemic has also brought the focus on how technology will shape the maritime sector in the future. The themes covered are inference about the industry in decarbonization, cybersecurity, artificial intelligence, management, and last but not least, structure design and simulation.

We hope that through the various technical papers, readers across the industry – business leaders, professionals and technologists – will be encouraged to move beyond their current boundaries. These papers are written by accomplished professionals and academics. Among the eleven papers featured in this edition include the following:

Can shipyards in Singapore remain relevant? The threats and opportunities ahead by Lim Soon Heng

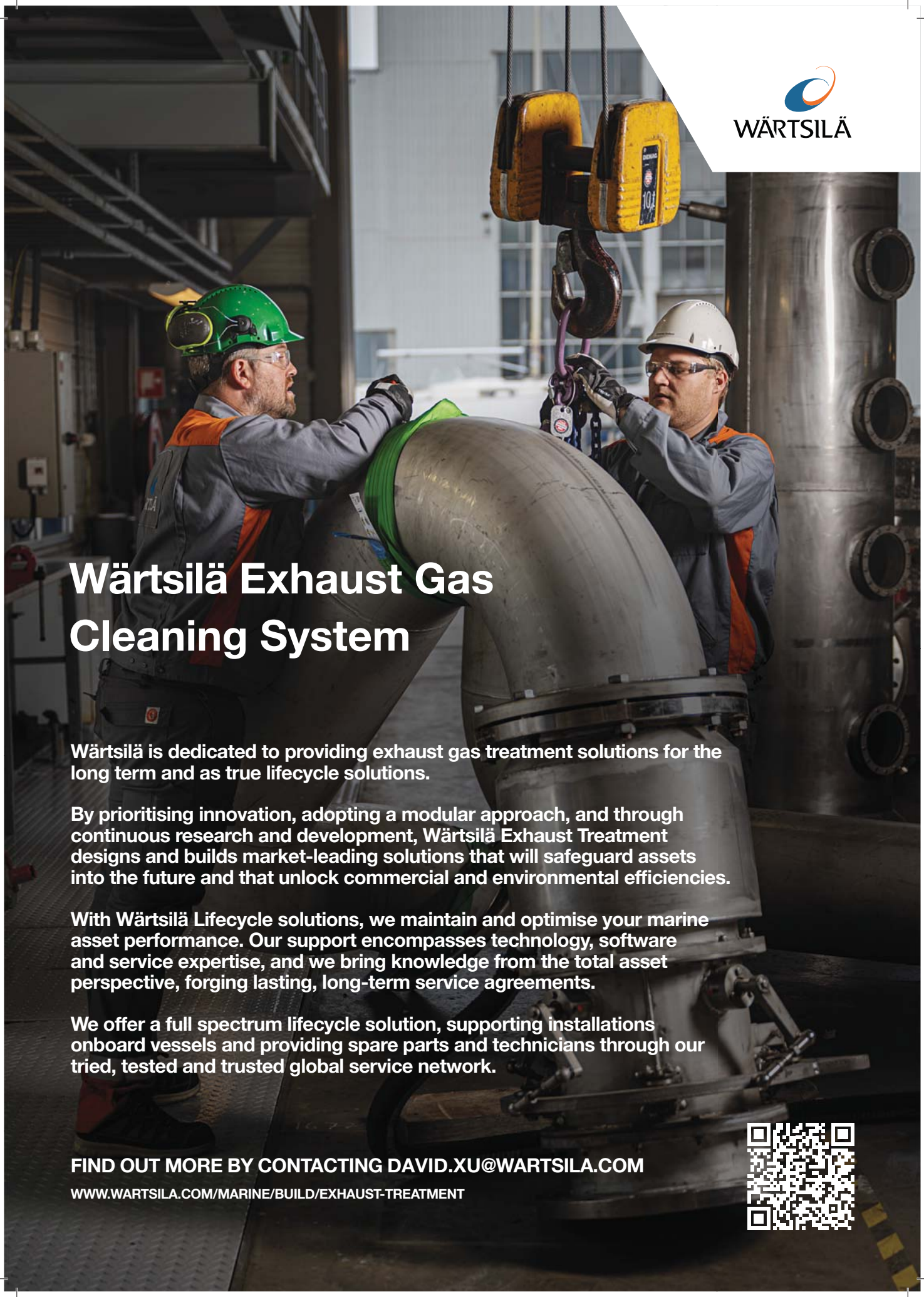
Challenges in Meeting Upcoming EEXI Requirement by Shukui Liu, Baoguo Shang, Joo Hock Ang, and Jun Jie Tan

Application of Artificial Intelligent on Cargo Identification during Port Tally by Johnson Zhu

In closing, on behalf of the SNAMES Council, I would like to appreciate the companies and partners who have unreservedly supported the Journal and SNAMES over the years via advertisement placements, event sponsorships and participation in SNAMES-organised events. We look forward to our partners' continual strong support and our members in our activities.

Sincerely

Dr Ji Xi
SNAMES Publication Chairperson



WÄRTSILÄ

Wärtsilä Exhaust Gas Cleaning System

Wärtsilä is dedicated to providing exhaust gas treatment solutions for the long term and as true lifecycle solutions.

By prioritising innovation, adopting a modular approach, and through continuous research and development, Wärtsilä Exhaust Treatment designs and builds market-leading solutions that will safeguard assets into the future and that unlock commercial and environmental efficiencies.

With Wärtsilä Lifecycle solutions, we maintain and optimise your marine asset performance. Our support encompasses technology, software and service expertise, and we bring knowledge from the total asset perspective, forging lasting, long-term service agreements.

We offer a full spectrum lifecycle solution, supporting installations onboard vessels and providing spare parts and technicians through our tried, tested and trusted global service network.

FIND OUT MORE BY CONTACTING DAVID.XU@WARTSILA.COM

WWW.WARTSILA.COM/MARINE/BUILD/EXHAUST-TREATMENT