

Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.
- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author's moral rights contained in Part IX of the Copyright Act 1968 (Cth).
- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

A COMPREHENSIVE ANALYSIS OF SMART SHIP SYSTEMS AND UNDERLYING CYBERSECURITY ISSUES

This thesis is presented in partial fulfilment of the degree of
Bachelor of Science (Security) Honours

Dennis Bothur

Principal Supervisor: Prof. Craig V
Supervisor: Dr Guanglou Zheng

School of Science
Edith Cowan University
2020

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

Abstract

The maritime domain benefits greatly from advanced technology and ubiquitous connectivity. From “smart” sensors to “augmented reality”, the opportunities to save costs and improve safety are endless. The aim of this dissertation is to study the capabilities of smart ship systems in the context of Internet-of-Things and analyse the potential cybersecurity risks and challenges that smart technologies may introduce into this accelerating digital economy.

The first part of this work investigates the architecture of a “Smart Ship System” and the primary subsystems, including the integrated bridge, navigation and communication systems, networking, operational systems, and sensor networks. The mapping of the connected subsystems is fundamental to understand how the entire vessel can be protected in a cyber context. The Internet of Ships is formed by connecting the smart ship systems with maritime infrastructure. The major services that the “Internet of Ships” can provide are discussed and analysed, such as terrestrial services, ship-to-shore services, marine safety and navigation services, offshore services and satellite services. These services facilitate many layers of supply-chain functions and interactions that are instrumental to the success of the maritime industry.

The second part builds on the gained understanding of the issues emerging from the digital transformation of seafaring. It introduces cybersecurity concepts and how these apply to the maritime domain. Then it outlines the threat sea-scape and gives guidance for a solid security program. A “Defence-in-Depth” cyber security resilience approach is proposed to protect the smart ship systems and the Internet-of-Ships with multi-layer measures, including security policies and procedures, physical security, perimeter security, network and host security, application security and data security. The most susceptible elements of the maritime sector are people – as target and as tools – for an attack. An improved appreciation of complexity of connected maritime systems along with a heightened cybersecurity awareness can prevent catastrophic incidents and protect lives and assets.

In summary, this dissertation gives a comprehensive overview of the shipborne subsystems of a Smart Ship System and the major maritime services it can provide in the context of the Internet-of-Ships ecosystem. The underlying cyber security issues and challenges are analyzed and a resilience building approach is discussed to protect the smart ships with multiple layers of security measures.

Contents

1. Introduction	1
1.1. Literature Review	1
1.2. Research Methodologies.....	10
1.3. Structure of the Thesis	12
2. Smart Ship Systems.....	13
2.1. Integrated Bridge	13
2.2. Navigation	18
2.3. Communication	25
2.4. Control.....	28
2.5. Summary.....	34
3. Internet of Ships	35
3.1. Terrestrial Services	36
3.2. Ship-to-Shore Services	38
3.3. Marine Navigation and Safety Services.....	40
3.4. Offshore Services.....	44
3.5. Satellite Services.....	47
3.6. Summary.....	48
4. Maritime Cybersecurity.....	49
4.1. Economic Opportunities	49
4.2. Cyber Risk	50
4.3. CIA	53
4.4. Challenges	54
4.5. Threat Actors, Targets and Motivation.....	59
4.6. Vulnerabilities	60
4.7. Building Resilience.....	62
4.8. Summary.....	68
5. Conclusion.....	70
References	72

List of Figures

Figure 1	IT and OT environments overlap.....	9
Figure 1	Intersection of Data, System, and Human	12
Figure 3:	Overview of Smart Ship Systems and primary subsystems for Navigation, Communication, and Control.....	14
Figure 4:	Simplified Smart Bridge network.....	16
Figure 5	VDR Furuno VR-3000 System configuration	17
Figure 6	VSAT Overview: VSAT enable critical systems on board and can process signals and data from multiple GNSS at various altitudes	18
Figure 7	VSAT system blocks	20
Figure 8	Shodan ship-tracker	21
Figure 9	Public, un-secured GPS interface	21
Figure 10	ECDIS integration with other Smart Ship subsystems	22
Figure 11	Air-gapped network.....	31
Figure 12	Integrated network.....	31
Figure 13	Shodan search for open Modbus devices (Port 502) in Perth, WA	33
Figure 14	User manual excerpt of Modbus solar meter showing default password	33
Figure 15	Potential security threats to navigation, communication, and control systems	34
Figure 16	Overview of five connected maritime service nodes of the Internet of Ships	35
Figure 17	AIS overview.....	41
Figure 18	Sample AIS route forecast.....	42
Figure 19	Sample AIS vessel details.....	42
Figure 20	Autonomous shipping milestones.....	49
Figure 21	The 5 top-rated challenges for Smart Ships.....	50
Figure 22	IT vs OT people	57
Figure 23	Critical and Non-Critical Infrastructure on board.....	60
Figure 24	“Defence-in-depth” layers of security measures.....	64

List of Tables

Table 1	Summary of publications.....	3
Table 2	Fundamental differences between IT and OT environments.....	7
Table 3	The Range of Research Approaches.....	11
Table 4	Key applications for maritime VSATs.....	19
Table 5	Communication modes connect corporate IT and OT:.....	26
Table 6	SATCOM equipment vulnerabilities and potential attacks.....	27
Table 7	Differences between IT and OT attributes.....	30
Table 8	Common ICS protocols and security features.....	32
Table 9	Maritime Satellite bands and usage.....	47
Table 10	Information asset inventory sample.....	51
Table 11	Sample risk assessment worksheet.....	52
Table 12	CIA threats to PNT information systems.....	54
Table 13	Systemic, human, and technological challenges.....	54
Table 14	Vulnerable systems on board.....	61

List of Acronyms

Acronym	Definition
ACU	Antenna Control Unit
ADU	Above Deck Unit
BUC	Block Up Converter Transmitter module to amplify signal and convert local IF to RF.
CORS	Continuously Operating Reference Station Terrestrial network of GNSS-supporting reference stations, available to on- and near-shore operations.
DGPS	Differential Global Positioning System
DVB	Digital Video Broadcasting (digital television standard)
GNSS	Global Navigation Satellite Systems Collective term for satellite constellations with the primary purpose of providing location and timing data for ground-based navigation. GNSS include GPS, GLONASS, BeiDou, and Galileo.
GPS	Global Positioning System Satellite navigation system developed and maintained by the United States Department of Defense.
IF	Intermediate Frequency
IOS	Internet of Ships
LAN	Local Area Network
LNA	Low-noise amplifier Signal-boosting module, often integrated in LNB
LNB	Low-noise amplifier and block down-converter Boosts weak incoming signals while cancelling out noise, converts high-frequency radio waves (RF) into lower frequency (IF) waves for demodulation and conversion to raw data.
LO	Local Oscillator Down-samples radio frequency to intermediate frequency used by BUC and LNB
OMT	Orthomode Transducer Linear waveguide used to separate incoming and outgoing frequency polarization by 90 degrees (orthogonal)
OPENAMIP	Open Antenna Modem Interface Protocol

Acronym	Definition
	IP based protocol developed by iDirect to facilitate the exchange of information between an ACU and the satellite router. Open-source protocol used to command the antenna. Since 2006 adopted as industry-wide standard.
PNT	Position, Navigation, Time
	Set of capabilities required to facilitate a myriad of time and/or location dependent applications, derived from the Navigation Message broadcast by GNSS.
RF	Radio Frequency
SHF	Super-High Frequency 3-30GHz; Wi-Fi, Satellite communications
SSS	Smart Ship Systems
TCP/IP	Transfer Control Protocol/Internet Protocol Suite of protocols and standards to facilitate data transfer and communication among internal or external network nodes.
UHF	Ultra-High Frequency band 0.3-3 GHz; UHF Television, mobile phones,
VHF	Very-High Frequency band 0.03-0.3 GHz; VHF Television, FM radio
VSAT	Very Small Aperture Terminal

1. Introduction

The maritime sector is a vital subset of critical infrastructure and accounts for more than 90% of cargo transported globally (National Institute of Standards and Technology, 2017). While remote-controlled and self-steering ships are already on the horizon, “smart” enhancements can be added to an existing vessel at any stage of its lifecycle. Smart sensors, robotics, augmented reality, big data analytics, and machine learning are only a few of the topics that receive great attention from the maritime media and technology vendors. These are advertised as ultimate solutions for cost-reduction, machinery control, crew welfare, and compliance in a highly regulated and competitive market.

Shipping companies understand the competitive advantage of these solutions and have only one choice – to participate in the process of digital transformation. Old and new technologies, and the mix of both, introduce a wealth of new cybersecurity challenges and increase the financial and logistical onus for the secure implementation and adequate crew training of smart technology. (Cimpean et al., 2011; SAFETY4SEA, 2017)

This research is fundamentally motivated by the maritime sector’s dependence on digital systems and the security and safety of its stakeholders. The aim of this thesis is to provide a nuanced overview of the of the technologies that both enable and endanger digitised ships and the digital network of maritime stakeholders.

The transformation of the industry is comparable to the aviation industry or critical utility infrastructure, where cyber-physical (operational) technology merges with information and smart devices. The adoption of smart and mixed environments has implications on every level of the organisation, and the human factor is central to the success and the security of this process. Added connectivity within internal and external networks opens up countless systems to a greater audience of potential cybercriminals and leaves many businesses at risk.

1.1. Literature Review

The following section outlines the concepts that serve as background and motivation for this work.

1.1.1. IoS and SSS

The Internet of Ships (IoS) and Smart Ship Systems (SSS) are the two essential concepts emerging from the digitisation of vessels by integration of old and new technologies for better performance and compliance. However, the increasing demands for efficiency and connectivity force maritime stakeholders to deploy new technology that is poorly understood and implemented.

The benefit of mapping out subsystems on connected ship systems is that operational management can understand where the areas of concern are, and how to prioritise and justify the allocation of resources to these areas. The benefit of viewing the IoS as the ecosystem of the maritime cyber-

world is that larger and systemic supply-chain risks can be identified and treated in line with the organisation's overall risk strategy.

Due to the rapid advancement in computing technology, especially the “Internet of Things” or IoT, any and all industries move towards digitisation and the use of “smart” innovations. In the media, the concept of Smart Ships is mainly associated with self-steering vessels, but autonomous navigation is only one aspect of smart shipping. Current ships have a life expectancy of over 20 years and will not be completely replaced in the short term. Instead, new sensors and devices are integrated with existing infrastructure to augment existing processes and provide visibility through data collection.

The information and documentation of Smart Ship Systems is based on resources from shipbuilding and manufacturing companies, finance & insurance groups, and the critical infrastructure, but also from researchers in the private, military, and education sectors. The literature agrees that maritime users can benefit from digitisation, but understanding and protecting from threats

The second main concept is the IoS – a virtual ecosystem that connects all maritime cyber services. Existing work confined the term “Internet of Ships” to the integration of IoT devices into ship design and shipbuilding ((G. Liu, Perez, Muñoz, & Regueira, 2016; The Royal Institution of Naval Architects, 2017)) and the provision of a unified infrastructure for ship data analytics (“Internet of Ships Open Platform”, IoS-OP, (Ikeda, 2017)). Wu et al. have provided some foundational insight and a layer-based approach to describe the transmission of data across heterogeneous and dynamic networks and the associated security challenges for wireless IoS architectures (Wu, Sun, Wu, & Miao, 2016).

While the concept of IoS has been used previously, it is sensible to use the term to describe the digital maritime ecosystem (akin to “Smart Cities”, the “Internet of Vehicles”, and the “Industrial Internet of Things”) that extends into each of the five major services nodes explained in Section 3.

1.1.2. Legal frameworks and publications

Technologies and threats evolve constantly; this means that law and policymakers need to respond quickly and appropriately to provide rules and assistance for the maritime community. The main contributors are authorities such as the Baltic and International Maritime Council (BIMCO), the International Maritime Organization (IMO), the American Bureau of Shipping (ABS), and the National Institute of Standards and Technology (NIST). Table 1 summarises recent frameworks, guidelines, and standards publications aimed to help maritime stakeholders to understand the risks and to ensure the cyber-safe operation of their assets and infrastructure.

Table 1 Summary of publications

Publication title	Organisation/Reference	Purpose
Framework for Improving Critical Infrastructure Cybersecurity	National Institute of Standards and Technology (2014)	Set of technology neutral standards and best practices to complement an organisation's risk management process.
Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1	National Institute of Standards and Technology (2017)	Draft update refines, clarifies, enhances predecessor
The Guidelines on Cyber Security Onboard Ships	(Baltic and International Maritime Council, 2017)	References, guidance, and examples for risk assessment and mitigation tailored to the maritime sector. Aligned with high-level guidelines from NIST and IMO.
ABS CyberSafety Volume 1 The Application of Cybersecurity Principles to Marine and Offshore Operations	American Bureau of Shipping (2016a)	Summary and introduction to Volume 2.
ABS CyberSafety Volume 2 Cybersecurity Implementation for the Marine and Offshore Industry	American Bureau of Shipping (2016b)	Specific guidelines focused on capabilities, risks, practices, and resources to achieve measurable levels of resilient cybersecurity. "ABS CyberSafety™" Certification requirements, process and capability matrix.
Measures to enhance Maritime Security: Report of the Working Group MSC 96/WP.9	Marine Safety Committee Working Group, International Maritime Organization (2016)	Marine Safety Committee Working group guidance on development of national maritime security legislation
Understanding Cyber Risk: Best Practices for Canada's Maritime Sector	(Transport Canada, 2016)	Overview of maritime cyber threat environment. Categorises cyber systems and maps relationships between all stakeholders. Highlights reporting requirements and responsibilities. Best Practice advice to prevent potential vulnerabilities.
Navigation and Vessel Inspection Circular (NVIC) 05-17;	United States Coast Guard (2017)	Draft guidelines for addressing cyber risks at Maritime Transportation Security Act (MTSA) regulated facilities.
Supply chain risk management practices for federal information systems and organizations	Boyens, Paulsen, Moorthy, Bartol, and Shankles (2014)	NIST Special Publication 800-161

Publication title	Organisation/Reference	Purpose
Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequence	US Department of Homeland Security; Moteff (2005)	Generic models and terminology to enhance common understanding of the risk assessment and reduction activity priorities.
Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach	U.S. Department of Homeland Security (2013)	Risk management guidelines for facility owners, operators and US Federal agencies tailored to Critical Infrastructure sector.

1.1.3. PNT – Position, Navigation, Timing

A critical component of modern navigation at sea is Position, Navigation and Timing (PNT), which refers to the set of spatial and temporal information which is broadcast by satellite systems and used by various systems on board. PNT sources include Global Navigation Satellite Systems (GNSS), mobile telecommunications networks, Continuously Operating Reference Stations (CORS), as well as other land-based differential Global Positioning Systems (GPS) and inertial sensors, chip scale atomic clocks, and pseudolites (Welles & Nichols, 2017).

PNT is essential for domain-awareness and navigational systems on board a vessel – it enables a wide range of maritime services, including safety and distress systems (GMDSS), fleet management, vessel traffic services (VTS) and port operations, asset and cargo tracking, industrial automation, information system synchronisation, and security access control (Hudson Analytix Inc, 2017). On board, networks rely on precisely timed interactions between servers, clients, controllers, sensors, and actuators which are integrated with control and management systems, navigation and communication subsystems, as well as information and industrial control networks (Australian Government Space Coordination Committee, 2018; Dinning, 2014; UK Government Office for Science, 2018).

Major risks emerge when the vessel is out of range of reference sources and GNSS navigation messages become the single source of truth (Zachhuber et al., 2013). The blind trust in the accuracy of electronic positioning systems means that falsified coordinates may not be detected. Spoofed data in the system can display incorrect positioning on the electronic chart display (ECDIS) and inadvertently get the ship to broadcast its own position incorrectly (AIS) and subsequently interfere with vessel traffic or other port navigation services (Jovanovic, Botteron, & Fariné, 2014; Silverstein, 2016; Soloviev & Venable, 2009).

PNT is essential to the modern data-driven economy, which is why the Australian Government recognised the protection of PNT as one of the country’s core interests (Australian Government Space Coordination Committee, 2018) (AGSCC, 2018). The benefits of PNT for Australian agriculture, mining, and construction alone have been estimated to be between \$800 million and \$1.5 billion per annum (Geoscience Australia, 2016).

The ubiquity of PNT provides the means for improvements and innovation in private, public, military, and scientific communities (Choy, Kuckartz, & Dempster, 2016; European GNSS

Agency, 2016). Businesses aim to save resources with intelligent fleet tracking, route optimisation, remote monitoring, sensor feedback, spare part management, and early warning systems (Acil Allen Consulting, 2017). It follows that a PNT-blackout can have catastrophic consequences and studies show that it would cost the UK alone more than 5 billion GBP over a five-day period without PNT. The maritime sector would account for more than 20% (GBP 1.1bn) of these losses (London Economics, 2017).

IoS and SSS environments rely heavily on uninterrupted flow of PNT while becoming increasingly interconnected and co-dependent. Permanent links between IT and OT networks expose a great attack surface. The compromise of any connected system, program, or user, has the potential to impact operations on a much greater scale than ever before.

Attacks can be planned in detail from public information and once a foothold is established, can take many different pathways through the connected network. Not only is there more exposed outdated software on legacy systems, but there is also a wealth of information on their flaws available on the internet Hery and Karri (2010). Previous attacks on maritime stakeholders have highlighted that these campaigns were carried out over months of intense reconnaissance, planning, and development.

GNSS – Global Navigation Satellite Systems

Global Navigation Satellite Systems (GNSS) broadcast PNT across most parts of the globe. GNSS currently comprise the United States Global Positioning System (GPS) and the Russian Global Navigation Satellite System (GLONASS). The Chinese “BeiDou” and the European “Galileo” constellations of navigation satellites are both expected to reach full global operational capability by 2020. India’s IRNSS and Japan’s QZSS are restricted to coverage of regional areas (European GNSS Agency, 2016).

The US GPS is the most readily available GNSS around the world for public and military use. GPS was developed in the 1970s to provide satellite-based navigation for the U.S. Department of Defense (DoD). The satellite system reached full, uninterrupted global coverage in 1995, when all 24 GPS satellites began to orbit earth. A lower-precision version of the GPS service was made accessible to civilian use in the early 2000s (Easton, 2013). Since its inception, the technology has enabled countless applications across many industries and sectors, including critical infrastructure, transportation, agriculture, construction, and airspace (El-Rabbany, 2002).

Navigation message

PNT’s useable information form is contained in the Navigation Message Each navigation satellite broadcasts Navigation Messages in regular intervals. The message is transmitted in five 300-bit subframes and carried over different frequency bands, e.g. In the case of public GPS, 1575.42 MHz (L1 C/A) (Kaplan & Hegarty, 2006).

Navigation messages include the satellite’s current coordinates and the timestamp based on the atomic clocks on board the satellite. This information is needed to compute precise satellite locations to derive receiver’s position on the ground. A receiver on Earth needs four satellites in range to calculate its own location. The receiver’s trajectory and velocity are calculated based on signal travel time and Doppler shift. Known error sources and biases (e.g. receiver bias) can be

corrected with alternative reference sources (e.g. Differential/DGPS, CORS, eLoran) when the receiver is within range of these terrestrial transmitters (Hale, 2007; John A. Volpe National Transportation Systems Center, 2001).

Disruption

The delivery of PNT via GNSS signals can be disrupted in different ways (Pace & Camacho, 2015). Attacks are generally based on signal interference (range-level attacks) or data/measurement spoofing (data-level attacks – (Caparra et al., 2016; Skey, 2017).

Bhatti and Humphreys (2017) conducted research for The University of Texas and emphasised the misplaced trust of integrated bridge systems in the integrity of GNSS signals. The authors presented a spoofing detection framework which is integrated into the ECDIS software. It uses Doppler logs and gyrocompass data to verify GPS measurements and detect malicious, “Hazardously Misleading Information”. However, the authors concluded that this sensor-driven detector may not be able to detect subtle masquerading and data spoofing before the hazardous condition occurs. Other research into PNT-assurance has evaluated GNSS orbit- and clock error-corrections mechanisms and showed that multi-GNSS receivers provide additional value (Li et al., 2015) but noted differences in correction accuracies and connection times between different GNSS systems (GPS, GLONASS, Galileo; (L. Wang et al., 2018). (Torre & Caporali, 2015) also provided evidence that multi-GNSS receivers introduce inter-system biases for specific

Signal Jamming

The electromagnetic spectrum is tightly occupied and regulated but new technologies demand ever more space to transmit wirelessly (International Civil Aviation Organization, 2011). Jammers are devices intended to impair the capability to receive and/or relay PNT data by generating Electromagnetic Interference (EMI). The ownership of jamming devices is restricted by local and federal laws and operating a jammer is prohibited (e.g. U.S. FCC - (International Civil Aviation Organization, 2011; Pace & Camacho, 2015)). Authorities tested the effect of commercially available GPS Jamming devices with a range of 3-400 meters. When a ship entered the jamming zone, multiple critical services were disrupted, e.g., Differential GPS (DGPS) receivers, AIS transponders and the DSC system (digital selective calling). These are of crucial importance for navigation, collision avoidance, and search and rescue operations (CyberKeel, 2015).

Interference, or jamming attacks can be widespread or directed, depending on the power level of the jamming device. The satellite signal is weak, and it only requires a slightly higher level of noise to prevent the receiver from displaying data correctly.

Spoofing

Spoofing occurs when an attacker impersonates a trusted information source. A transmitter matching the GNSS signal-structure overpowers the real GNSS signals which are weak due to the distance travelled from satellite to earth (Dobryakova, Lemieszewski, & Ochinnikov, 2014). The objective is to manipulate the receiver’s timing and navigation output to mislead the victim and threaten its safe journey. Spoofing transmitters such as Software-Defined Radios (digital signal processor, (RTL-SDR, 2018)) can interfere with receivers in a few hundred meters’ distance. Recent reports even suggest large-scale spoofing experiments have already been conducted by a

nation-state actor. More than 20 vessels in the Black Sea reported anomalies and false GPS readings, making them appear to be 25 nautical miles in-land (Jones, 2017).

Spoofing attacks are possible because satellite signals are sent in plaintext and require no authentication to read. Therefore, messages can easily be captured, manipulated, and replayed as crafted Navigation Messages on the GPS frequency. Without any safeguards, the GPS receiver will not query the integrity of the message and provide it to all trusting subsystems.

Spoofing attacks become more likely as we move faster towards augmented and autonomous navigation while relying on GNSS protocols that have no way to assure confidentiality, integrity, and availability of the transmitted data.

1.1.4. IT/OT Convergence

Information Technology (IT) and Operational Technology (OT) are two traditionally separate concepts. IT refers to the management of administrative operations, in contrast to OT which manages industrial operations. The OT environment describes interconnected sensors and controls under centralised management to orchestrate individual processes. The term "IT/OT Convergence" is used to describe the merging, overlap, and co-dependence of both concepts.

Figure 1 illustrates the overlap of these two environments. IT and OT teams must work together to facilitate resourcing, scheduling, and operation management and provide intelligence and reporting for the organisation. While there is *some* technological overlap, the network protocols used in OT are largely different to the protocols used in IT. Table 2 summarises the major differences between IT and OT environments to highlight the two traditionally separate mindsets.

The issues of integrating IT and OT systems into SSS create a vast new attack surface, which will be explored in Sections 2 and 3.

Table 2 Fundamental differences between IT and OT environments

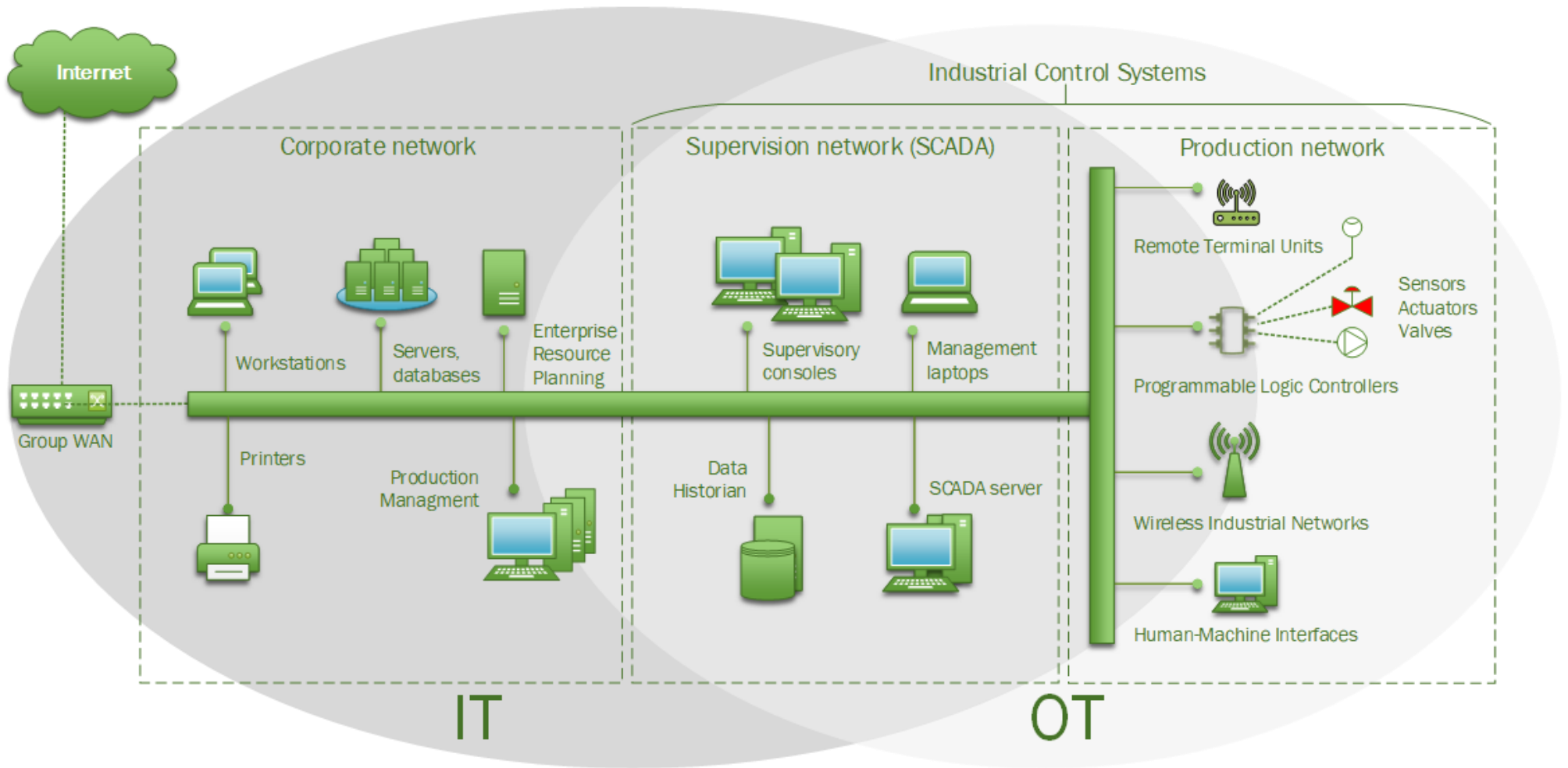
	IT	OT
Definition	<i>"Application of computer systems to store, retrieve, transmit and manipulate data in the context of businesses"¹</i>	<i>"Application of hardware and software detecting or causing changes in physical processes through direct monitoring and or control of physical devices."²</i>
Purpose	Store, process, and transfer information	Control and monitor processes and assets
Environment	Dynamic; based on query and response	Deterministic and predictable; based on control and work-flow
	Information-only environment	Cyber-physical environment
	Delays acceptable	Timing critical
	Standard architectures and methodologies	Legacy systems, purpose-built customisations
	Commercial off the shelf (COTS)	Real-time operating systems, embedded firmware
	Component lifetime 3-5 years	Component lifetime 10-30+ years

¹ Daintith, John, ed. (2009), "IT", A Dictionary of Physics, Oxford University Press

² <https://www.gartner.com/it-glossary/operational-technology-ot/>

	IT	OT
	Built around fault tolerance, interoperability, and ubiquitous connectivity	Built around control, automation, and longevity
	Incorporates dynamic addressing, routing, and recovery into protocols.	Designed for local access only, little ability to incorporate other aspects, such as security
	Large number of hosts and gateways	Limited number of gateways
	High bandwidth and throughput demands	Modest throughput acceptable
People	Computer and networking background	Engineering or purely technical background
	Strong knowledge of business systems and technology	Strong knowledge of plant and processes
	Used to working with routers, switches, firewalls, and domain controllers, as well as troubleshooting web, email, and business applications.	Trained to operate ICS components such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTU's), Human-Machine Interfaces (HMIs). Intimate knowledge of legacy systems and ICS protocols (e.g. Modbus, DNP3, etc.).
	Lack of understanding of processes	Lack of IT experience and working with IT
Priorities	<p>“Data is King”</p> <p>Maintaining confidential access to approved users, ensuring that the data is accurate and reliable, and it is accessible when needed.</p> <p>Based on the CIA model, the order of priorities is:</p> <ul style="list-style-type: none"> • Confidentiality • Integrity • Availability 	<p>“Process is King”</p> <p>Maintaining control of processes, preventing disruptions of OT systems, which can lead to the loss lives, equipment and ecological damage.</p> <p>The order of priorities is:</p> <ul style="list-style-type: none"> • Control • Availability • Integrity • Confidentiality.

Sources: Adapted from Gregory-Brown and Harp (2016), Effendi (2015), Sistrunk (2016)



Source: Adapted from (Williamson, 2015),(Soullie, 2014b)

Figure 1 IT and OT environments overlap

1.1.5. Maritime Cybersecurity

The field of maritime cybersecurity owes much of its increasing significance to the fact that satellite systems enable data-connectivity at the most remote location. Even with IT capabilities on shore, ships had no direct connection to a network that could potentially endanger the systems on board. Advances in technology along with the pressure to improve efficiency have forced the maritime industry to create those data connections, and with it the exposure to the world of cybercrime.

Many cybersecurity issues relate to network and human security, but most problematic is the integration of IT and OT systems on board and in ports (as indicated in Section 1.1.4). While these challenges and solutions are similar to terrestrial and aviation domains, the maritime domain has a unique reliance on satellite equipment for navigation, communication, and control.

Governments and organisations such as NIST³ and IMO⁴ work hard to provide regulatory frameworks and guides for the digital transformation of the maritime domain. These contributions were summarised in Section 1.1.2. Other publications on maritime cybersecurity are often motivated by technology vendors or providers of security systems. A major area of concern, research on satellite equipment has already revealed significant vulnerabilities as well as the industry's susceptibility to malicious interference and data spoofing.

1.2. Research Methodologies

1.2.1. Significance

The maritime domain has become alert to the risks emerging from the inevitable digital transformation. Surveys among shipping executives have shown that their top concerns are cybersecurity and crew training in new technologies (SAFETY4SEA, 2017). All maritime users, such as port authorities, logistics companies and coast guards, are exposed to the same threat environment, but not many can afford additional resources for an entire security program. Especially commercial users face the conundrum that new technology benefits efficiency and returns, but requires large upfront investments to acquire, implement, and secure these systems.

This work aims to contribute to maritime cybersecurity with a common understanding of complexities and intricacies of multiple technological ecosystems and their dependence on each other. It provides perspectives which are necessary to grasp both, the large threat environment, and the vulnerabilities of individual technologies and processes.

The perspective of “Smart Ship Systems” focusses on the ship and the main cybersecurity issues that relate to the integration of systems and its ability to safely navigate the waters, to maintain communication, and to ensure control over the engine and steering (“Navigation-Communication-

³ National Institute for Standards and Technology

⁴ International Maritime Organization

Control"). SSS refer to technology enhancements on current vessels including Internet-of-Things (IoT) devices and sensors, processing systems for enormous amounts of data ("Big Data Analytics"), and the development of cyber-physical systems.

The concept of "Internet of Ships (IoS)" describes the maritime digital cyber infrastructure as a layer of interconnected service domains. The contribution of this thesis extends to five major domains of IoS and the challenges with the technologies and services supported by these domains.

1.2.2. Research Objectives

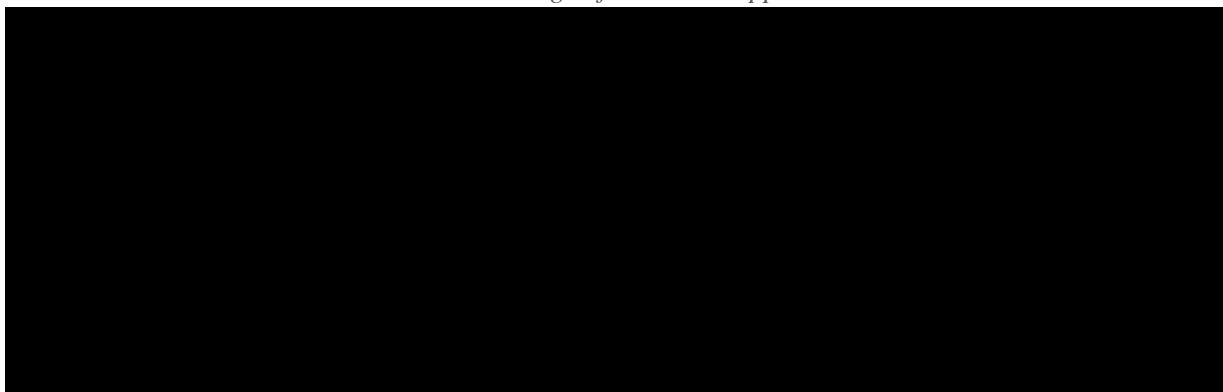
The following research objectives are addressed in this thesis:

- To study the complex maritime cyber-environment with a focus on connected service domains (Internet of Ships), as well as new and converging technologies on board (Smart Ship Systems)
- To understand the maritime threat-landscape and risks related to specific components of service domains and systems on board
- To contribute strategies to improve cyber-resilience on Smart Ship and throughout the Internet of Ships

1.2.3. Approach

Galliers, a pioneer in information systems research, viewed the objects of research interest on a spectrum between empirical (quantitative) research and purely interpretational (qualitative) research (Table 3). Our research objective, to understand challenges of maritime cybersecurity, can be approached in multiple ways, but a "Descriptive/Interpretive" approach has the best application when analysing and categorising a large amount of technologies and concepts. Epistemologically, this comprehensive review may combine Interpretivism with positivist elements.

Table 3 The Range of Research Approaches



Source: (Galliers, 1990)

1.2.4. Methodology

The primary research for this this thesis was conducted through a descriptive, literature-based analysis. Data sources include books, research papers, government reports, whitepapers and manuals, special publications, and electronic articles and presentations. The cited literature in this thesis was published between 1981 and 2019, with 84% (133 of 158) after the year 2010

Cybersecurity is a young field of research and while some topics can be highly scientific (e.g. cryptography, quantum physics), others may focus on code, engineering, psychology, or governance. Edgar and Manz (2017) describe “Cyber space” as the overlap of data, system(hardware), and human (social) – see Figure 2. While cybersecurity research areas emerge where these three areas intersect, there has not been any discovery of “first principles of cyber space”. Therefore, cybersecurity research evolves with the gained information and slowly creates knowledge to predict and future-proof cyber space/

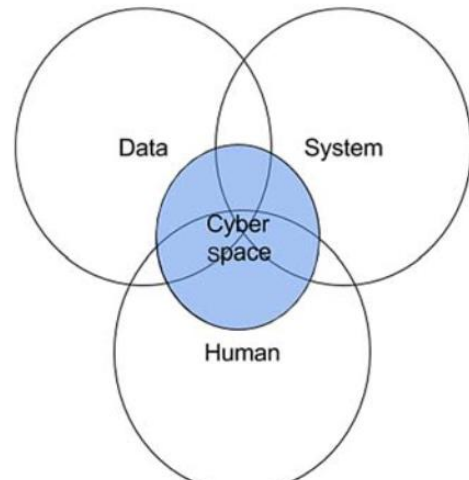


Figure 2
Intersection of Data, System, and Human

The literature-based research methodology results in a comprehensive review that interprets cybersecurity concerns in a maritime environment. Maritime cyber concepts are explained in the broad context of the digital shipping community and in the confined context of the connected vessel. The output is an improved understanding of the technologies and their underlying issues with recommended approaches to reducing the risks of interacting in the maritime cyber space.

1.3. Structure of the Thesis

The thesis is structured as follows:

Section 2 explores and categorises the technologies that make up a Smart Ship System. The outline of various technologies and protocols can provide the foundation for future improvements to the cybersecurity posture of the modern maritime industry.

Section 3 explains in detail the five major service nodes of the Internet of Ships and explains how critical maritime services are connected through a complex mesh of legacy infrastructure, current systems, and cutting-edge technologies.

Section 4 provides an comprehensive overview of risk, challenges, vulnerabilities, and threats to the maritime domain, before elaborating on different strategies to build organisations that are cyber-prepared.

Section 5 concludes this thesis and outlines the findings and the direction of future work in the maritime sector.

2. Smart Ship Systems

Being “smart” means to make the best decisions and predictions based on the available information and resources. In the context of Smart Ship Systems (SSS), smart improvements include any device with embedded wireless functions, advanced environmental sensors, increased processing capability, or machine learning algorithms. Any modern ship can be referred to as a “Smart Ship” if it takes advantage of digital technologies to improve performance and reduce human errors.

The following section is an investigation of the main smart ship systems and subsystems, including the integrated bridge, navigation and communication systems, IT networks, operational technology (OT) systems, and sensor networks. The overview of smart ship systems is visualised in Figure 3 and explained in the following sections.

2.1. Integrated Bridge

The “integrated” bridge is the brain of the smart ship. The bridge is the centre of command with access to data from a multitude of sensors and subsystems. Data is collected, analysed, and displayed for the captain and crew to make fast decisions and oversee the safe navigation of the vessel. In addition to local monitoring with SCADA (Supervisory Control and Data Acquisition), mechanical systems can also be controlled, monitored, and automated from the bridge. Sensors from these systems provide health information and real-time feedback.

The bridge also has oversight of:

- Power control system
- Propulsion and machinery management
- Cargo management
- Access control system
- Passenger servicing and management
- Passenger facing public networks
- Administrative systems
- Crew education and welfare systems
- Communication systems
- Core network infrastructure
- Security and HVAC systems

Smart ships are equipped to communicate on multiple frequencies and via different technologies to provide the best possible redundancy and coverage. Resilient communication channels are imperative to the safe and efficient operation of the vessel at sea. Satellite Communication systems (Satcoms) are transceivers used for voice and data communication and operate on a spectrum between 3 and 30GHz and more. These devices are integrated with the bridge and installed throughout the smart ship network.

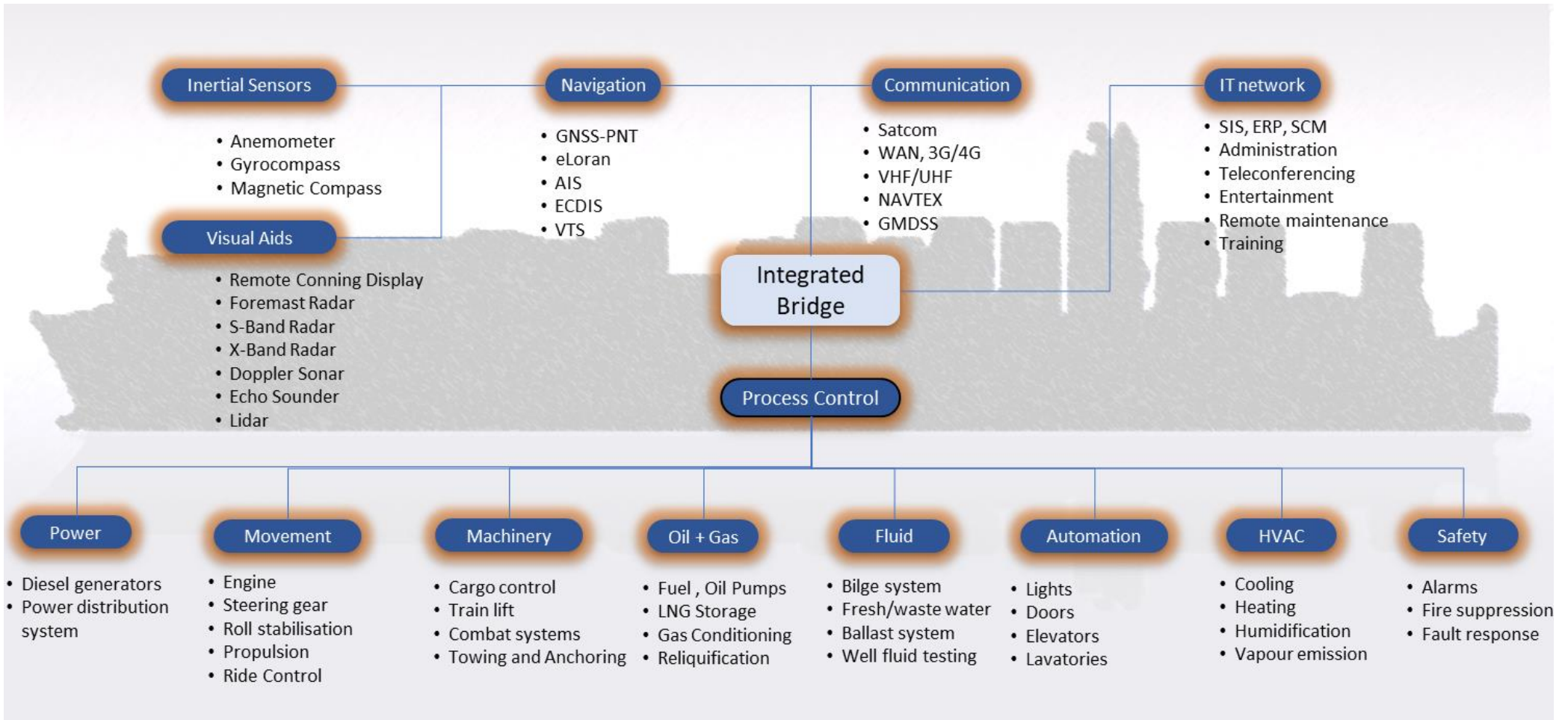


Figure 3: Overview of Smart Ship Systems and primary subsystems for Navigation, Communication, and Control

2.1.1. IT Systems

The bridge is tightly integrated with the IT infrastructure, which also enables core business and operation systems. The crew uses applications like Microsoft Office for daily administrative tasks and emails, as well as browsers for internet searches and downloads. Other software on board leverages shared databases and resources for accounting, cargo and passenger management, human resource planning and administration (Hudson Analytix Inc., 2017).

Figure 4 shows an example of an IT network architecture. The two main external data connections are satellite communication systems (e.g. VSAT) and GSM transceivers (e.g. 3G/4G) near terrestrial infrastructure. Incoming data goes through a firewall and is routed to the respective sub-networks (i.e. Virtual Local Area Networks, VLANs). Data on board is distributed via ethernet cables or wireless LAN access points (WLAN APs).

An IT network with several sub-networks, servers, and devices suffers from the same vulnerabilities as terrestrial networks. But in addition, seaborne IT systems are more exposed to physical threats and isolation, which makes frequent security updates and maintenance even more difficult and less of a priority. Unless computers and programs are always patched and updated, there is a genuine risk that users of non-critical systems to introduce malicious software that spreads across the network. For example, malicious code can be hidden in documents or spreadsheets and run when the user opens them from an email attachment (“macro virus”). The email-vector is also used for “phishing”, but instead of delivering a file or code to run, it relies on the user actively engaging to hand over data or control. Attackers either lure the victim into disclosing private information, or into downloading and executing malicious code which then allows unauthorised access to the computer or network. If workstations have administrative privileges enabled, malware infections can be caused when users install software from unsecure online sources.

The Ship Information System (SIS) is part of the IT network and the main reference for vessel engineers and operators. It contains data on the ship’s components, assets, and resources. The SIS is typically accessed for maintenance and troubleshooting purposes from the bridge, local workstations, portable devices, or remote internet connections. The SIS is synchronised with land-based management systems when the vessel is in range or manually via portable hard drives. Both methods of data transfer increase the risk of introducing malware, but it is more likely that an infected portable device is plugged into a workstation without appropriate antivirus-protection.

IT networks on board also provide the crew with access to video-telephony, entertainment, email, social networking, distance training, telemedicine and more. These services on board are not essential for the safe voyage but play an important role for the crew’s welfare and satisfaction. They allow staff to “switch off” after a shift and can indirectly and positively affect the motivation and mindfulness when on duty. Internet-based entertainment services are facilitated via Satcoms and Wi-Fi networks on the ship.

The crew-VLAN is not critical, and therefore less strictly secured and monitored. The VLAN may be logically detached from other network-segments, but softer control of this segment can give an attacker a foothold in the system. For example, an infected USB media device is connected to a personal laptop and that laptop is connected to the crew-VLAN. The malware runs from the infected USB and spreads to other locations, or it installs a backdoor or that allows remote code execution (RCE) so that the attacker can explore the network, learn credentials, find vulnerabilities, and prepare for other, more sophisticated attacks in the future. The use and security of personal devices and portable storage should be therefore be tightly managed on board.

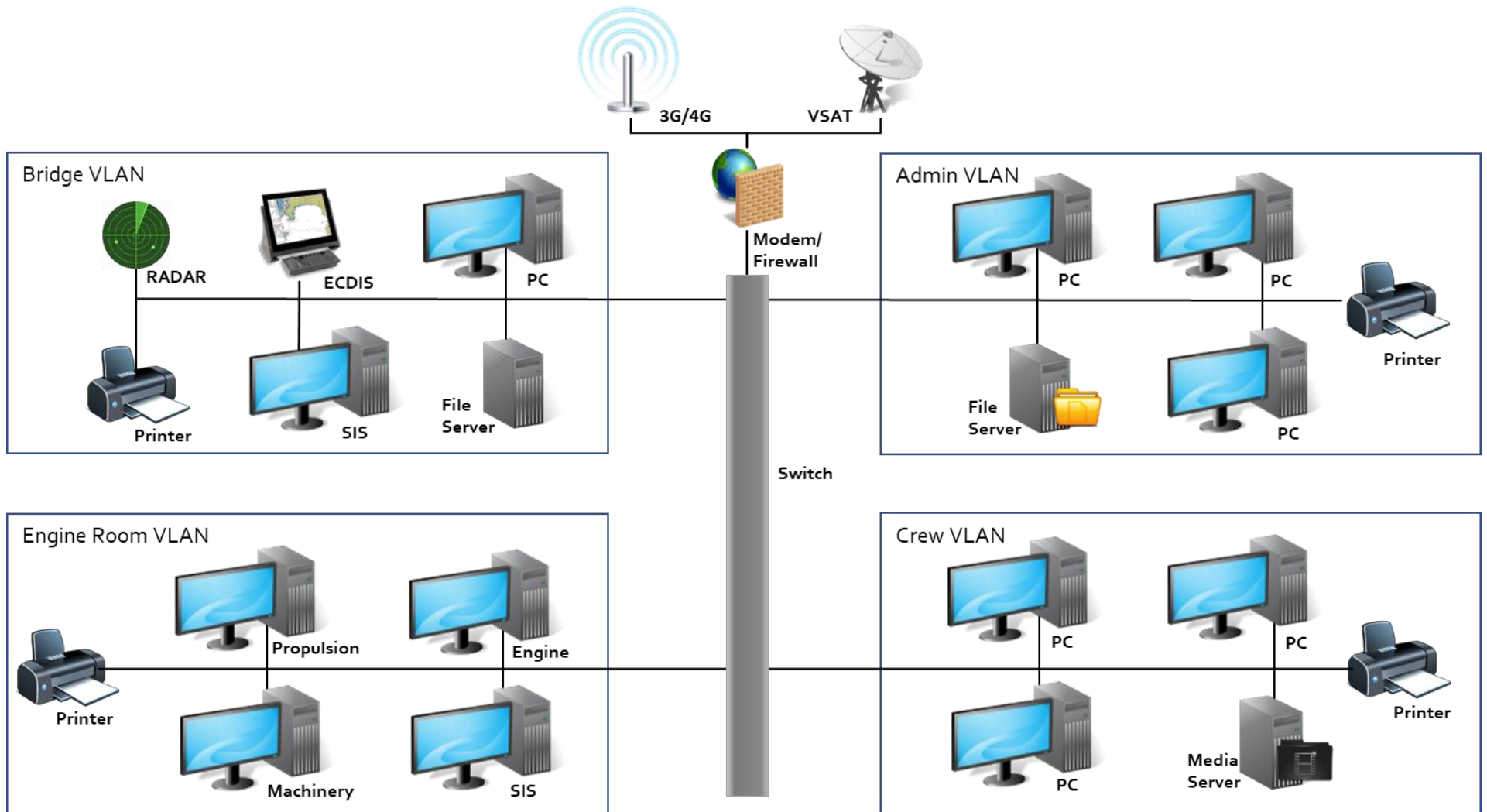


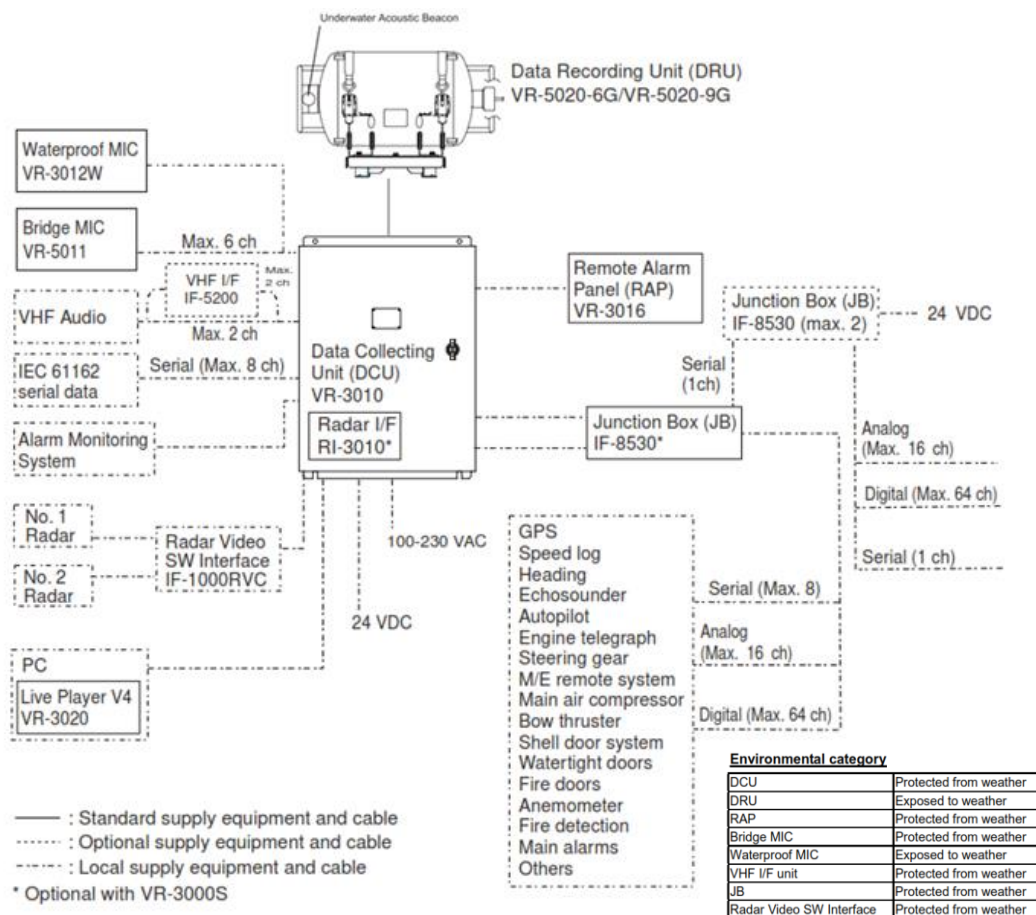
Figure 4: Simplified Smart Bridge network

2.1.2. VDR – Voyage Data Recorder

The Voyage Data Recorder (VDR) serves a central purpose on board as it automatically collects various data for the purpose of assisting investigators after a marine incident. The VDR is similar to an airplane’s black box as it records voice communications, location, sensor data, and other event logs from subsystems. VDRs are mandatory on all commercial vessels greater than 300 GRT and on all passenger ships (International Maritime Organization, 2009).

The VDR consists of a Data Recording Unit (DRU) and a Data Collecting Unit (DCU), a Remote Alarm Panel (RAP), and microphones to record bridge audio. The VDR datastore is sealed in a protected capsule and equipped with an acoustic beacon. Any physical tampering or manipulated data input can jeopardise the forensic integrity and impact on a potential incident investigation.

Figure 5 shows a schematic of the commercial VDR model Furuno VR-3000. It exemplifies the multitude of alarm systems and sensors that can be logged on board. Santamarta (2015) audited this product and determined a range of critical software vulnerabilities. He found several buffer overflow and code injection flaws, weaknesses in the firmware update mechanism, and insecure encryption protocols in use. Santamarta demonstrated that he could fully compromise the device, modify and delete all the data, and even spy on the crew through the microphones.



Source: (Furuno, 2006)

Figure 5 VDR Furuno VR-3000 System configuration

2.2. Navigation

The “Smart Captain” relies on a range of navigation subsystems to find optimal routes, avoid bad weather or steer away from dangers. Smart navigation technology on board can also facilitate data exchange (e.g. satellite communications, radios, telex receivers) and display information on various screens on the bridge (e.g. ECDIS) and other workstations on the vessel.

This section introduces the major components of the navigation subsystem: Very Small Aperture Terminal (VSAT), Electronic Chart Display Information System (ECDIS), and navigation aids.

IoS navigation services will be outlined in Section 3.3 below and include satellite services, Automated Identification System (AIS), Global Maritime Distress and Safety System (GMDSS), and electronic Aids to Navigation (eAtoN)s.

2.2.1. VSAT –Very Small Aperture Terminal

VSATs are enterprise- and consumer-level satellite communication stations for two-way voice, data, and video streaming and provide the ship with additional functionality via multi-frequency and multi-constellation satellite networks. These include navigation satellite systems, but also constellations for weather monitoring, earth observation, and communications.

VSAT technology was first developed for television signal reception in remote areas, but the development of TCP/IP satellite broadband technology make VSATs a useful investment that can augment numerous applications and systems on board. VSATs enable data communication in an extremely challenging and dynamic environment.

VSAT transmit narrowband data (e.g. PNT, remote control commands, payment terminal transactions) and broadband data (e.g. Voice-over-IP/VoIP). Figure 6 summarises the main subsystems on board a vessel that process data (e.g. PNT) from GNSS at orbit Earth at different altitudes (Low-Earth Orbit, Medium Earth Orbit, High Earth Orbit).

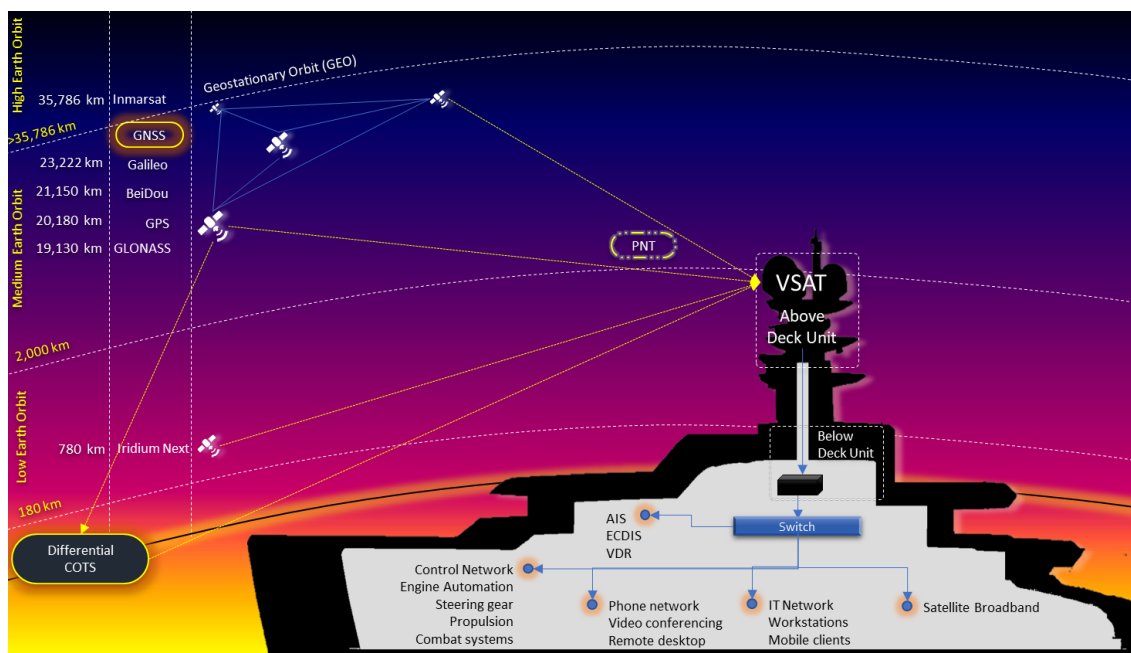


Figure 6 VSAT Overview: VSAT enable critical systems on board and can process signals and data from multiple GNSS at various altitudes

Market research by Comsys (2017) shows that the demand for stabilised VSAT services (maritime VSAT) will rise steeply in the coming decade. The adoption is greatly driven by operational efficiency and improved processes (Stark Moore Macmillan, 2011). VSATs are available for vessels of all sizes – from recreational yachts to Ultra-Large Container Vessels (ULCV). Currently more than 1.3 million vessels can theoretically carry VSAT, with the large-yacht sector comprising the greatest number of opportunities. About 71,000 owners are actual or near-term potential customers. Another prospective market is the commercial shipping sector, where currently 13,200 vessels are equipped with VSATs. This number is predicted to reach 33,000 by 2025 (Marlink, 2018).

Aside from the commercial incentives of running a VSAT, it enables services on board which are mandated by national and international rules aimed to protect the safety of people, assets, and the environment. For example, the International Civil Aviation Organisation (ICAO) mandates Satellite-Based Augmentation Systems (SBAS) for aircraft, while the International Maritime Organization (IMO) dictates the minimum required equipment, depending on the vessel size and purpose, e.g. navigation (AIS, ECDIS), search-and-rescue (GMDSS), and event monitoring and logging (VDR).

VSAT terminals operate on C-, Ku- and Ka bands to provide services like broadband internet, emergency services and alerts, remote cargo management, vessel routing, ECDIS, Radio over IP, telemedicine, crew welfare, tele-training, and many more (Santamarta, 2014c). Table 4 summarises the key applications for VSAT users across different sectors of the maritime domain.

Table 4 Key applications for maritime VSATs

Maritime Domain	Key Applications
Commercial shipping	<ul style="list-style-type: none"> • Voice communication • Crew welfare and training • Electronic charts and weather information • Ports and Customs reporting • Remote IT services • Inventory control • Remote process control, inventory, and telemetry
Fishing industry	<ul style="list-style-type: none"> • Online markets and auctions • Vessel monitoring • Regulatory reporting • Telemedicine
Oil and gas	<ul style="list-style-type: none"> • Crew welfare and training • System automation, cloud computing • Live monitoring and conferencing • Seismic data transmission
Cruise industry	<ul style="list-style-type: none"> • Entertainment and video streaming • Banking and point-of-sale transactions • Guest and reservation services • Onboard wireless services • High-speed Internet

Sources: (IDirect, 2016; Maral, 1995; Rogers, 1989; Stark Moore Macmillan, 2011)

A simplified VSAT system architecture is depicted in Figure 7. It illustrates the system blocks of Above-Deck-Unit (ADU), Antenna Control Unit (ACU), and attached IT/OT network segments. The ADU comprises an adjustable satellite dish and antenna modules, and the ACU includes modem, splitter and the control system for antenna movements (SATCOM, 2013). A direct control-interface between ADU and ACU is provided via an industry-standard protocol like Open Antenna-Modem Interface Protocol (OpenAMIP; (Lara, 2015).

Internet exposure

The VSAT aperture is vulnerable to physical sabotage on board, but it is possible to launch an attack through the satellite internet connection. If it has a public IP address and open ports, a ship's VSAT terminal can be located via Shodan's search engine and ship-tracker (Figure 8). The header information provided in Shodan search results typically shows manufacturer and/or model details. With this information, anyone can access user manuals and other specifications, including the factory-set username and password for the administrator. Thus, an attacker can gain unauthorised access if they can locate the ship on the Internet and the VSAT credentials have not been changed. An attacker with access to a VSAT can move it, switch it off, tamper with navigational settings, but also manipulate log entries and alter evidence for forensic reconstructions of incidents.

Research revealed that many connected VSAT devices are poorly configured (open ports, default credentials, flawed firmware), and attackers could easily access VoIP-call histories, modify system settings, and upload malicious firmware. Figure 9 shows a screenshot of the VSAT control panel, obtained by researchers over public internet and accessed with default credentials.

The modem's external interface enables the direct stream of data between the ACU and the vessel's IT router and switched through to distributed network nodes, including the bridge, enterprise- and control networks, and the workstations for electronic navigation. Any misconfiguration of network equipment widens the attack surface and opens opportunities for an attacker to pivot throughout the network and to critical control systems (Morse, 2017).

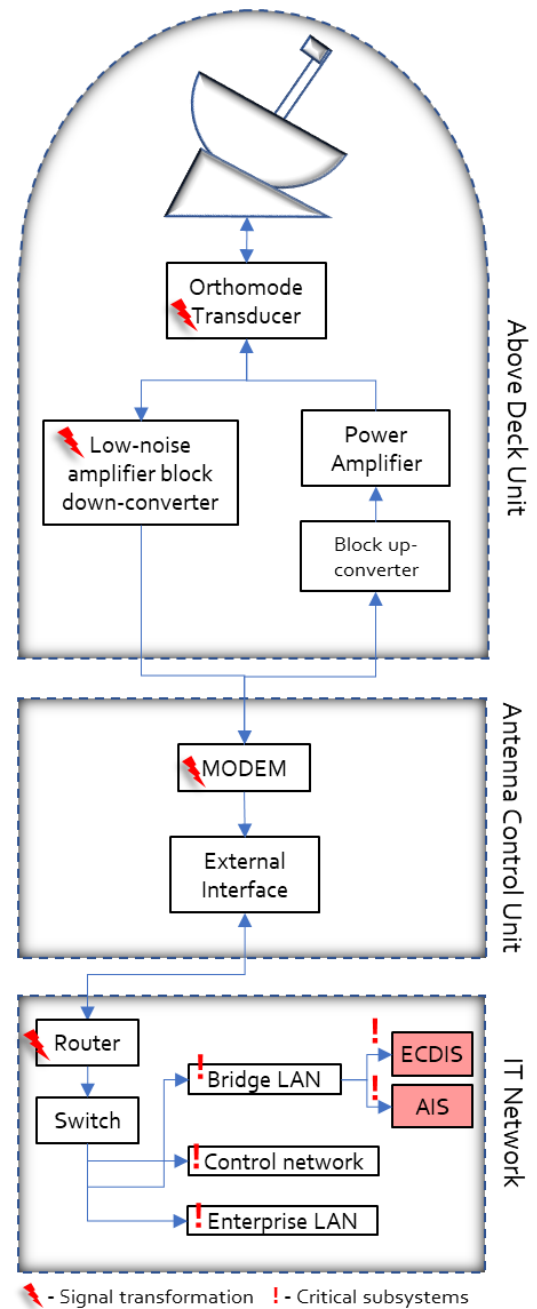
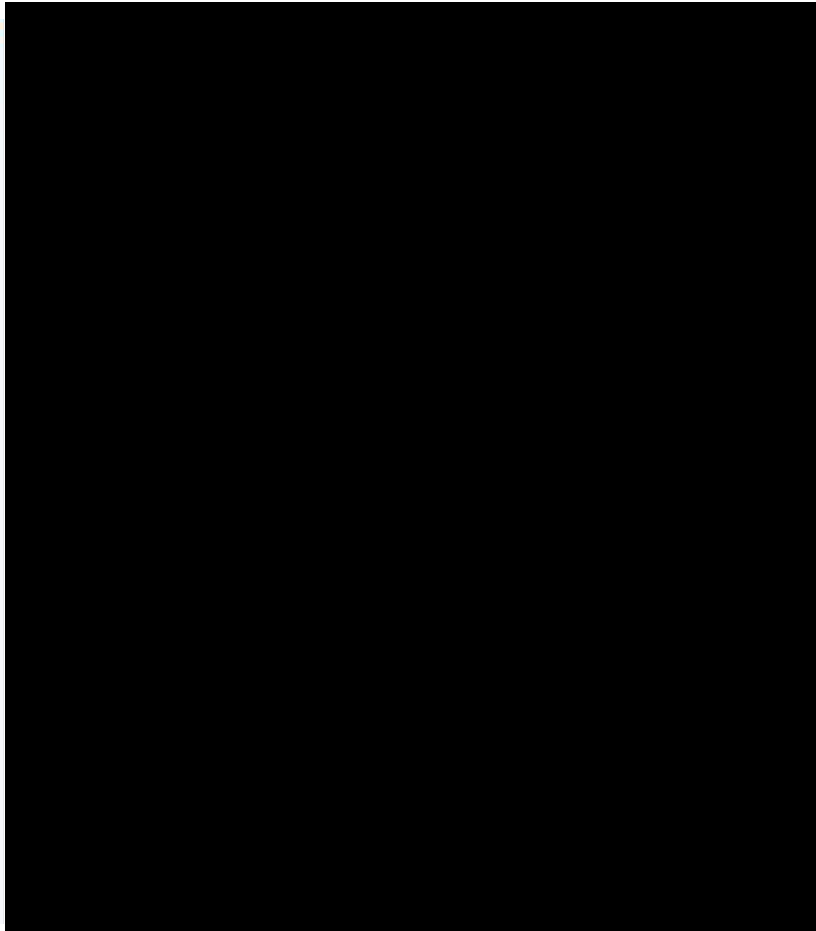


Figure 7 VSAT system blocks



Matherly (2017)

Figure 8 Shodan ship-tracker



x0rz (2017)

Figure 9 Public, un-secured GPS interface

Interference

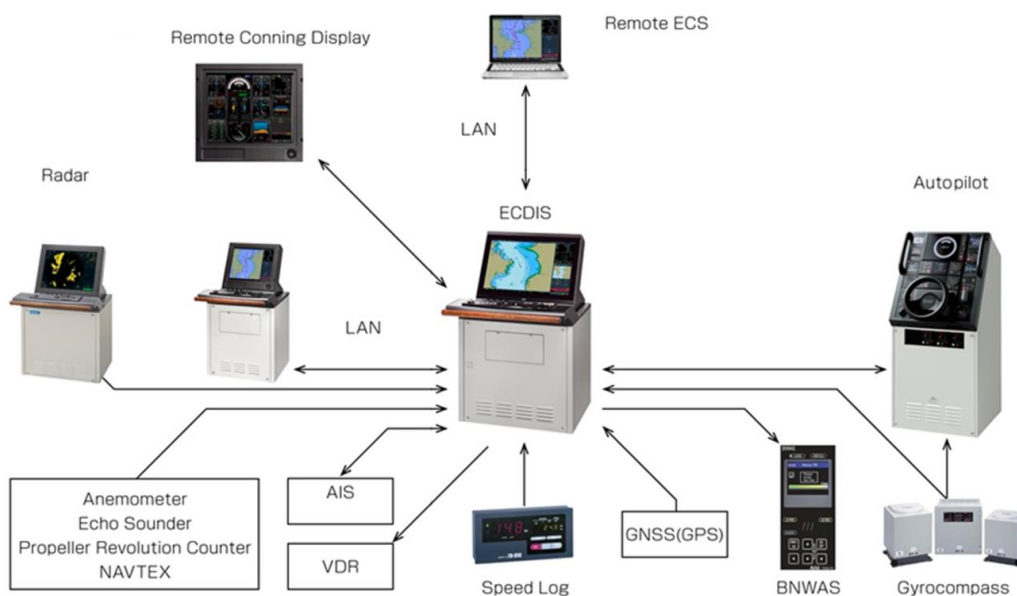
VSATs and other signal receiving equipment are exposed to signal- and data interference and degradation, which can lead to unreliable position calculations. Apart from atmospheric and cosmic effects, Electromagnetic Interference (EMI) also includes multi-path effects from signal reflection from structures, walls or the terrain (Acil Allen Consulting, 2017).

As indicated in Figure 7, multiple subsystems along the “receive feed” modulate or convert the signal before it is processed by applications. Each component produces noise that can interfere with the correct PNT processing and output sent to the sensors and applications. The Low-Noise Block-Converter (LNB) boosts the weak center frequency of the satellite signal while filtering out interferences and noise. The block down-converter module uses local oscillation to convert the raw radio frequency (RF) from the satellite to an intermediate frequency (IF) with a wavelength that can be processed by subsequent modules. The analogue IF signal travels to the ACU, where the modem converts it into raw digital data.

2.2.2. ECDIS – Electronic Chart Display Information System

The Electronic Chart Display Information System (ECDIS) is software that runs on workstations on the bridge of the vessel. Electronic maps (Electronic Navigational Charts – ENC) are intended to replace traditional paper chart navigation. ECDIS is now mandated by the IMO for all commercial vessels (International Maritime Organisation, 2017). Sensor feeds into the ECDIS system come from a multitude of other systems, including VSAT, RADAR, and AIS (see Figure 10). Disastrous navigational decisions can be expected when the sensor feeds or e-charts have been intercepted and tampered with.

Figure 10 ECDIS integration with other Smart Ship subsystems



Source: Adapted from Tokyo Keiki (2017)

ECDIS can be connected to the VSAT via the ship’s IT network. The VSAT data feed provides the vessel’s current PNT, which is displayed on the electronic navigational chart (ENC) on a

computer monitor. GNSS-broadcast PNT is available in almost any location, reliable, and most precise, while other systems such as RADAR and gyrocompass can augment ECDIS and provide additional assurance of PNT. ECDIS is a safety-critical application but the effects of unreliable PNT input and its interpretation by the software must be further scrutinised. Disastrous navigational decisions can be caused if other sensor feeds have been tampered with.

ECDIS implementations on board have a range of weaknesses. For example, ECDIS software often runs on legacy systems, such as Windows XP desktop computers. These systems no longer receive security updates from vendors and are thus exposed to many well-known exploits.

Researchers have audited commercial ECDIS software and highlighted further significant weaknesses and security risks. They proved that attackers could read, replace, and delete any data that was stored on the host computer (Dyryavy, 2014). The software ran an outdated local Apache web server, which was susceptible to directory traversal and denial-of-service attacks. The web server allowed the dangerous HTTP methods “PUT” and “DELETE”, which would give an attacker the opportunity to delete and replace files in the software. The software was also vulnerable to HTTP Header Injection, which allowed to post malicious content into the “host=” parameter.

The integrity of ECDIS electronic navigational charts (ENCs) can be protected via the S-63 Data Protection Scheme. S-63 is designed to prevent unauthorised copying of data, restrict organisations to only allow access to the purchased licensed material, and to authenticate the ENC source using a digital signature (National Oceanic and Atmospheric Administration, 2005).

S-63 was adopted as standard in 2002. It encrypts the basic transfer database with the Blowfish algorithm and includes SHA-1-hashing and CRC32 integrity checks (International Hydrographic Organization, 2012). Both Blowfish and SHA-1 are today considered insecure for cryptographic implementations.

The map material is loaded onto the system via the internet, or manually via USB drives. As explained in Section 2.1.1, this provides a vector for a compromise and can lead to unauthorised access to data on the connected network.

Some general recommendations to protect the integrity of ECDIS include:

- Choose software manufacturers who are verified to follow Security Development Lifecycles.
- Include ECDIS software in the ship network patch- and update management regime.
- Use Antivirus scanners and monitor the chart files when they are uploaded to the software.
- Limit the physical access to ECDIS and components to approved and trained personnel only.

2.2.3. AIS

Automated Identification System (AIS) transmitters broadcast the ship’s identification details (e.g. name, country of registry, tonnage), as well as their coordinates, via VHF radio or other means to surrounding receivers. This data is either displayed on integrated e-charts (e.g. ECDIS) or on separate RADAR-like screens.

AIS is part of the navigation subsystem of a smart ship and it tracks other ship's location to prevent collisions. To assure the integrity of the ship's own broadcast message, it must absolutely trust the location and timing data from the VSAT subsystems. Bhatti and Humphreys (2017) demonstrated that AIS systems can be simply deceived into displaying injected, fake GPS coordinates, which would force the captain to steer in the attacker's preferred direction.

AIS is explained in more detail as part of the IoS in Section 3.3.1.

2.2.4. Navigation aids

The navigation aids for augmentation and fail-over include AIS, VTS, ECDIS, and eLoran. Visual and inertial navigational aids on board complement information from other sensors and communication subsystems to ensure the safest possible voyage. Note that digital, or electronic Aids to Navigation (eAtons) are covered separately in Section 0. Navigation aids on board include the following:

- **Inertial Measurement Units (IMU):** IMUs are used for position and orientation estimation when GNSS is lost. IMU devices contain inertial sensors – a three-axis accelerometer and a three-axis gyroscope based on microelectromechanical system technology (MEMS). The accelerometer measures external specific force (acceleration and the earth's gravity). Gyroscopes sense angular velocity – the rate of change of orientation (Kok, Hol, & Schön, 2017).
- **Gyrocompass:** This is navigational instrument which uses a gyroscope to accurately display the true geographical north. A gyrocompass is based on the rotation of the earth, rather than its alignment with magnetic forces. Thus, the gyrocompass is not susceptible to magnetic interference on board (e.g. ferrous metal in the vessel's hull) (Bai & Bai, 2019).
- **Magnetic compass:** Magnetic compasses have aided mariners for centuries to ascertain the vessel's heading. The compass needle aligns with the line of magnetic force of the earth and points to the magnetic north pole.
- **Conning Display:** This visual display unit provides data essential for the precise and safe navigation in a clear and visible format capable of being read at some distance from the screen (Babicz, 2015). The Conning unit displays the vessel's status information, including heading, rudder angle, speed, thruster pitch, propeller revolution and pitch, water depth, and wind speed and direction (Kongsberg, n.d.).
- **CCTV cameras:** Closed-Circuit Television (CCTV), uses a network of cameras on board to provide video surveillance of operations. In addition to security monitoring of restricted areas, CCTV can provide visual aid for other purposes, including man-overboard detection, monitoring of maneuvering and berthing operations, cargo monitoring, and most importantly: accident and incident investigation (SAFETY4SEA, 2019).
- **Anemometer:** This device measures and reports wind speed and direction relative to the vessel (Babicz, 2015)
- **Echo Sounder:** Short pulses of sound beams are sent out and when they are reflected back from the sea bed or other objects in its path, the device calculates the distance the beam has travelled (NSW Department of Primary Industries, 1981).

- **LiDAR:** Light Detection and Ranging (LiDAR) is a remote sensing method using a laser, scanner, and specialized GPS receiver. Most commonly for topographic and bathymetric mapping in airborne systems, LiDAR has significant benefits for critical situational awareness, object identification, and tracking capabilities to augment existing SSS (Marine Handling & Logistics, 2018; National Oceanic and Atmospheric Administration, 2018).
- **RADAR (Foremast Radar, S-Band Radar, X-Band Radar, Automatic Radar Plotting Aids-ARPA):** Different types of RADAR (Radio Detecting and Ranging) are used to detect any solid objects around the vessel. RADAR plotting is tightly integrated with navigational subsystems, e.g. ECDIS (Babicz, 2015).
- **Doppler Sonar:** These systems detect the frequency shift of sound scattered from a moving object (Tollefsen & Zedel, 2003). This provides additional ship speed information for the integrated bridge.

Each navigation aid has vulnerabilities and could be misused in different ways to falsify sensor data or degrade and disrupt the input altogether.

2.3. Communication

Smart vessels can communicate via multiple modes, protocols, and technologies to provide the best possible redundancy and coverage. These technologies are integrated with the bridge and installed throughout the smart ship network. Resilient communication channels are imperative to the safe and efficient operation of the vessel at sea.

Satellite Communication systems (Satcoms) are transceivers for voice and data communication and operate on a spectrum between 3 and 30GHz and more. Satcom equipment, radios, cellular mobile devices, and Wi-Fi routers are required to access communication channels on Ultra High Frequencies (UHF) frequencies (300MHz-3GHz). Very High Frequencies (VHF) equipment receives radio and television broadcasts at 30-300MHz. The Navigational Telex System (Navtex) is used to transmit alerts and receive maritime safety information on 490/518 kHz (MF), while signals for maritime radio and navigational aids (eAtoNs) are broadcast on Very Low Frequencies (VLF) and Low Frequencies (LF) between 3 and 300 kHz.

Table 5 summarises the communication modes linking IT and OT systems on board and on shore. The design and configuration of the links and channels rarely consider authentication and encryption methods, thus exposing potentially vulnerable and legacy system to the internet.

IT systems on vessels are often connected with onshore facilities and this further increases the exposure to systemic and persistent threats (Baltic and International Maritime Council, 2017).

Table 5 Communication modes connect corporate IT and OT:

	IT system	OT systems	Modes
Port and Marine Facility	<ul style="list-style-type: none"> • Operation/resource management • Container management • Material management • Automated cargo expediting • Container inspection system • Driver identification systems • Financial recordkeeping systems • HR (Human Resources) systems • Client, marketing information • Records management • Automated report management • Security management systems 	<ul style="list-style-type: none"> • Cranes and other moving systems • Pipeline management • HVAC • Fuel tank monitoring • Over-height measuring system • Dry bulk commodity monitoring system • Auger systems, conveyor belts, scales • Anemometer • Environmental monitoring systems 	<ul style="list-style-type: none"> • Wi-Fi • Email, fax, phone, etc. • NAVTEX • VSAT
Vessel	<ul style="list-style-type: none"> • Electronic track log • Office applications • Fuel consumption analysis • Just-in-time spare part ordering 	<ul style="list-style-type: none"> • GPS, DGPS, AIS, LRIT, ARPA, VTS, and other navigation • ECDIS • BNWAS and Electronic navigational and wheelhouse systems • GMDSS • SSAS • AtoN systems connected to shore or buoy-based transceivers • Engine room monitoring • VDR and S-VDR • Anemometer • Ship Energy Efficiency Systems 	<ul style="list-style-type: none"> • Onboard Wi-Fi and internet • VoIP, Satellite networks • Radar, SITOP, NAVTEX • Satellite phones, other ship-to-shore communication

Source: (Transport Canada, 2016)

IOActive researchers analysed client software and firmware from popular Satcom vendors Harris, Hughes, Cobham, Thuraya, JRC, and Iridium. They found that *all* of the tested products have severe security flaws and explained how attackers could potentially exploit them (Santamarta, 2014a). It stands none of the manufacturers follow secure programming standards and best practice (e.g. Secure Software Development Life Cycle–SSDLC) to protect their systems and customers from unauthorised access. The most common vulnerabilities include backdoors and stored password stored within the firmware. Designed to make the (remote) troubleshooting and maintenance efficient for the vendor, these flaws are easily exploited by an adversary. See Table 6 for further information on each of the tested vendors and products.

Table 6 SATCOM equipment vulnerabilities and potential attacks

Vendor	Product	Vulnerability Classes	Potential attack scenario
Harris	RF-7800-VU024 RF-7800-DU024	<ul style="list-style-type: none"> • Hardcoded credentials • Undocumented protocols • Insecure protocols • Backdoors 	Widely used by NATO. Attacker injects malicious firmware update; malicious code can relay device's GPS location to the enemy. Code can disable communication or damage the terminal, potentially leading to loss of life
Hughes	ThurayaIP 9201/9202/9450/9502	<ul style="list-style-type: none"> • Hardcoded credentials • Undocumented protocols • Insecure protocols • Backdoors 	Used across critical infrastructure. Backdoor 'admin code' can be generated and attacker can send spoofed SMS control messages to the terminal. Potential to use for fraud, denial of service, physical damage or data spoofing.
Cobham⁵	EXPLORER (all versions) SAILOR FB 150/250/500	<ul style="list-style-type: none"> • Weak password reset • Insecure protocols 	EXPLORER models used in two-thirds of Inmarsat satellite terminals. Malicious firmware installed during personal internet-browsing on terminal. Malware then leaks GPS coordinates to attacker.
Cobham	SAILOR VSAT 900	<ul style="list-style-type: none"> • Weak password reset • Insecure protocols • Hardcoded credentials 	VSAT terminals deployed on ships, communicating to various systems onboard. Compromise may lead operators to make devastating navigational decisions based on spoofed ECDIS chart data. Catastrophic consequences possible, e.g. when cargo is hazardous and ship is grounding.

Source: Adapted from (Santamarta, 2014a)

Based on these results, it is “almost impossible to guarantee the integrity of thousands of Satcom devices” (Santamarta, 2014b). One compromised device can put the entire Satcom infrastructure at risk. Owners and vendors are urged to maximise their efforts to mitigate these risks:

- Evaluate network exposure of devices
- Implement security policies
- Enforce network segmentation
- Apply traffic flow templates (TFT)
- Vendors to provide security patches, recommended configurations, and official workarounds

⁵ Formerly known as Thrane & Thrane

2.4. Control

The integration of modern protocols with legacy control systems proves to be complex, as learned in other industries and critical infrastructure. Maritime stakeholders work with multiple platforms and protocols to add interoperability layers, but the lack of skills and resources often results in compromised solutions and increases the potential for unintended or malicious security incidents.

Industrial Control Systems (ICS) on ships help to reduce human errors, increase resource efficiency, prolong equipment life, and ensure economic advantages (J. Wang & Zhang, 2000). Intelligent process control is incorporated in all mechanical systems on board. ICS regulate and monitor environmental parameters on board, including temperature, pressure, level, viscosity, flow control, speed, torque, voltage, current, machinery and equipment status (Zaghloul, 2014). Figure 3 shows the extent of the systems that can be controlled, monitored, or automated using ICS. An ICS typically consists of these components:

- **Sensors and actuators:** Interact with the physical world, e.g., pressure sensors, valves and motors.
- **Local Human-machine interface (HMI):** Allows monitoring and control of sub-processes, sensors and actuators.
- **Supervisory screen:** Provides remote supervision of automated processes.
- **Data historian:** Records all data from production and SCADA networks, allows export to corporate IT systems, e.g. ERP (Enterprise Resource Planning).

(Soullie, 2014a)

Operational Technology (OT) incorporates Industrial Control Systems (ICS), which in turn comprise of the management layer (Supervisory Control and Data Acquisition system – SCADA) and the distinct processes within the production network (Discrete Process Control systems – DCS and Programmable Logic Controllers – PLCs).

ICS that are integrated in other business processes, e.g. resources planning, provide opportunities for smart decisions and interactions with cyber-physical systems.

Since the first lightbulb was installed in a ship in 1880, electric power has become an essential of seafaring (Skjong, 2017). From running communication equipment to alarm systems, even electrical propulsion has been a viable since the 1990s. Today, electricity on board is generating using a prime mover and an alternator powered by a diesel generator. The Power subsystem includes the generator and the main switchboard to control the distribution. Power Management Systems (PMS) are critical to distribute electricity, to minimise the risk of a blackout, and to maximise fuel efficiency. Electrical systems are tightly integrated with other automation and control systems enable functionality for safe and optimal operation (Radan, 2008).

Maritime process control systems are characterised by the use of point-to-point communication and proprietary hardware, software, protocols, and MMIs (Man-Machine-Interface) (Rødseth, Øgaard, & Hallset, 1992). We explore a range of resulting challenges in the following sections.

2.4.1. Fear of Breaking Things

Ships are designed to work for up to 50 years, but not all systems and software on board have a similar life span (Fitton, Prince, Germond, & Lacy, 2015). Shipowners are reluctant to touch any technology that appears to work as required. Just to improve security, replacement of equipment could cause significant compatibility issues, require large-scale maintenance outages, or be simply financially prohibitive. Upgrades to other attached systems also have the potential to interfere with other ICS and are therefore not considered at all. Unfortunately, outdated software and the absence of a regular patching or virus-scan regime can allow an attacker to use malicious techniques which would otherwise not be a threat.

The “Fear of Breaking Things” also applies to the inadequate configuration of hardware and software, the ignorance of best implementation practices and inadequate network segmentation and access control for third parties, e.g. for remote maintenance (Baltic and International Maritime Council, 2017).

2.4.2. Process is King

ICS control and monitor parameters on board, including temperature, pressure, level, viscosity, flow control, speed, torque, voltage, current, machinery, and equipment status (Zaghloul, 2014). ICS are often so critical that pausing them even for system upgrades is simply impossible. Ship operators work under extreme conditions and see no value in cybersecurity procedures – their highest priority is the uninterrupted process control. A major concern is that operators and engineers routinely bypass security for convenience and efficiency, which could have a cascading effect on the entire organisation (Zurich, 2014). This behaviour is attributed to the lack of awareness and skills, the commercial pressure to save time, and the plain non-adherence to security policies.

2.4.3. Integration and Convergence

SSS comprise technology from many different eras and vendors. It is crucial for integrators, implementers, and operators of ICS to understand the system’s limitations and vulnerabilities of its components and protocols. Primary control systems (hydraulic, electrical, automatic control) are vital to the ship’s safe voyage and exposed to difficult environmental challenges, such as pressure, vibration, and humidity. These control systems are now integrated via the ship’s distributed IT network. A continuous link between IT networks and on-shore facilities enables remote access for monitoring, fault-finding, and troubleshooting reduces site travel costs and streamlines the collection and analysis of field data (Moxa Inc., 2017; Orbcomm, 2017).

Operators and administrators can easily lose track of the countless combinations of legacy and current technologies, topologies, protocols, and communication modes on board. Most of these components were designed and programmed without any security in mind and data is transferred in plaintext. The onus of *securing* the components should be shared between the vendor, who follows a secure development framework, and the operator, who configures the components in line with industry standards and recommendations. The reality is often that either party assumes that the other party is responsible and no-one does it at all, leaving many critical weaknesses for attackers to exploit (Shoultz, 2017). Table 7 provides a reference of the major differences between IT and OT priorities.

Table 7 Differences between IT and OT attributes

Attribute	IT	OT
Confidentiality (Privacy)	High	Low
Message Integrity	Low-Medium	Very High
System Availability	Low-Medium	High
Authenticate	Medium-High	High
Non-Repudiation	High	Low-Medium
Time Criticality	Delays tolerated	Critical
System Downtime	Tolerated	Not acceptable
Security Skills/ Awareness	Usually good	Usually poor
System Life Cycle	3-5 years	15-25 years
Interoperability	Not critical	Critical
Computing Resources	Unlimited	Very limited with older processors
Software Changes	Frequent	Rare
Worst Case Impacts	Loss of data	Equipment destruction, injuries, death

Source: Adapted from Information Security Audit and Control Association (2016)

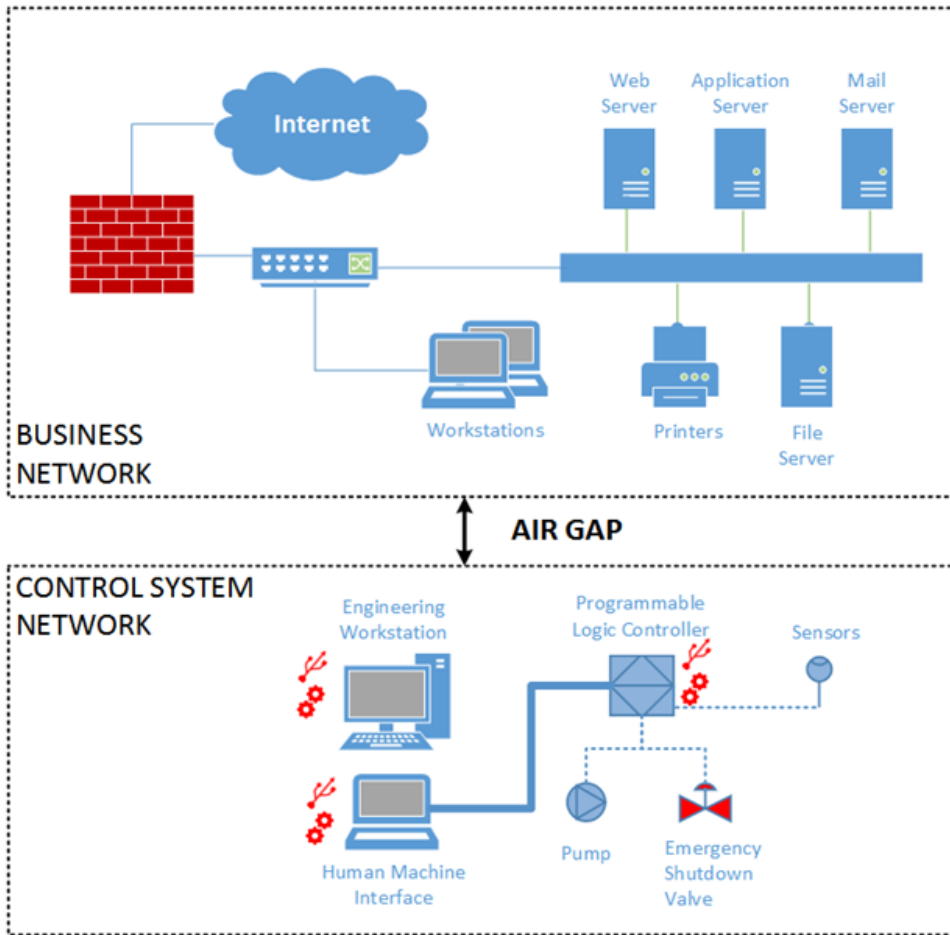
Many non-malicious incidents and outages are attributed to the physical and mental fallibility of humans, for example from data input errors to the general lack of security awareness. However, even the design and configuration of IT/OT data links and channels rarely consider authentication and encryption methods, thus exposing potentially vulnerable and legacy systems to the Internet. Furthermore, IT systems on vessels interface with onshore facilities and other IoS elements, which increases the potential exposure of the ship to systemic and persistent threats. There is a great interest to protect the confidentiality and integrity of the transmitted information between on- and offshore systems, which can be invaluable for criminal operations. Compromised port- or customs databases may allow criminals to locate precious cargo, track containers with contraband, or delete any evidence of suspicious activities.

“Air-gaps” physically separate critical systems and networks from the corporate IT network and the internet (see Figure 11 below). The 2010 Stuxnet incident first demonstrated that even Critical Infrastructure ICS in isolated networks are no longer impenetrable by adversaries (Falliere, Murchu, & Chien, 2011). In this case, attackers physically deployed USB drives containing malware to infect the ICS network with the intent to cause disruption and damage. The attacker’s methods and tools have been widely analysed and publicized and today it is a trivial effort to replicate these type of attacks with software suites like “Brutal Kangaroo” (Paganini, 2017).

With the digital transformation of the maritime domain grows the need for permanent connections between business IT networks and control systems (Transport Canada, 2016). IT networks provide the opportunity to integrate core business and operation systems on board and leverages shared databases and other systems (refer to Figure 12). For example, these systems can be used for accounting, cargo management, customs and shipping, human resource planning, and administration (Hudson Analytix Inc, 2017). As result of converging technologies and OT-integration into enterprise systems, persistent TCP/IP connectivity is needed. This may not just be limited to internal company networks, but often extend to technology vendors who require persistent remote connectivity to honour their maintenance and troubleshooting contracts.

There is every reason to take advantage of new technologies on board if the risks are understood and mitigated

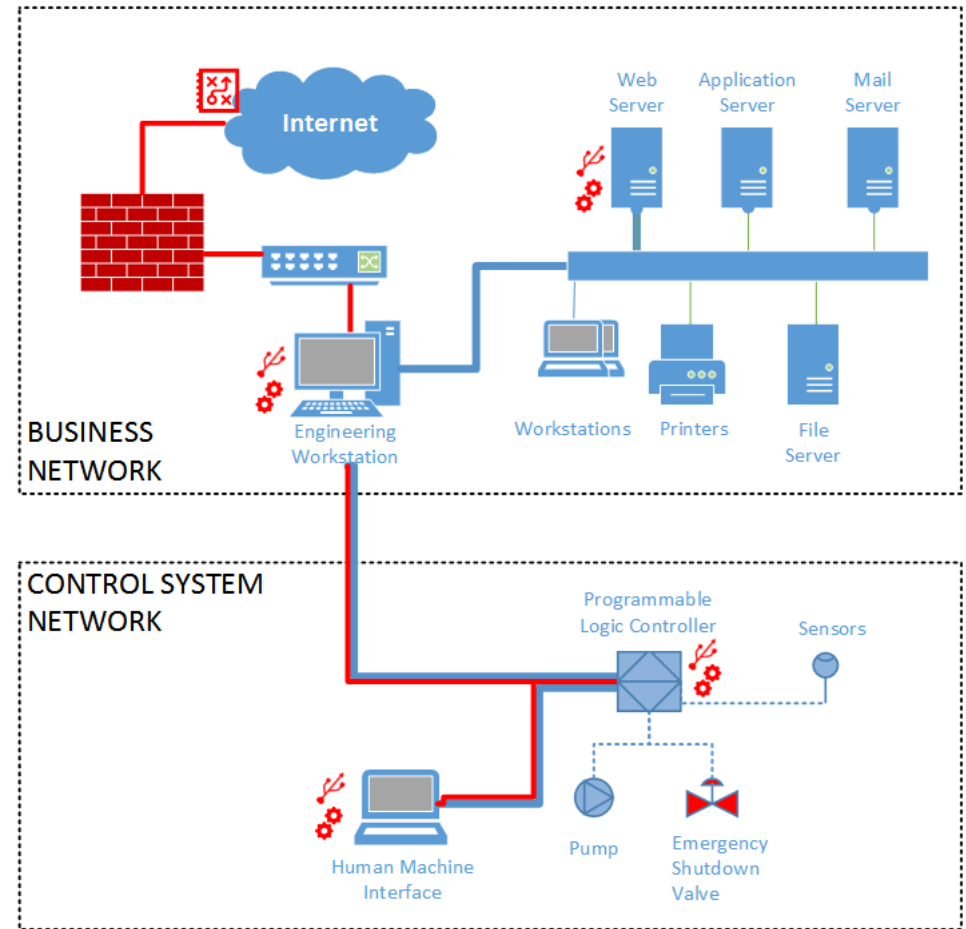
Air-gapped Business and ICS Network



Source: Adapted from (United States Coast Guard, 2017)

Figure 11 Air-gapped network

Integrated Business and ICS Network



Source: Adapted from (United States Coast Guard, 2017)

Figure 12 Integrated network

2.4.4. ICS protocols

Protocols used in ICS were originally developed without security and serial communication and local access. TCP/IP networking capabilities were added subsequently for logistical and commercial benefits (e.g. remote access). This means that the underlying protocol is still inherently flawed and can potentially be exploited and controlled over the internet.

Soullie (2014a) tested a range of commercial Programmable Logic Controllers (PLCs) and found that all products are vulnerable and insecure at protocol- and implementation level. He audited open ports 102 (Siemens S7) and 502 (Modbus) and found that most PLCs have plain HTTP and FTP interfaces and thus allow dangerous commands (read/write/delete) to be submitted to the controller. Table 8 gives a summary of common protocols used in ICS, their application, and their security features.

Table 8 Common ICS protocols and security features

Protocol (TCP/UDP port)	Application	Security features
Schneider Modbus (TCP/502)	Process Automation	Clear-text transmission No authentication
Siemens S7 (TCP/102)	Process Automation	No authentication No encryption
EtherNet/IP (TCP/44818, UDP/2222)	Process Automation Ethernet Industrial Protocol (Rockwell Automation)	No security features
BACnet (UDP/47808)	Building Automation and Control network	Has security features but manufacturers do not implement them
Niagara Tridium Fox (TCP/1911)	Tunnel to remote SCADA networks. Facilitates communication between workstations and devices and components (e.g. BACnet)	Has built-in security and authentication features

Source: Adapted from (Soullie, 2014b)

2.4.5. Open ICS interfaces on the internet

The search engine *Shodan* scans the entire IP range on the internet for directly connected devices (e.g. webcams, industrial control systems, and embedded devices (Matherly, 2017)). This can reveal manufacturer names, product codes, and other data which is useful for a potential attack. Vendors generally publish default credentials on their websites and many terminals run with unchanged default factory settings, including administrator usernames and passwords. This allows for a compromise of the network and may give up an entry point to critical control systems.

(Mirian et al., 2016) studied the public exposure of ICS devices and located 3.5 million devices with an open TCP port 502. They narrowed down the result to the Modbus protocol and collected device information from 4700 devices. This included vendor names, product codes, and other valuable data for a potential attack. To an adversary, the presence of Modbus, S7, or DNP3 protocols may indicate exploitable vulnerabilities. Figure 13 shows a sample search result for open port 502 (Modbus default) in Perth, Australia. Modbus is known to transmit data in clear text without authentication (Soullie, 2014b).

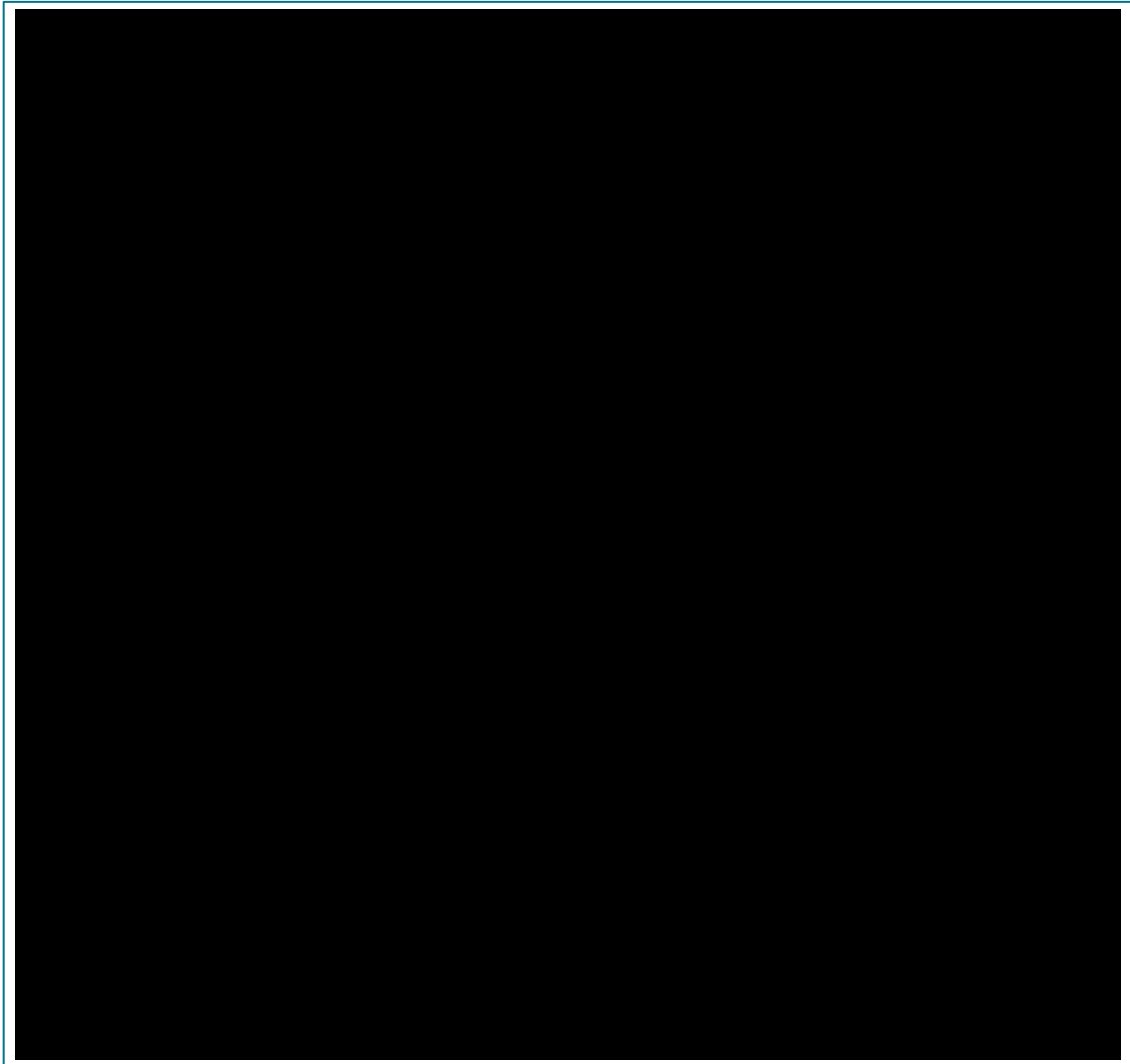


Figure 13 Shodan search for open Modbus devices (Port 502) in Perth, WA

The result immediately shows the type of controller that is connected, and an internet search reveals that it is a smart solar controller. Further research may tell the attacker specific or common credentials for this manufacturer (e.g. Figure 14) or other protocol-level flaws that have been publicised and be used to launch an attack.

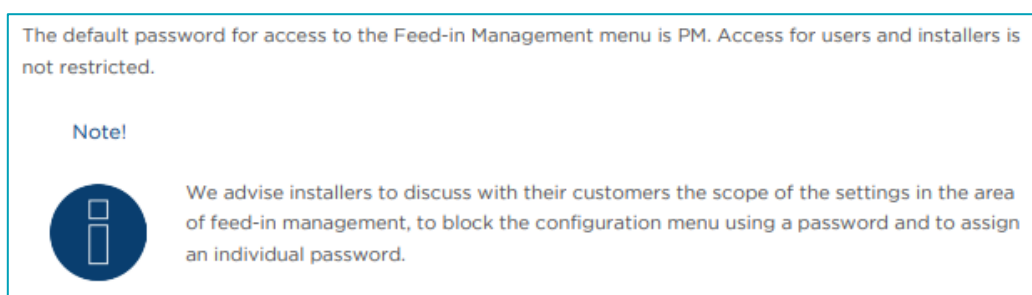
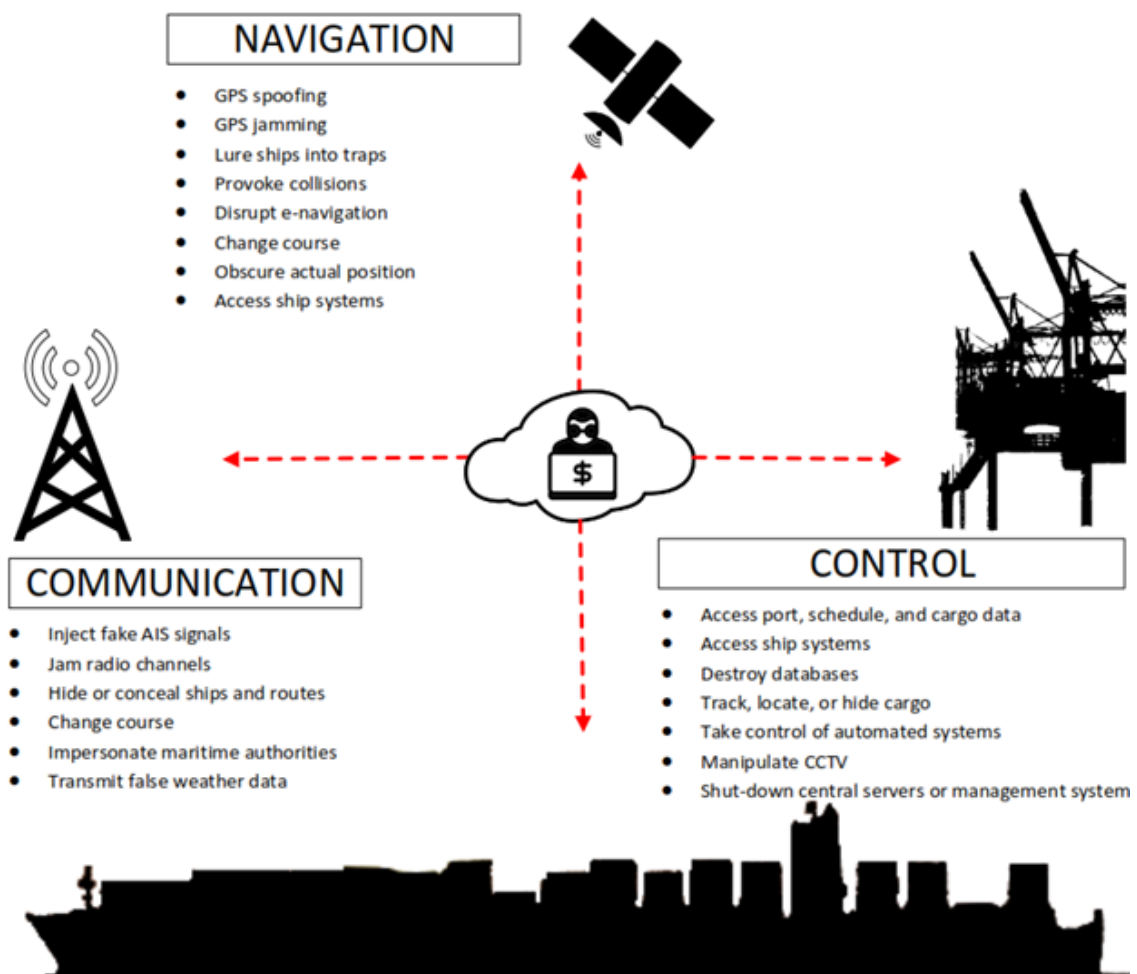


Figure 14 User manual excerpt of Modbus solar meter showing default password⁶

⁶ https://www.solar-log.com/manuals/manuals/en_GB/SolarLog_Manual_3x_EN.pdf

2.5. Summary

This section explored some of the major systems and subsystems on a vessel that facilitate smart decision-making for navigation, communication and control. The most likely threats on board arise from system glitches, compatibility or legacy issues, human errors, and other unintended events. However, this section demonstrates that SSS are also widely exposed and very susceptible to malicious cyber-attacks. After introducing the systems with overarching functions (bridge, VDR, IT networks), this section has analysed the remaining attack vectors for SSS from three perspectives: navigation, communication, and control. The attack vectors are summarised in Figure 15 and will be useful for mapping the cyber-threat landscape, which is further explored in Section 4.



Source: Adapted from (Lampe & Schwartze KG, 2015)

Figure 15 Potential security threats to navigation, communication, and control systems

3. Internet of Ships

The concept of the “Internet of Ships” (“IoS”) is the logical ecosystem that connects all maritime stakeholders, using diverse technologies and communication protocols. As mentioned existing work used the term “Internet of Ships” referring to the integration of IoT devices into design and building processes, (G. Liu et al., 2016; The Royal Institution of Naval Architects, 2017) and for a unified platform for ship data analytics (Ikeda, 2017)). Nevertheless, in this thesis, IoS is referred to as a technological ecosystem (akin to “Smart Cities”, the “Internet of Vehicles”, and the “Industrial Internet of Things”) that extends into each of the five major services nodes:

1. Terrestrial Services
2. Ship-to-Shore Services
3. Marine Navigation and Safety Services
4. Offshore Services
5. Satellite Services

The section examines these five areas of the IoS and the vital services they facilitate (summarised in Figure 16). When multiple industries and partners rely on the exchange of data on so many levels, the number of vulnerabilities rises along with the exposure to global threats.

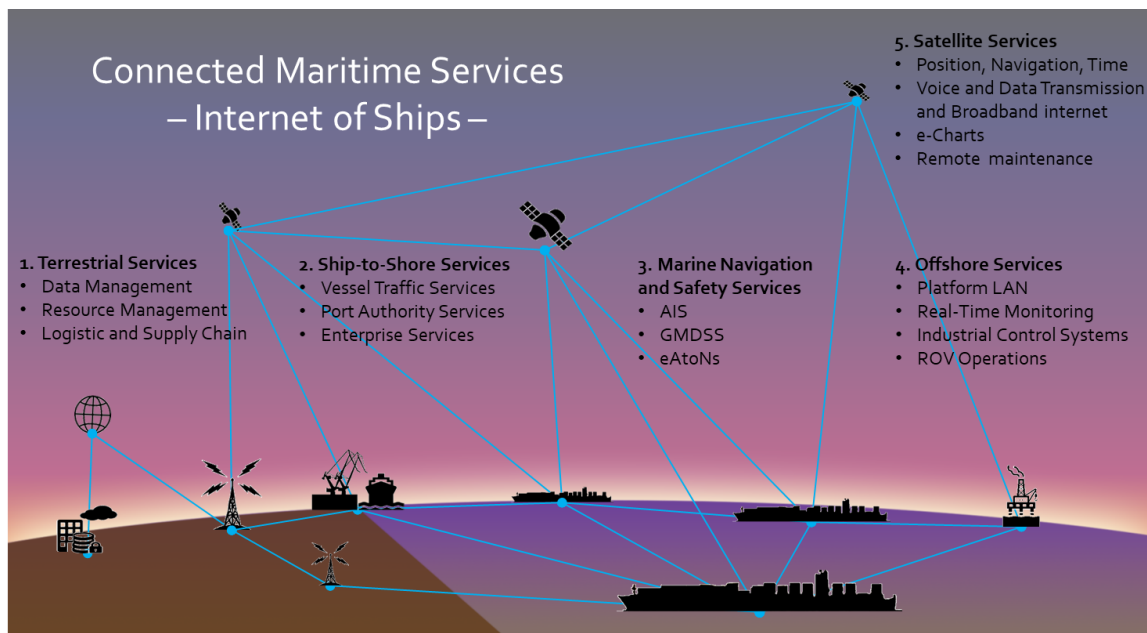


Figure 16 Overview of five connected maritime service nodes of the Internet of Ships

3.1. Terrestrial Services

A key factor for the success of any business is the efficient management and use of resources including time, money, and people. Terrestrial services assist the maritime industry with these critical business capabilities. Shipping companies use real-time data from all operations, on land and at sea, to streamline the scheduling of outages, equipment allocation for maintenance tasks, and ordering of spare-parts only when needed (Transport Canada, 2016). The land-based node of the IoS infrastructure is the backbone of the industry as it connects to datacenters, clients, suppliers, and the rest of the world.

The following section summarises the essential terrestrial IoS services: Data Management, Resource Management, and Supply Chain and Logistics Management.

3.1.1. Data Management

Data collection and storage

Ships are equipped with either integrated or distributed “Ship Information Systems” (SIS), which collect a wealth of data from ship sensor networks, control networks, and voyage recorders (S. Liu, Xing, Li, & Gu, 2014). Traditionally, this data was either stored on the ship, or not retained at all. Today, the shipping company typically downloads voyage datasets to the branch database when the vessel arrives at the port.

SIS are synchronised with port-based branches or directly with the company head-offices via Wide Area Networks (WAN), Global Systems for Mobile communications (GSM), or satellite broadband links. Alternatively, engineers copy the data on portable hard drives and take them off board. Vessel data is then stored for analysis on company servers on-premise, at local shared datacenters, or on “Platforms as a Service” (PaaS), e.g. Amazon Web Service or Microsoft Azure (S. Liu et al., 2014).

The collection and management of ship and business information involves handling of data by different parties with different levels of trust, skill, and awareness. An unsuspecting contractor with an infected USB drive can create as much disruption as a malicious or disgruntled insider with elevated access to internal databases. Section 4 provides further examples and measures to reduce many of the risks associated with data transfers and management.

Data analysis and modelling

SIS collect great amounts of information from thousands of datapoints on board including from environmental sensors (e.g. Heating, Ventilation, Air-Conditioning systems – HVAC), health sensors (e.g. from Hull, Mechanical & Electrical systems – HM&E), alarm and security systems, and voyage data recording systems, and many more. These large and diverse datasets are commonly described as “Big Data” and their analysis and modelling provide opportunities to optimise port cargo positioning, monitor vessel performance, improve customer service, simplify complex procedures, automate processes, and fast-track decisions (IBM Corporation, 2018).

Data analysts can predict failures before they occur and schedule replacements before parts break (“Preventative maintenance” and “Just-In-Time spare parts management”). This not only minimises disruptions to the vessel’s schedule and the time spent idle in ports, it also helps extend the operational service life of the equipment (Bensing, 2009; UNCTAD, 2017).

Companies offering cloud Software- or Platforms-as-a-Service (SaaS/PaaS) allow shipowners to save costs by outsourcing the computing and analysis to third-party infrastructure. This means that large amounts of data will be transferred over potentially uncontrolled media to transform “Big Data” into digital intelligence. The actual risk of processing data in the “Cloud” depends on the contracts, policies, and safeguards of the hosting company’s own infrastructure.

3.1.2. Resource Management

Resource management refers to the allocation of physical equipment and the scheduling of maintenance tasks, but also to the management of employees and contractors (Human Resources). Efficient resource management relies on data analytics and predictions. Enterprise resource planning (ERP) systems are widely implemented in organisations with the aim to collect all corporate information in a central database and make it visible to everyone responsible for resource allocation and management (Dechow & Mouritsen, 2005).

Trust in an ERP system can only go as far as the manufacturer can be trusted to develop the program securely, and the systems administrator can be trusted to securely configure and integrate it into the rest of the enterprise infrastructure. Other major issues with ERP systems are network disruptions (denial-of-service), poor configuration, exploitable web-interfaces and databases, and the lack of error-tracking by operators and others (Goel, Kiran, & Garg, 2012).

3.1.3. Logistics and Supply Chain Management

Maritime logistics are regarded as the primary means of transport and ships carry about 90% of all trade globally (Allianz Global Corporate & Specialty, 2017; Panayides & Song, 2012). Any disruption within the network of manufacturers, suppliers, and end-users (supply chain) can have major effects on the economy. To keep the supply chain intact, all cargo including parts, goods, resources, food, and livestock must be traced from its origin to its destination.

The technologies at the forefront of digital data collection are barcoding, Radio-Frequency Identification (RFID), Global Positioning System (GPS), and IoT devices and sensors. IT networks facilitate the integration of smart devices and sensors with centralised control and monitoring of cyber physical systems (CPS), e.g. pick-and-carry cranes for containers. Enterprise IT networks provide connections between the necessary computing resources and sustain the continuous flow of information between the participants of the IoS supply chain.

Shipping companies and ports invest heavily in digitisation and automation to keep up with the growing demands from exporters and importers (Australian Logistics Council, 2010). In addition to commercial pressure, the shipping industry is bound to strict regulations regarding environmental sustainability and the reduction of carbon emissions. Data Management and Resource Management Services are closely integrated with Supply Chain Management (SCM)

systems to provide meaningful, real-time support for critical business decisions (Australian Logistics Council, 2010).

In June 2017, a malware infection caused the Danish shipping giant A.P. Moller-Maersk financial losses of more than US \$300M. The attack started when an employee of a opened a malicious email and allowed ransomware to spread render Maersk's entire container business inoperable. Attached systems had to be shut down to prevent the malware from spreading to other networks and third-party resources. The ripple effects disrupted operations on a global scale (Mimoso, 2017; Symantec Security Response, 2017).

Protecting the entire supply chain from cyber-attacks is near-impossible given that many potential attack vectors are already ingrained into the supply chain. However, the risk of cyber-attack can nonetheless be reduced. Systematic approaches to mitigating supply chain risk start from the inside out, i.e. with getting transparency around all information assets and processes, and understanding, enumerating, and securing all interfaces with third parties and their level of access to information systems.

3.2. Ship-to-Shore Services

Ship-to-Shore Services include IoS functions that establish communication channels for the real-time exchange of information between ships and on-shore entities, including port authorities, customs agencies, and shipping companies. These channels are vital for the safe navigation in and around ports, but also ensure the efficient processing of inbound and outbound cargo and passengers.

3.2.1. VTS – Vessel Traffic Services

Vessel Traffic Services (VTS) are “Joint Cognitive Systems (JCS)”, comparable to Air Traffic Control (ATC) as they embed humans and technology to monitor and coordinate complex and dynamic ship movements near shore and in ports (Praetorius, 2014). VTS are mandated under the “International Convention for the Safety of Life at Sea (SOLAS)” and guided by the International Maritime Organization (International Maritime Organization (2009) and local maritime authorities (e.g., the Australian Maritime Safety Authority (2013)).

To coordinate traffic, VTS operators communicate with ships via Very-High Frequency radio (VHF radio) and they rely on other systems including closed-circuit television cameras (CCTV), radar, and the Automated Identification System (AIS). The combination of voice, visual, and sensor data is a reliable navigational aid and significantly reduces the risk of collisions and groundings in areas of high traffic in and around ports.

The service uses combinations of technologies including radar, AIS and voice communications (Shoultz, 2017). VTS exposed to disruption or tampered data which can lead to marine traffic incidents.

3.2.2. Port Authority Services

Communication interfaces between ships and port authorities enable the monitoring and enforcement of reporting requirements and regulatory compliance (e.g. Chapter V, SOLAS (International Maritime Organization, 2009); Marine Order 63 (Vessel reporting systems) 2015, under the Australian Navigation Act 2012 (Australian Maritime Safety Authority, 2017)).

Vessels communicate wirelessly with port authorities to identify themselves, report their position, and gain access to the port (Boyes & Isbell, 2017). Customs agencies exchange data with foreign vessels before they can load or unload any cargo or passengers. The coast guard, for example, may request to inspect data from the vessel's Ship Information System (SIS) to investigate any incidents or violations of safety and environmental regulations.

Port Authorities are key ship-to-shore services as they continuously facilitate the tracking and movement of vessels and cargo. Due to the central authority, Ports exchange data with a wide range of maritime stakeholders – from military to commercial enterprises to private boat-owners.

Port Authorities store and handle vast amounts of confidential data (e.g. the Bill of Lading, records of financial transactions). From 2011 to 2013, criminals used keyloggers to maintain unauthorised access to the cargo system of Port Antwerp. They were able to locate containers with contraband and load them on to their own trucks. Then they deleted the evidence of the container's existence (Magal S3, 2014).

As mentioned above, ports are implementing more and more digital technologies and transform into "Smart Ports". The main objective for port operators is to improve safety and security, but more beneficial for shipping companies is the increase of operational efficiency in a domain of strong competition and small margins (UNCTAD, 2017). The transformation to Smart Ports is largely made possible by small, inexpensive, wireless IoT devices, advanced industrial systems and robotics, and Big Data analytics and modelling with improved machine learning algorithms (Australian Logistics Council, 2010).

3.2.3. Enterprise Services

Ship-to-shore enterprise services are essential because they connect the vessel directly with the shipping company and give access to real-time data to monitor health and performance and allow rapid decision making (Deloitte, 2017). Shipping agencies often use port-based offices for data-exchange with the ship via WAN, Wi-Fi, or GSM/3G/4G for a range of functions, including:

- Passenger service portal
- Voyage performance monitoring
- Ship health monitoring
- Cargo inventory and logistics
- Fuel and oil management
- Updates of hydrological, meteorological, and map data

Enterprise services are attractive attack vectors, especially for corporate criminal organisations. Major risks include corporate espionage, sabotage, and fraud. An example for espionage occurred

when confidential data was stolen from Japanese and Korean companies between 2011 and 2013. A successful spear-phishing attack unloaded the malware “Icefog” to create a backdoor for the criminals. The profiles of their spear-phishing targets suggest that the attackers were interested in shipbuilding and maritime operations. They spent a significant amount of time in the network while they exfiltrated documents and passwords and then cleaned up their tracks (Kaspersky, 2013). An incident of sabotage occurred in 2011 when attackers broke in to the carrier information system of the Islamic Republic of Iran Shipping Lines (IRISL). They deleted all container data and disabled internal communications networks. This significant disruptions and financial losses to the shipping company (CyberKeel, 2015), (DiRenzo, Goward, & Roberts, 2015). A case of fraud was discovered after criminals used malware to deceive a company into transferring money to the criminal’s bank account. World Fuel Services lost \$18m [32].

Ship-to-shore services are essential elements of the IoS and deserve attention from the cybersecurity perspective. Data routinely moves across security domains using a mixture of safe and unprotected transmission channels. The ship-to-shore interface is the primary link to the supply chain and particularly vulnerable to physical threats (lack of access control), signal interception and interference (unsecured datalinks) and social engineering (e.g. phishing, impersonation, USB-drop attacks).

3.3. Marine Navigation and Safety Services

It is vital for a safe voyage and for fast response times in emergency situations to be able to access maritime navigation and safety services and protocols. These services – most notably AIS, GMDSS, and eAtoNs – depend greatly on the uninterrupted connectivity between technologies and systems on board and other nodes of the IoS. This section describes the purpose and the components of these systems and how they fit into the IoS.

While the main safety concern is the satellite connection for positional fixes, these services are also vulnerable to Electromagnetic Interference (EMI). The satellite signal travels great distances and is susceptible to loss due to unintended noise (e.g. weather conditions) or malicious overpowering with a jamming device. Another significant risk is the tampering of an attacker with the location and timing data for vessel traffic or emergency services. The following details three major navigation and safety services with their cybersecurity issues, keeping in mind that many weaknesses relate to the unsecured or unverified input of data into these systems.

3.3.1. AIS – Automatic Identification System

AIS is a maritime tracking system which continuously broadcasts the ship’s position and other vessel information via VHF signals to other ships and coastal authorities in range. AIS is used to provide “fast, automatic and accurate information in order to reduce the risk of collisions” (Australian Maritime Safety Authority).

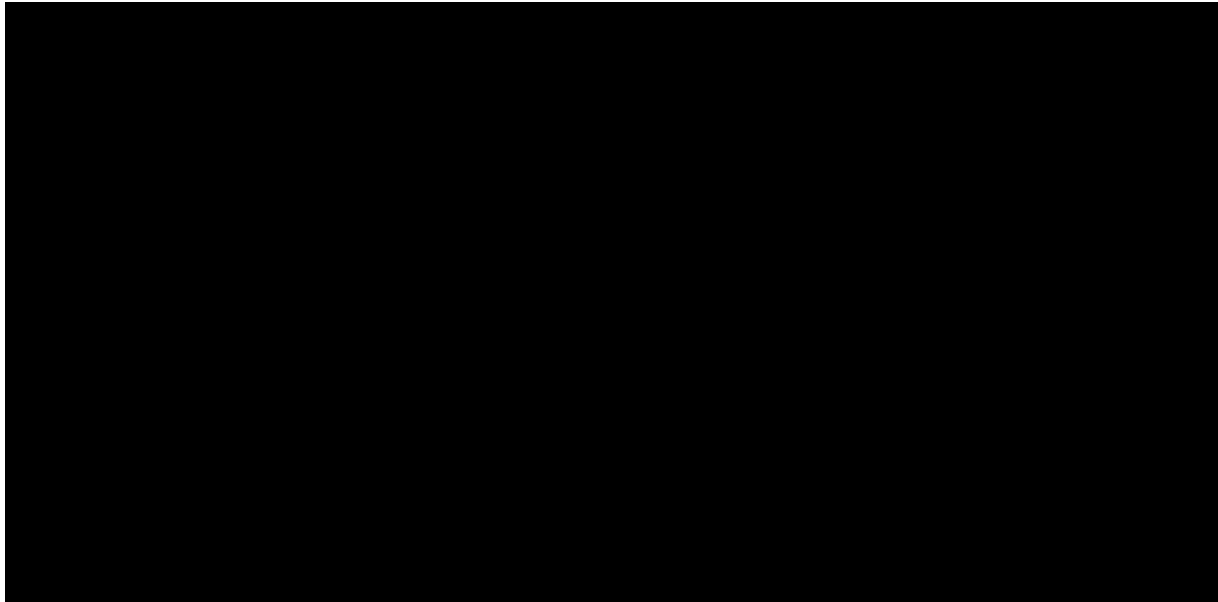
AIS is a component of the Vessel Traffic Service that assists with port navigation, rescue operations, and accident investigation. Similar to the Automatic Dependent Surveillance-Broadcast (ADS-B) system used in air-traffic control (Parkinson, 2011), AIS is critical for

maritime domain awareness to avoid collisions, groundings, and other accidents (Australian Maritime Safety Authority, 2018).

AIS is mandatory on all passenger vessels, on ships on international voyages with 300 or more gross registered tonnage (GRT), and on cargo ships with 500 or more GRT not engaged in international voyages (International Maritime Organization, 2015). In addition to the regular, short-range AIS broadcast, the IMO requires vessels to report their geographical location four times per day to their country of registration via Long Range Identification (LRIT).

AIS was historically constrained to the range of VHF transponders and was only available near ports or other vessels up to 20 nautical miles. Today, AIS can also be tracked via constellations of dedicated micro- or nano-satellite across the world (“s-AIS” – satellite AIS) (Høyve, Eriksen, Meland, & Narheim, 2008; Masters, 2018).

Figure 17 shows an overview of AIS message content and generic physical setup with a computer connected to a display, to multiple VHF receivers for redundancy, and to the navigation subsystem.

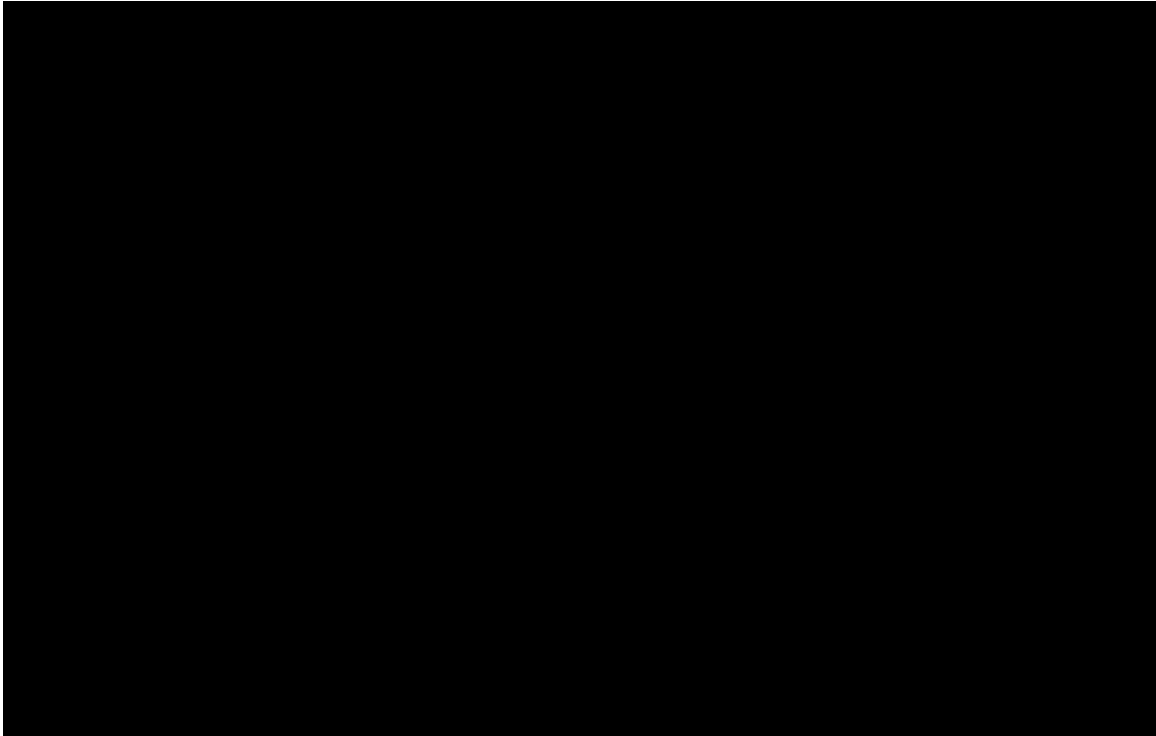


Source: <https://www.psicompany.com/ais/>

Figure 17 AIS overview

Researchers Balduzzi, Wihoit, and Pasta (2013) studied AIS and used inexpensive off-the-shelf equipment to demonstrate how trivial it is for an attacker to exploit its vulnerabilities and compromise the integrity of the data that the system relies on. AIS transponders communicate over the air without any authentication or integrity checks. Balduzzi injected AIS signals via a Software Defined Radio (SDR) to place fake “man-in-water” beacons and he utilised frequency-hopping to disable the AIS transponder and render the ship invisible. He managed to modify all ship details (name, cargo, position, course), he triggered fake CPA alerts (closest point of approach) and injected false weather reports. This experiment proved that AIS is broken at protocol *and* implementation level. Relying on the potentially incorrect information can lead to catastrophic outcomes and loss.

In addition to the vulnerable technology, AIS data of all vessels is online and publicly available via websites like vesselfinder.com and marinetransport.com (MarineTraffic, 2017; VesselFinder Ltd, 2017). Sample AIS information (including voyage history, destination, and vessel details) is provided in Figure 18 and Figure 19. The International Maritime Organisation (2004) has “condemned the regrettable publication on the world-wide web, or elsewhere” as it provides a wealth of information on the vessel and its route which can be invaluable for a targeted attack.



Source: MarineTraffic (2017)
Figure 18 Sample AIS route forecast



Source: MarineTraffic (2017)
Figure 19 Sample AIS vessel details

3.3.2. GMDSS – Global Marine Distress and Safety System:

GMDSS is an internationally agreed set of protocols and equipment to support alerting, positioning vessels in distress, search and rescue operations, safety broadcasts and general communications. The availability of this service is critical to locate vessels in distress and save human lives. GMDSS equipment is mandatory to carry on passenger vessels and cargo ships above 300 tons on international voyages (in accordance with SOLAS, the International Convention for the Safety of Life at Sea Convention 1974 (Shoultz, 2017)).

Search and Rescue (SAR) services rely on accurate and time-critical data and voice communication using the components that enable GMDSS on board:

- **Digital Selective Calling (DSC):** This is a digital enhancement to marine radiotelephony (e.g., Very High Frequency [VHF], Medium/High Frequency [MF/HF]). DSC allows to send digital distress signals to other DSC transmitters via a registered MMSI number (Mobile Service Identity Number) and to receive acknowledgement from shore stations (Australian Maritime Safety Authority, 2013; International Telecommunication Union, 2015).
- **Inmarsat terminal:** Where radio or DSC facilities are unavailable, distress signals are relayed to SAR authorities via satellites. Currently, the Inmarsat satellite constellation can provide near-global coverage for satellite communications (INMARSAT, 2019).
- **Emergency Position Indicating Radio Beacons (EPIRB):** EPIRB are small, battery-powered, buoyant devices that are registered in a global database. EPIRBs can be activated in situations of distress to continuously transmit a signal on 406.0-406.1 MHz (Australian Maritime Safety Authority, 2013). The International Cospas-Sarsat program is a dedicated satellite system that listens to these distress signals and notifies the nearest station on the ground. From there, the alert is escalated to a Rescue Coordination Centre which will arrange the SAR operations. EPIRBs can also be fitted with AIS capability (EPIRB-AIS) (Australian Maritime Safety Authority, 2019; International Maritime Organization, 2008).
- **Search-and-Rescue Transponder (SART):** All GMDSS regulated vessels and life rafts must carry a SART on board. SARTs are either radar- or AIS-based buoyant devices. In the event of an emergency, the device is manually activated to detect any incoming X-band radar pulses from other ships or planes. It responds with a signal that shows on the radar screen as a series of 12 dots pointing in the direction of the craft in distress. AIS-SARTs are equipped with GPS and also transmit the vessel ID and location via VHF to all AIS-equipped vessels in range (Orolia Maritime, 2019).
- **Maritime Safety Information (MSI) Receiver:** MSI is a set of broadcast protocols, describing distress messages, urgency messages, warnings, coastal warnings, local Sea Safety Message (SSM) warnings and general messages. MSI is transmitted via Navigational Telex (NAVTEX) or Inmarsat satellite broadcast bands (Australian Maritime Safety Authority, 2013).

An attack on the integrity or availability of GMDSS could have severe consequences to the safety of human lives. Malicious activation of emergency beacons or impersonation using a spoofed MMSI of the vessel in distress could lure responders away from the actual vessel, potentially leaving victims without help to survive. The MMSI identifies maritime stakeholders which are registered with safety authorities. MMSI can be spoofed similar to an IMSI (International Mobile Subscriber Identity) in consumer communication devices.

3.3.3. eAtoNs – Electronic Aids to Navigation

Situational and spatial awareness are critical for a vessel for safe navigation and avoidance of accidents. Physical structures (e.g., buoys, lighthouses, wrecks) help navigate through difficult lanes of passage by marking water depths or underwater obstructions (Shoultz, 2017).

These "Aids to Navigation" (AtoNs) can be equipped with AIS to enhance their visual usefulness and automatically broadcast the structure's characteristics and location (United States Coast Guard, 2016). These electronic Aids to Navigation (eAtoNs, also called Virtual AtoNs) show as virtual markers on a navigation display. eAtoNs can tag other vessels, wrecks, reefs, or other obstructions and alert nearby vessels in real-time (Jensen, 2009; Wright, 2017).

GNSS and electronic navigational charts (ENC) are also regarded as types of eAtoNs (Nicholson, Tutt, & Ward, 2015).

"A virtual aid to navigation (Virtual AtoN) does not physically exist but is a digital information object promulgated by an authorised service provider that can be presented on navigational systems" Wright (2017)

The trust in the integrity of eAtoNs allows the captain to safely maneuver the vessel through difficult passages and avoid collisions or groundings. Because they rely on vulnerable AIS technology and virtual buoys on electronic charts, eAtoNs are also susceptible to tampering, impersonation, and denial-of-service. It is possible to cause disastrous navigational decisions if eAtoNs are deleted or spoofed to appear in a different location on the electronic display.

3.4. Offshore Services

The following section outlines five major Offshore Services that relate to the IoS. Offshore installations such as Oil & Gas platforms or wind farms represent complex cyber systems that continuously exchange data with surrounding vessels and other platforms (e.g. via AIS, GMDSS, voice communications) and act as physical and virtual navigational markers (AtoNs, eAtoNs). Offshore services use broadband satellite connections (e.g. VSAT), 3/4G, troposcatter, undersea fibre-optic cables, and microwave line-of-sight, where these technologies are available (Comtech Systems Inc., 2014).

Due to their remote location, offshore IoS services are less vulnerable to threats from outside attackers, but they are still openly exposed to malicious or unintended threats from employees and contractors (e.g. malware on USB or field laptop), acts of nature, global external threats (e.g. large-scale jamming/spoofing), and unauthorised access via satellite communications or other

side-channels. The following section describes the main technologies with potential security issues and attack vectors.

3.4.1. Platform LAN

Offshore installations include oil platforms, drilling rigs, coastal defense systems, wind farms, and research facilities. It is critical for these installations to be able to communicate with other IoT nodes in range (e.g. terrestrial services, navigation and safety systems). On the platform itself, voice and data communication is enabled by Local Area Network (LAN) and Wireless LAN (W-LAN) infrastructure to service all areas of the platform operation.

Today, the shipping companies are expected to provide media and entertainment via local networks, and access to broadband internet for email, social media, and video streaming, to help staff to "switch off" between straining shifts in isolated areas. Providing for "Crew-welfare" requires increased bandwidth, which is one of the major selling points for satellite broadband technologies. But not every shipping company can afford to provide this level of internet access for everyone and this is where compromises are made.

Employees bring their own laptops or mobile devices, connect them to the network (with or without a "Bring-Your-Own-Device/BYOD" policy), play licensed or pirated media and share the media with other employees via removable storage devices. This also applies to official workstations and field laptops, which typically run with elevated privileges. The perception of isolation naturally leads people to feel less threatened by cyberattacks. There is a real risk of virus or ransomware infection that could impair parts of operations or stifle the entire network.

A recent report by the US Coast Guard (USCG) relayed one such incident where malware was accidentally downloaded by an employee and then impacted the dynamic positioning system, so the platform had to perform an emergency breakaway to avoid an accident (Crandal, 2018). In 2010, another non-targeted attack disrupted safety systems ("blowout preventer system, BOP") and computer systems on a South Korean oil drilling platform in transit. To prevent any catastrophic consequences due to the loss of safety systems, the rig had to shut down 19 days while the virus was cleared and all systems were brought back on-line (Crandal, 2018; Shaik, 2013). Outages, including those caused by cyberattacks, cost energy companies millions of dollars each year, but these attacks can have far worse consequences than the loss of money.

3.4.2. Real-Time Monitoring

Monitoring of sensor data and other information has been central to offshore operations since the 1940s. Trend analysis and anomaly detection are enabled with improved data-capture technologies and data quality. Today, real-time data (RTD) makes it possible to perform enhanced analytics and to achieve improved efficiency and risk management (Transportation Research Board, 2015). RTD can assist with weather predictions, scientific observations, piracy warnings, and responses to emergency situations.

The main uses for Real-Time Monitoring (RTM) in offshore drilling activities and production technologies have been identified as follows:

1. Subsurface and formation analysis; well planning and modelling
2. Wellbore stability and drilling integrity monitoring and analysis
3. Instrumentation for drill floor and rig operations
4. Bandwidth requirements for data collection, transmission points, wireless/wired, and standard protocols
5. Onshore center – data aggregation standardised interfaces, screens, display of relevant data, user interface, predictive capabilities, monitoring and alarming

Bureau of Safety and Environmental Enforcement (2014)

RTM improves performance, quality, and reliability of offshore operations; but most importantly enable automation that limits the human exposure to dangerous environments ((Transportation Research Board, 2015).

3.4.3. Industrial Control Systems

Industrial Control Systems (ICS), are essential to the operation of offshore installations. The local networks are designed to enable alarm and safety systems, environmental control (e.g. Heating, Ventilation, Air-Conditioning, HVAC), remote control and monitoring of subsea operations and experiments, and centralised management of automated processes (Supervisory Control and Data Acquisition, SCADA). Section 2.4 has provided the background on process control systems which applies equally to OT in offshore installations as it does to vessels and shoreside infrastructure.

3.4.4. Remotely Operated Vehicles

Remotely Operated Vehicles (ROVs) are instrumental to the development and maintenance of subsea fields. ROVs provide the safest means to interact with the underwater environment while speeding up operations and reducing overall expenses. As explained by Ioseba Tena (2011) The development of ROV capabilities includes benefits in the following areas of offshore operations:

Construction Support: Offshore construction involves expensive equipment and highly complex engineering tasks. ROVs can monitor the process, but also perform other duties, for example moving objects into required positions.

ROV Surveys: ROVs are equipped with a wide range of sensors that can gather high-resolution data with great navigational accuracy. While useful to save time and costs, the survey data has great value in comparing and analysing datasets to study the environmental impacts of subsea operations.

Inspection, Repair, and Maintenance: Navigational and station-keeping capabilities of ROVs allow maintenance engineers to plan inspection routes and observe underwater systems in a consistent and repeatable manner. Advanced ROV can automatically inspect features, detect faults, and carry out repairs in real-time.

Some of the common sensors on ROVs include:

- Doppler Velocity Log – using acoustic signals to measure speed
- Altitude and Heading Reference System (AHRS) – non-magnetic gyrocompass with pitch and roll measurements
- Depth sensor – pressure sensors to measure the depth of the ROV
- Multi-Beam Imaging Sonar (MBI Sonar) – streaming imagery to track subsea structures
- Acoustic Transponders determine the ROVs position using Ultra-Short Baseline (USBL) or Long-Baseline (LBL) positioning methods
- Inertial Navigation Solution (INS) – providing velocity and position data from integrated accelerometers, gyrocompasses, and aiding sensors

(Ioseba Tena, 2011)

3.5. Satellite Services

Satellite Services are the essential to the IoS because they provide capabilities for navigation, communication, and control in all domains, especially in remote locations at sea. Many of the concepts in Section 1.1 regarding PNT and satellite communications extend from the use of ships to the other IoS domains and often establishes the connection between them. As indicated in Section 2, SATCOM terminals enable different critical services on the vessel, e.g. VSAT, GMDSS, or FleetBroadband. Maritime satellite services operate on multiple frequencies, catering to different types of requirements and bank accounts. Table 9 summarises the main maritime frequency bands used for satellite services.

Table 9 Maritime Satellite bands and usage

Band	Frequency	Equipment type - common usage
L-Band	1–2GHz	Mobile Satellite Service used on small vessels – reliable but low bandwidth, small equipment, low power, low throughput
C-Band	4–8GHz	VSAT on passenger vessels and business-critical systems on offshore vessels. Reliable and high-bandwidth, larger antennas needed but can cause microwave interference
X-Band	9–12GHz	VSAT for government and naval usage – reliable and similar throughput to C- and Ku Band
Ku-Band	12–18GHz	VSAT, most commonly used maritime band, alternative to C-Band on commercial vessels. High bandwidth, high throughput. Smaller equipment and less power required, more susceptible to rain fade
Ka-Band	25.5–40GHz	VSAT, like Ku-Band but new to the market. Very high frequency requires high pointing accuracy and different antenna feed to Ku-band. Highly susceptible to rain fade

Source: <https://marlink.com/satcom-frequency-bands-and-how-they-affect-maritime-users/>

3.5.1. Position, Navigation, Time (PNT)

Global Navigation Satellite Systems (GNSS) broadcast accurate spatial and temporal data to support tracking and navigation functionality. These Position, Navigation, and Timing (PNT) capabilities are provided at no cost to the public via GNSS. Section 1.1.3 describes PNT and GNSS in detail.

3.5.2. Voice and Data Transmission, Broadband Internet

Media and communication satellite systems provide access to broadband internet, TV streaming, Voice-over-IP (VoIP), email, social media and more. Broadband internet and satellite communication require a monthly subscription with a provider like Inmarsat or Iridium. While entertainment services on board are not critical for operations and the safety on board, they play an important role for the crew morale and welfare (Abaimov & Ingram, 2017). Crew or guest-networks provide uncontrolled access to the internet and expose the users to malicious threats. These networks should be securely segmented, ideally using separate hardware switches, to reduce the risk of attacks spreading to other IT or OT networks (Baltic and International Maritime Council, 2017).

3.5.3. e-Charts – Electronic Navigational Charts (ENC)

Electronic Navigational Charts (ENC) are typically used on ships with Electronic Chart Display Information Systems (ECDIS) which explored in Section 2.2.2.

The importance of the trust in ENC for safe navigation in challenging environments cannot be understated. ENC must be issued by or on behalf of a Governmental body that meets the IHO ENC Product Specification, otherwise they are not compliant with SOLAS. Distributing companies still offer the “traditional way” of providing updated chart material via CD-ROM, which is arguably the safest way to assure its integrity. In addition, distributors offer to download updates from their websites or via email through satellite internet connection. As previously mentioned, the integrity of downloaded ENC should be protected with the S-63 data protection scheme (International Hydrographic Organization, 2010). The implementation and strength of the encryption algorithms used in the scheme, however, has been disputed. A skilled attacker may be able to point the download to an alternate location where malicious content is hosted or be able to tamper with the download transmission itself.

3.5.4. Remote Maintenance

Communication satellite systems provide the ability to connect to sensitive ship networks in any location in the world with onshore systems for remote maintenance and management of assets (United States Coast Guard, 2017).

Any remote access to offshore assets, including vessels and platforms, should be tightly secured and regularly monitored. It is also critical that any remote procedures are closely coordinated with the key personnel on board (Baltic and International Maritime Council, 2017)

3.6. Summary

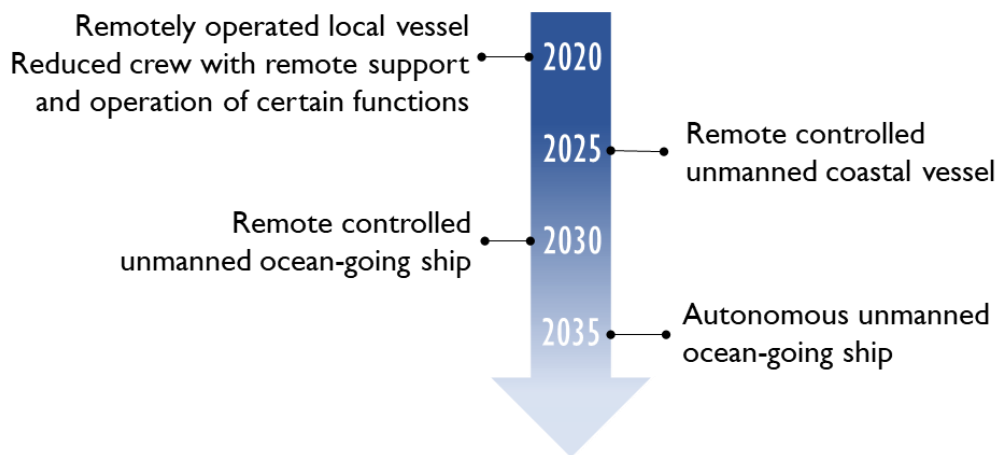
The digital transformation of the maritime industry fully underway. The exploration of the five main service domains of the IoS has shown the limitless complexity of the technologies and systems that enable the modern maritime transportation system. The supply chain stretches from land-based offices to satellite services, all the way to geographically isolated offshore systems. Dangers lurk at every intersection and we aimed to highlight issues in the critical and most common technologies and functions for maritime users.

4. Maritime Cybersecurity

The previous sections demonstrated that the maritime sector takes advantage of many cyber-technologies to operate safely, efficiently and reliably. Unfortunately, computer systems and components are inherently vulnerable and constitute potential risks to the safety and security of humans, assets, and the environment (United States Coast Guard, 2017). This section looks at different aspects of cybersecurity to help identify and mitigate these risks in a systematic way.

4.1. Economic Opportunities

Research and development into unmanned shipping is led by the project MUNIN (Maritime Unmanned Navigation through Intelligence in Networks The MUNIN Research Project (2016) and Rolls-Royce, who aim to deliver the first remote-controlled ships for commercial use by 2020, with self-steering vessels on international waters by the year 2035 (Rolls-Royce, 2016). The development of autonomous shipping is primarily focussed on optimised use of ship space, crew, and resources. Initially only supplementing the traditional functions, autonomous technologies will bring a range of direct and indirect benefits to the shipping sector, and transform the way shipping businesses operate (Allianz Global Corporate & Specialty, 2017). Rolls-Royce claim that their research and development progress is promising to deliver a remote-controlled ship for commercial use by 2020, with autonomous vessels on international waters by the year 2035 (Figure 20).



Source: Adapted from Rolls-Royce (2016)

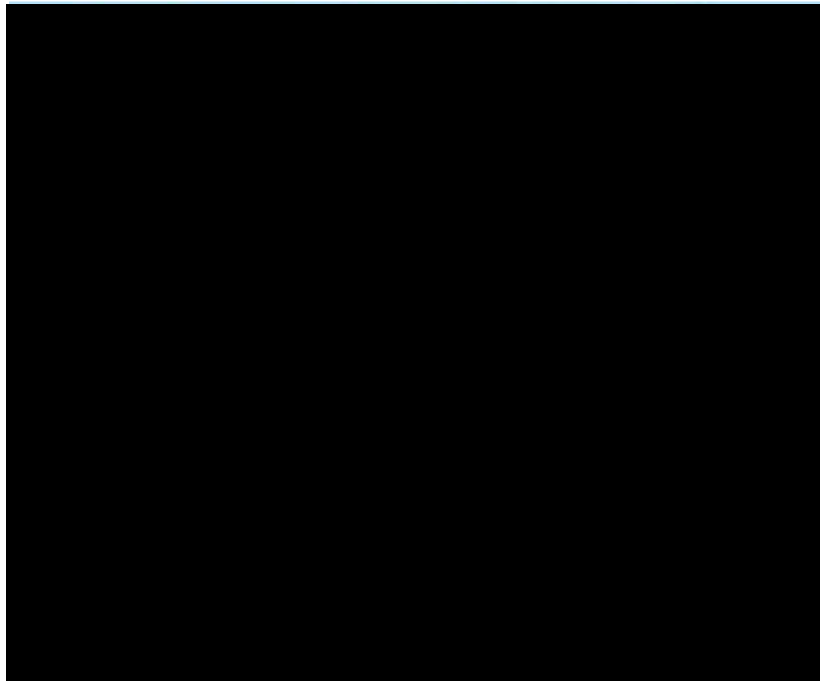
Figure 20 Autonomous shipping milestones

The AAWA project (Advanced Autonomous Waterborne Applications Initiative) is a cross-sector collaboration led by Rolls-Royce. It is exploring the areas of sensor fusion (integrating various sensor technologies), control algorithms (decisions based on sensory data), and communication and connectivity (capacity for sensor monitoring and remote control). The initiative also aims to guide the industry in cybersecurity and risk management approaches, which are both crucial to the safe and successful operation of autonomous vessels (Rolls-Royce, 2016).

These transformational technologies will enable a greater understanding of the ocean and a more economic, efficient, and environmentally sustainable usage (Shenoi et al., 2015). However, there are great uncertainties for future developments as current regulations are constantly struggling to catch up with the technological progress.

SAFETY4SEA, a pro bono initiative "fostering Safety Excellence & Sustainable Shipping"⁷, surveyed maritime stakeholders to understand the industry's perception of the 'smart' era and its challenges and opportunities. The survey found that digitisation in the shipping industry is "imminent" and that, apart from building skills in new technologies, stakeholders are primarily concerned about new cybersecurity challenges (Figure 21).

The industry is already perceived to be vulnerable to cyber threats, and the study showed that awareness is increasing. Most maritime stakeholders understand the importance of adequate crew training and familiarisation with systems to ensure the safe and secure operation on board (SAFETY4SEA, 2017).



Adapted from (SAFETY4SEA, 2017)

Figure 21 The 5 top-rated challenges for Smart Ships

4.2. Cyber Risk

The maritime community routinely manages “traditional” risks to the Marine Transportation System (MTS) to protect its infrastructure and people. The risk related to cyber technology plays an increasingly important role, as the disruption of any of the vital systems can lead to significant loss of life, environment, and property (Marsh & McLennan & Global Marine Practice, 2014; United States Coast Guard, 2015). Risk management is crucial to sustain a safe commerce

⁷ <https://www.safety4sea.com/>

environment and to protect a nation’s security and sovereignty. A global, strategic and technology-agnostic approach to risk governance and information exchange will benefit all maritime stakeholders and improve general readiness and resilience (International Risk Governance Council, 2011; Online Trust Alliance, 2016).

4.2.1. Risk assessment

Different cyber-systems on board a ship require different levels of protection (United States Coast Guard, 2015). For example, the disruption of the entertainment system has less severe consequences than the outage of the propulsion management and control system. Organisations must be able to identify and map out all of their systems to prioritise the security efforts and resources appropriately (Byres & Cusimano, 2012). Organisations must identify all physical and logical information assets and their sensitivity to guide resources to protect them. The information asset inventory is instrumental to establish a risk management plan which is the foundation of a solid, risk-based strategy. See Table 10–Information asset inventory sample. It provides types and examples of assets that may be of interest to attackers. Adversaries target different cyber systems based on their motivation. Both threat actors and their possible goals are detailed in Section 4.5.

Table 10 Information asset inventory sample

Type	Examples
Information assets	<ul style="list-style-type: none"> • Personal information: credentials, financial data, health records, etc • Confidential information: Client data, contracts, processes, plans, blueprints, etc • Operational information: Data integrity, networks, etc • Business information: Competition, competency, reputation • Money: Financial data, payment terms, processes
IT assets	<ul style="list-style-type: none"> • Network infrastructure and endpoints (physical devices) • Webservers, applications • Devices, sensors, process control equipment • Personnel

Sources: (American Bureau of Shipping, 2016b), (Hudson Analytix Inc, 2017)

4.2.2. Risk rating

As part of the risk assessment, the “Impact” rating expresses the degree of damage or costs caused by an event. The rating is subjective to the organisation and should be determined in consultation with stakeholders from different levels, e.g. managers, operators, safety advisors, and technical personnel. This input is important to cover all aspects of the organisation. Table 11 gives a sample of a risk assessment worksheet. For each risk scenario, a severity-score is assigned for the impact and the likelihood for an event to happen. The overall risk-rating for a scenario is based on these two evaluations.

Considerations for the evaluation of impact and likelihood include:

- Types of breaches (e.g. loss of confidentiality, availability, or integrity)
- Classification levels of assets (based on sensitivity and restoration effort)
- Reputational damage to the organisation
- Effects on customers, business partners, employees, suppliers
- Legal, regulatory, or contractual requirements as result of an incident
- Impact on operations and effectiveness
- Financial losses
- Effect on the environment

Table 11 Sample risk assessment worksheet

Risk	Threat actor	Vulnerability	Existing safeguards	Impact	Impact	Likelihood	Risk rating
Stored data (e.g. logs, programs) intentionally modified through local access	Malicious insider	Lack of screening and access control	<ul style="list-style-type: none"> • Personnel screening • Access control logs • Offsite backups 	<ul style="list-style-type: none"> • Economic loss • Safety compromise • Denial of service 	Medium	Low	Low
Malware enters control system through remotely connected computer	Negligent employee	Remote access, no antivirus protection, lack of training/awareness	<ul style="list-style-type: none"> • Antivirus on remote access clients • VPN server, verification of client antivirus status 	<ul style="list-style-type: none"> • Economic loss • Product safety • Loss of reputation 	High	High	High

Source: Adapted from Byres and Cusimano (2012)

4.2.3. Risk mitigation

Activities to control and reduce risks include limitation, avoidance, acceptance, or transferal:

- Limit risk: Enable all possible protection measures to limit the impact of an event
- Avoid: Cease the risk activity
- Accept: Monitor risk and accept consequences of events
- Transfer: Pay a third party to cover the costs in the event

The *cyber-insurance* industry itself represents a risk to maritime stakeholders, due to the uncertainty of the roles and responsibilities and the ongoing debate about what is and what is not covered (Marsh & McLennan & Global Marine Practice, 2014). The purpose of Section 4.7

(Building Resilience) is to provide measures to limit and mitigate the risk of attacks on maritime cyber-system and infrastructure.

4.2.4. Incident reporting

The cyber-threat to maritime infrastructure is real. However, the general lack of disclosed incident data is alarming because it is necessary for a comprehensive analysis and accurate risk evaluation. Organisations are either unaware of the compromise, they try to avoid reputational damage, or they are unfamiliar with a trusted, secure unified reporting platform.

The Australian Government established the Trusted Information Sharing Network for Critical Infrastructure (TISN) in the year 2003 to *“provide a secure environment for critical infrastructure owners and operators across eight sector groups to regularly share information and cooperate within and across sectors to address security and business continuity challenges”* (Attorney-General's Department, 2017). Airbus Defence and Space has recently partnered with the CSO Alliance Maritime and built a secure online reporting portal⁸ to help counter maritime crime on a global scale (Port Technology, 2017).

4.3. CIA

To put this research in the context of Information Systems Security, we consider the *CIA*-triad and group the main threats into the categories "Confidentiality", "Integrity", and "Availability" (Singer & Friedman, 2014):

Confidentiality: Access to information assets is only granted to users with the clearance. Attacks on Confidentiality typically aim to monitor the network or exfiltrate sensitive data, e.g. financial statements or personnel records.

Integrity: Information must be protected to ensure systems and people can rely on its accuracy. Attacks on Integrity intend to alter the user's awareness or interfere with physical systems that depend on information systems or assets.

Availability: A system, function, or information asset must be accessible when it is required. Attacks on Availability impair the flow of legitimate traffic by flooding the system with malicious traffic or noise. These “denial-of-service (DoS)” attacks also refer physical sabotage or shutdown of systems that prevents legitimate users from accessing the system.

For example, GNSS Jamming prevents the receiver from obtaining legitimate information by overpowering the signal with electromagnetic noise. This equates to a loss of availability of PNT data which could mean that electronic navigation cannot be trusted and instead the crew relies on visual aids and

⁸ <http://www.csoalliance.com/page/the-vision>

Table 12 outlines further attacks targeting the confidentiality, integrity, and availability of maritime information systems.

Table 12 CIA threats to PNT information systems

Confidentiality	Integrity	Availability
<ul style="list-style-type: none"> • Unauthorised access through unsecured connections and devices • Unintended revelation of ship/cargo location data • Impersonation of authorities and other third parties 	<ul style="list-style-type: none"> • Unreliable coordinates displaying and broadcasting false position • Incorrect timing data impacting IT network synchronisation and certificate-based authentication 	<ul style="list-style-type: none"> • Sensor blackouts • Triggered false alarms • Losing track of cargo and other assets • Control of central servers and networks • Gain access to port, schedule, cargo data • Exfiltrate, manipulate, destroy databases

4.4. Challenges

The greatest challenge for resilient shipping companies is to securely manage large, geographically distributed networks and assets. They are often located in remote locations, may rely on wireless communications links, and have control channels run over public networks. The threat of an attack via these channels is realistic, but it is much more likely for an employee to be negligent and plug a malware infected USB drive into a PC that is connected to the network.

The following section (summarised in Table 13) will look at cybersecurity challenges from a systemic, human, and technological perspective. The convergence of IT and OT environments is unavoidable, thus many of the challenges relate to this development. This baseline will help to focus on critical areas and to prioritise actions to mitigate the risk.

Table 13 Systemic, human, and technological challenges⁹

Type	Challenges
Systemic	<ul style="list-style-type: none"> • Greater scope and physical consequences • Historical separation of knowledge and skills • Different priorities (CIA vs CAIC) • Budget constraints and management buy-in • Incident reporting • Market restructuring • Offshore reliance

⁹ Sources:(Eisenhauer, Donnelly, Ellis, & O'Brien, 2006; Gregory-Brown, 2017; Gregory-Brown & Harp, 2016; Healey, Meckler, Usen, & Cottle, 2016; ICS-CERT, 2016; National Institute of Standards and Technology, 2014)

Type	Challenges
Human	<ul style="list-style-type: none"> • Unawareness of threats and lack of training • Lack of trust in each other • Historical separation of mindsets • Skills shortage
Technological	<ul style="list-style-type: none"> • Legacy systems and protocols • Fear of breaking things • Outages and performance • Logging is hard • Remote locations – Communication • Remote locations – Physical security • System accessibility • Growing risks from increasing interconnectivity, interdependency, and complexity • Lax control of access control • Online resources

4.4.1. Systemic challenges

Systemic challenges relate to issues that are common across an industry or research area. Systemic challenges of maritime cybersecurity include:

- **Greater physical consequences:** While IT security is exclusively concerned with digital assets, shipping operators control a cyber-physical environment. Consequently, the (accidental or intentional) loss of control over the system has a greater effect on real world – it can cause the damage of equipment, the loss of lives, or ecological damage.
- **Historical separation of knowledge and skills:** IT and OT technologies were developed for separate purposes. Protocols and technologies have evolved in different directions, which led to the siloing of knowledge and control in each sector.
- **Different priorities (CIA vs CAIC):** Control and Availability are of utmost importance in the OT world. This fact must be considered in the allocation of security resources, but most importantly, incorporated the risk management plan.
- **Budget constraints and management buy-in:** Maritime executives are now understanding the importance of cybersecurity and generally allocate a separate budget. The operational business units were traditionally responsible for the physical security of their assets. There was no need to include resources for cybersecurity, because OT systems were not connected to the outside world and thus not targeted. Now that OT is blended with IT and thus exposed, the cybersecurity budget needs to be extended to allow appropriate resources for both environments.
- **Incident reporting:** Information about past incidents allows teams to learn lessons and allocate resources to better prepare for a similar event. Unfortunately, organisations only share their breach data reluctantly, out of fear of reputational or legal consequences. Thus,

very little incident data is available on attacks to analyse and draw conclusions from. Security architects face the great difficulty to quantify and demonstrate threats to the executive suite.

- **Market restructuring:** The development of new and smart technologies, and their integration with current systems will inevitably change the face of the shipping market. The introduction of new products, vendors, and suppliers naturally extends the risk surface for maritime stakeholders as there are more potentially unsecured links in the supply chain.
- **Offshore reliance:** An OT environment consists of hardware and software from vendors from many different countries of origin. The foreign ownership of a manufacturer always presents a risk from the influence of nation-states. They may force the vendor to build mechanisms into their products that allow the nation-state to exfiltrate valuable information. Foreign ownership may also infer that maintenance and support availability might become an issue.

4.4.2. Human challenges

Human challenges relate specifically to the fallacies of human nature and the issues associated with people at the intersection with systems and data. Human challenges include:

- **Unawareness and lack of training:** Cybersecurity simply is not high enough on the agenda of shipping operators and engineers because their main concern is the uninterrupted operation of the vessel. Their systems never used to have connections to external networks. Hardware, software, and protocols were designed for simple, local and fast connections with no contingency for encryption or authentication. The attention of operators and engineers must now be drawn to the increased risk and the threats introduced to their environment. Furthermore, OT and IT staff should receive combined training to understand the necessity for a coordinated approach to network security between business and control systems.
- **Lack of trust in each other:** IT and OT staff are forced to work together, but they do not necessarily have the time or interest to understand what kind of skills and responsibilities the work of their counterpart entails. The lack of knowledge about the other department often causes uncertainty and distrust. Trust, however, is a crucial element of security and needs to be addressed at the socio-cultural level of the organisation.
- **Historical separation of mindsets:** IT professionals and OT specialists “speak” different languages (programming, protocols, priorities), which often makes communication difficult and leads to teams working independently rather than collaboratively. Often, boundaries and responsibilities are unclear. Consequently, less attention is paid to securing the communications interfaces between both environments. Figure 22 illustrates this issue.
- **Skills shortage:** Cybersecurity professionals are already in high demand by industry and government. OT cybersecurity is still in its early stages and if there is a budget for a dedicated position, organisations are unsure what to look for in candidates. There are dramatic differences to IT in training, roles and responsibilities. It is important to foster a collaborative environment where IT and OT specialists can be trained to secure their domains and understand the value of exchanging knowledge that can help their counterpart to help them.

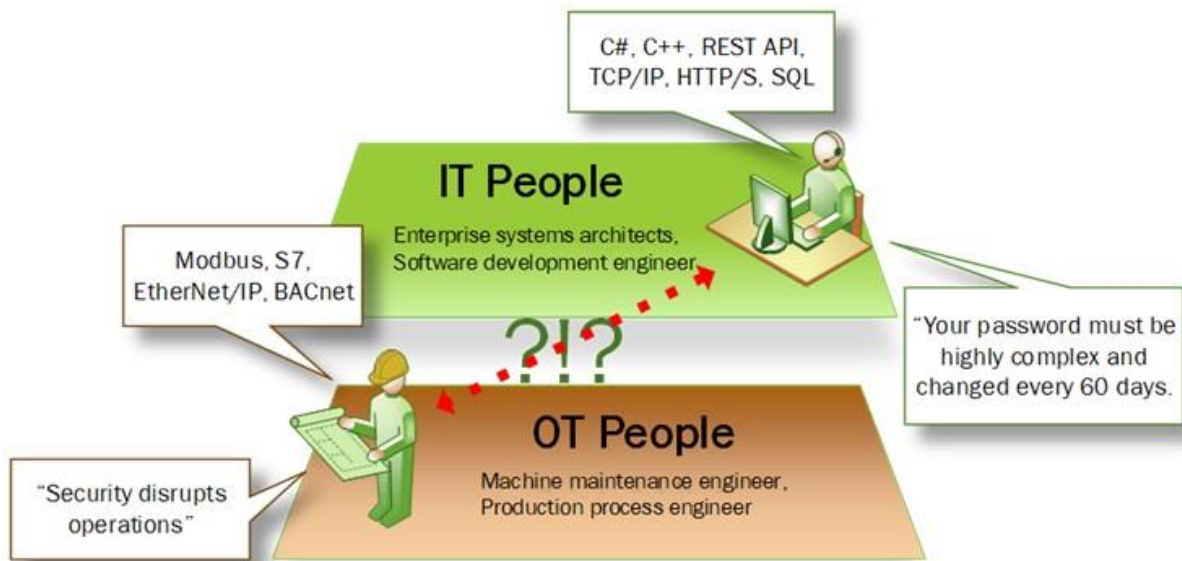


Figure 22 IT vs OT people

4.4.3. Technological challenges

Technological challenges also arise at the intersections with humans and data. The major issues are:

- **Legacy systems:** Components in OT systems are built to last for the lifetime of the system. Typically, they are not compatible with modern (secure) operating systems and their firmware cannot be upgraded. Flaws in legacy systems are much more broadly published and thus easier to exploit. As the demand for real-time control and remote management of SSS increased, networking protocols (TCP/IP) were simply added to provide this interconnectivity. These systems are now exposed to the connected IT network and the internet and remain vulnerable unless there is a protection mechanism in place.
- **"Fear of breaking things":** OT systems are so reliant on uptime that many IT security professionals are afraid to pressure-test them. The focus of cybersecurity has been on IT systems, and there are many testing methodologies and tools available today. The security industry is yet to develop and refine non-intrusive scanning tools for testing OT environments.
- **"Logging is hard":** The devices, sensors, and components used in control systems are made for very specific purposes and designed to be as lightweight as possible. By default, the components don't have the processing power or storage capacity to keep logs of all security related events.
- **Outages and system stability:** OT systems cannot easily be taken offline, because the chain reactions might be unpredictable. It is difficult to update or patch live systems, unless there is a redundant failover system in place. Security tools must undergo exhaustive offline pre-deployment testing to ensure the continued uptime. Change or configuration management

processes are imperative as to not disrupt the operation of the vessel. Attacks on maritime critical infrastructure have cascading impact on physical systems. Failure in one sector can impact others, cause widespread economic damage.

- **Unsecure communication:** Many OT components of the SSS and IoS are remotely located or otherwise difficult to access. This raises multiple concerns regarding the security and the ability to connect to the asset via unsecured communications channels. In areas where 3/4G coverage is unavailable, technicians can only choose between satellite and two-way radio communications. Both are highly susceptible to interference and jamming, but an attacker can also intercept communications and inject malicious commands.
- **Access control:** IT systems administrators want to see what is going on in the network and limit that activity to approved transactions. The increasing convergence of IT and OT systems requires more users to access parts of both environments. This is often granted “ad-hoc”, without regard for principles of information security such as the “Separation of duties” or “Least privilege”. Often, login credentials are simply shared among groups, especially when elevated system access is required for a particular task. This is a recipe for disaster. It makes it impossible to retain the oversight and control over the application of permissions.
- **Growing risks from interconnectivity, interdependency, and complexity:** Connections between business- and control networks are often poorly designed to integrate systems that have been historically separated. Converging IT and OT environments also extend the scope of vulnerabilities and the consequences of an attack. A multitude of systems could be accessed through a single misconfigured router or modem.
- **What is perceived to be less critical, is secured less strictly.** For example, a trusted subcontractor may not be viewed as a threat to the security of the vessel. But it is possible that they use a common workstation to check their personal emails, and accidentally click on a malicious link and infect that workstation. If that computer is connected to any internal network, the virus could spread to the connected business or control systems and cause outages with disastrous consequences.
- **New components and technologies** are often introduced into the environment while trying to secure legacy systems (“Industrial Internet of Things – IIoT”). These devices have proven to be poorly secured “out-of-the-box” and they have the potential to interfere with operations as soon as they are installed. Smart components should be reviewed extensively and configured to best practices prior to adding them to the delicately tuned composition of existing elements.
- **Online resources:** The internet gives access to a great wealth of information on current and legacy OT components. This includes user manuals, training material and videos, but also blueprints, default configurations and credentials and tools that can be used to prepare and plan attacks against the IoS or SSS.

4.5. Threat Actors, Targets and Motivation

A threat actor is an entity with the intent to exploit a vulnerability or conduct an attack against a cyber system (Edgar & Manz, 2017). An understanding of the separate groups of threat actors will help to assess an organisation's risk exposure. The "2017 Cost of Data Breach Study" (Ponemon Institute LLC, 2017) found that close to half of the reported data breaches (cyber incidents) were caused by malicious entities(47%). The remainder was attributed to human errors, system glitches, and failures in business processes.

Threat groups with a vested interest in the maritime domain are:

- Competitors, industrial spies
- State-sponsored hackers
- Individuals/opportunists
- Disgruntled employees
- Insiders and saboteurs
- Criminal organisations
- Activist groups
- Foreign intelligence
- Terrorists

Each link within the organisational network and the supply chain is a potential hole for the intruder. Some organisations are more vulnerable than others, but the wide range of target groups within the maritime community include:

- Vessel owners and operators
- Ship management firms
- Port terminal operators
- Logistics companies
- Customs agencies
- Port state control
- Manufacturers
- Contractors
- Suppliers
- Navy

The main incentives for attacks on maritime organisations are money, information, and sabotage. Adversaries perceive the maritime domain as an easy and worthwhile target as stakeholders routinely transfer substantial amounts of money between each. Especially in the ship-to-shore environment, a wealth of information is transmitted across many different channels (North P & I, 2016). The main motivators for attacks are:

- Financial gain
- Disruption/sabotage
- Revenge/reputational damage
- Espionage (political/industrial)
- The challenge of breaking cyber defences
- Reconnaissance for sophisticated crimes
- Political/environmental activism
- Military engagement

Operators and administrators of maritime systems must keep track of countless combinations of legacy and current technologies, topologies, protocols, and communication modes on board. Each system component on board has its own set of potential flaws which give an intruder a wide range of options to gain unauthorised access to the ship's network. Many organisations are astonished that seemingly insignificant security flaws can lead to great rewards for the attackers and disastrous consequences for the victim (asymmetry of attacks).

4.6. Vulnerabilities

Vulnerabilities are flaws in a system with the potential to be exploited. The following section analyses the main weaknesses in IoS and SSS and identifies the essential systems and areas of concern. The shipping community is slowly gaining an understanding of cybersecurity processes and technologies, but it will take considerable amounts of time, resources, and effort to improve the security posture across the industry.

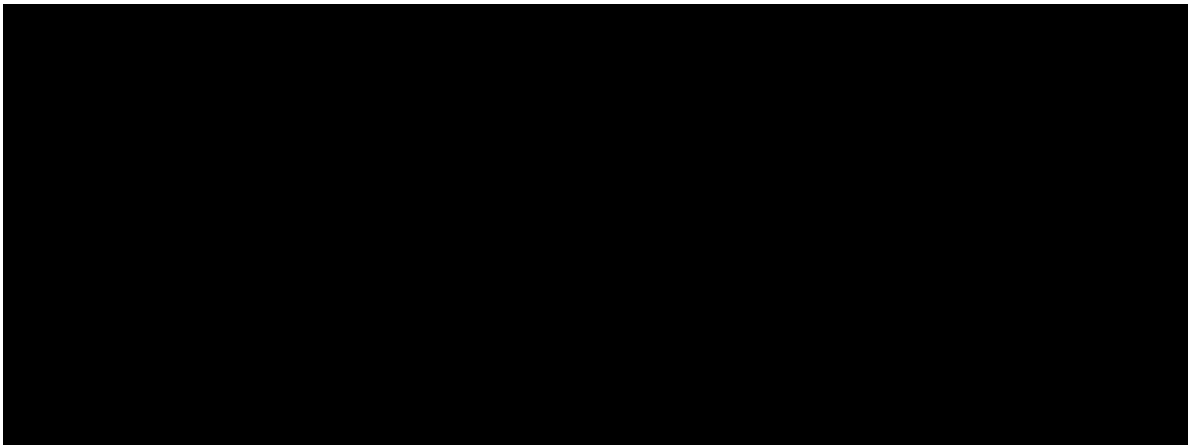
Critical and non-critical systems and services

Not every system on board needs the same level resources to protect them. Risk analysis shows that the severity of impact of an attack can be different from system to system, or from organisation to organisation.

A *critical service* in the maritime context ensures the safety of people, equipment, and the environment. For example, the Global Maritime Distress and Safety System (GMDSS), which is a set of standards and components to aid search and rescue operations for vessels in emergency situations. Each component of the GMDSS (e.g. satcom terminals, AIS transponders) comes with a set of potential vulnerabilities, which are detailed below.

Non-critical services include voice communications, crew welfare and entertainment systems, guest Wi-Fi, and video monitoring. These systems are perceived to be less critical to safety and operations and thus routinely left unpatched and exposed to attacks.

A *critical system* is vital for the safe operation of maritime infrastructure and the security of personnel. A critical system has a “sufficiently severe consequence of failure to justify the proactive effort of protecting it”¹⁰.



Source: Lagouvardou (2018)

Figure 23 Critical and Non-Critical Infrastructure on board

A *vulnerable system* is any system with a susceptibility for exploitation and can potentially offer an entry point for the adversary. In maritime critical infrastructure, vulnerable systems may

¹⁰ <http://www.lgam.info/critical-asset>

include industrial control systems, cargo and terminal management systems, navigational systems and *any other* connected system or service.

The technical nature of these systems exposes vulnerabilities which are not unique to the maritime domain. Many applications still run on obsolete, legacy operating systems (e.g. ECDIS on Windows XP), as the replacement would cause significant compatibility issues, require large-scale maintenance outages, or is simply financially prohibitive. Outdated antivirus software and the absence of a regular patching or update regime can allow an attacker to use malicious techniques which would otherwise not be a threat. This also applies to the inadequate configuration of hardware and software and the ignorance of best implementation practices. Another common oversight is the inadequate network segmentation and access control for third parties (Baltic and International Maritime Council, 2017).

Unfortunately, operators routinely bypass security- and access-control measures when these negatively affect operations. This has been a common observation in mixed IT/OT environments, as laid out in Section 2.4. Many non-malicious incidents are attributed to the physical and mental fallibility of humans. This includes technical input errors as well as the lack of awareness of existing cybersecurity policies. There is a range of cyber risks that are unique to the shipping industry. Table 14 outlines a number of these vulnerable systems.

Table 14 Vulnerable systems on board

Ship-to-shore interface	Onboard systems
<ul style="list-style-type: none"> • Performance monitoring • Maintenance and spare part management • Cargo, crane, and pump management • Voyage performance monitoring 	<ul style="list-style-type: none"> • Cargo management • Bridge system • Propulsion and machinery management • Power control system • Access control system • Passenger servicing and management • Passenger facing public networks • Administrative and crew welfare systems • Communication systems • Core network infrastructure • Security and HVAC systems

Sources: Adapted from (Hudson Analytix Inc, 2017) and Baltic and International Maritime Council (2017)

4.7. Building Resilience

Resilience aims to create and maintain a controlled system for critical applications to survive a cyber-attack with no loss of critical functionality. Resilience refers to a multi-layered approach to improve a systems resistance against human error, interference, and other sources of disruption.

As part of building resilience, “Cybersecurity” is a continuous process rather than a one-off project. It offers many tools and techniques that must be tailored to the organisation and seldomly provide value “out-of-the-box” without internal skillsets or expensive consultants. This section hopes to clarify that building resilience begins with taking a step back and viewing the organisation from multiple angles. A company must identify and evaluate risks in the context of the company, the industry, and the rest of the world. This understanding is important to develop strategies and budgets to protect the organisation from cyberattacks. The frameworks explored in Section 4.2 are very good starting points for maritime executives to analyse the cybersecurity posture of their organisation compared with the overall posture of the industry.

Taking steps improve resilience is to understand where the security issues in IoT ecosystem and SSS are possible and likely. It is critical to identify all systems that exchange data assets with each other and external interfaces. Any third-party with access to the network (e.g., for remote maintenance, event monitoring and resource planning) is a potential entry point for an attacker. External access permissions should be kept to a minimum and reviewed regularly.

Many security issues are found on the smart ship itself. The vessel’s subsystems are highly integrated and dependent on each other. Despite the fast adaptation of IoT capabilities on vessels, it is crucial to retain control over all devices on the network. Any rogue endpoint could potentially be exploited and used to further pivot through the entire network. Cybersecurity must be integrated in all operations in the way that systems are implemented to comply with occupational health and safety regulations and standards.

The remaining sections explores different approaches to improving organizational resilience against cyberattacks.

4.7.1. Defence in Depth

Cybersecurity is neither a product that can be bought off the shelf, nor a procedural blueprint that every organisation can apply in the same way. Securing maritime cyber-environments “in depth” means considering all aspects of the organisation, including governance, human security, physical security, network security, data security and building protection around each of the these layers. A layered approach includes procedural and technical countermeasures is summarised in Figure 24.

It at the organisation’s top level, where *strategies* are formed, and *policies* are created. *Physical security* prevents intruders from entering the vessel by using guards, locks, alarms, and technical access control. *Perimeter security* refers to measures which block attacks from entering the network through external communication connections. *Internal network security* is concerned with the design, configuration and implementation of security zones, network segments, and other network-based defences. The layer of *Host security* protects computers and other endpoints with

measures such as antivirus software and host-based firewalls. *Application security* prevents attackers from exploiting software flaws and entails secure software development, authentication, access control, and application vulnerability management. Finally, the *Data security* layer addresses how to protect the information itself, whether it is in use, in transit, or at rest. Each layer plays a significant role in the overall security of maritime critical infrastructure.

4.7.2. Security policies and procedures

The most important security asset on board is a vigilant employee. Policies and procedures give staff the necessary tools and guidance for their critical role within the organisation. Training and awareness programs enable staff to understand why, and how each individual can help. Policy and procedural documents should be clearly communicated, published, and acknowledged.

Policies should address how the content will be enforced and what the consequences are if ignored. The documents should be reviewed regularly to ensure they appropriately cover the organisation in a world of continuous technological advancements.

The policies should address and explain at least the following:

- Data recovery capability, backups, redundancy, business continuity and disaster recovery planning
- Administrator privileges, concepts of least privilege and the separation of duties
- Remote access control, use of encryption and Virtual Private Networks (VPN)
- Physical access, removable media controls, “Bring your own device” (BYOD)
- Acceptable personal use of IT systems
- Email, phishing, passwords rules
- Software upgrade, patch, and maintenance schedules
- Anti-virus/-malware software and signature updates
- White- or blacklisting and the use of third-party software
- Onshore support and contingency planning
- Equipment disposal, and data destruction



Source: Adapted from Effendi (2015)

Figure 24 "Defence-in-depth" layers of security measures

4.7.3. Training and Education

Policies and processes reflect the rules that protect the company as well as the employee. There is no value unless the employee is also equipped with the right tools and knowledge to follow these rules. Security Education and Awareness Training (SEAT) programs are essential and must be tailored to all levels of employees – from reception, dispatch, line managers, executives – all are in contact with different parts of the information system.

However, training staff around complex policies and procedures for equipment they have no contact with may be counterproductive. General cybersecurity awareness should be part of each employee's induction and cover passwords, email-security and phishing, updating and patching, personal antivirus and firewalls, installation of software, and personal mobile devices.

In addition, each department or group of employees should be aware of the risks associated with the software and procedures they use to perform their tasks. For example, administrative staff should be aware of malicious macros in office applications, engineers should know how to safely use USB-drives to update isolated systems, network administrators should know how to recognise and respond to network threats, while executives should understand how to encrypt a document folder or send a secure email.

Providing employees with clear teaching objectives and cultivating a sense of ownership over the relevant system components' cyber security can provide more resilience than thousands of dollars' worth of flashing equipment that is misconfigured or not poorly understood. It might be worth identifying interest and talent in-house and to build cybersecurity capability by rewarding staff with sponsored industry certifications and promotions.

4.7.4. Vulnerability Management

Planning for vulnerability management includes security assessments which can identify systems and assets that are susceptible to exploitation. All potential threats are recorded in a database and updated as new flaws are discovered.

Vulnerability monitoring includes log reviews from intrusion detection systems, firewalls, antivirus programs, or access control systems. The results obtained through monitoring should be regularly analysed to prepare defenses and minimise the impact should a vulnerability be exploited. Vulnerability management is responsible to find and apply updates and patches to mitigate any risks of exposure. Each discovered vulnerability and fix should be documented and updated in the vulnerability database. Tools for vulnerability management are available from Open Sources and from commercial providers (Goel et al., 2012).

Vulnerability assessments take a snapshot of a system and analyse it based on the knowledge and methods available at that particular point in time. Attack methods evolve, and new vulnerabilities are discovered over time, thus the protection strategy should be dynamic and reviewed on a regular basis. While there are technical differences between vulnerability assessments and penetration tests, both can be part of an overall *security audit*.

Vulnerability assessment: Enumerates, identifies, and reports noted weaknesses in a system, and provides recommendations to mitigate the associated risks.

Penetration test: Actively attempts to duplicate methods of an internal or external attacker, gaining access to the system. Gives insight to systems’ and security team’s ability to withstand an attack.

Awareness of the challenges outlined in Section 4.4 should lead decision-makers to allocate attention and resources to the protection of critical systems on SSS. The supply of skilled OT security providers low and even though IT security specialists are already in demand, transferring their skillset to testing OT environments is an entirely new challenge.

Common testing methodologies must be well adjusted and new tools must be developed to suit the unique requirements of IoS and SSS environments. The adoption of digital technology is certainly going to expand in the future and shipping companies will recognise the severity of the risks that they are exposed to.

In summary, testing in the domains summarised in Table 4 should be considered to develop a comprehensive view of the organisation’s security posture. A security specialist should be able to demonstrate different attack scenarios, build threat- and risk models, and perform compliance audits. Emphasis must be placed on a rigorous and repeatable testing schedule.

Table 4 Layers of depth of vulnerability assessments

Security domain	Testing considerations
Policy and Human security	<ul style="list-style-type: none"> • Interview key personnel • Update and upgrade management review • Incident Response, Business Continuity, Disaster Recovery plan • Change management process • OT security policies and procedures, including local and domain user policy and implementation, • Removable media and BYOD policies • Password policy and usage, including derived information (hashes, salts), create passive dictionary of common passwords
Physical security	<ul style="list-style-type: none"> • Visual inspections of premises • Camera locations, door locks, secure windows, etc. • Wireless access point (AP) tamper proofing • Physical access to workstations/servers • Security cabinet and telecoms equipment • Quality of industrial-grade equipment • Access logs
Perimeter access	<ul style="list-style-type: none"> • Remote access methods, protocols and techniques • Access control (logical and physical) to ICS servers, windows domain access, local field access, engineering key management, application access and usage, maintenance laptop etc • Wireless AP survey to detect unsecure Wi-Fi setup (typically used for uncritical field devices) and rogue Aps

Security domain	Testing considerations
	<ul style="list-style-type: none"> Review any external connections to third parties (e.g. remote maintenance)
Network	<ul style="list-style-type: none"> ICS/SCADA/OT interconnections to Business network Networking and security device configuration (routers, switches, firewalls, IDS) Firewall rules Servers (DCS, SIS, SCADA, DMC, Historian, etc) Analyse management interfaces to PLCs, managed switches, routers Identify vulnerable network services Network segmentation (controllers, servers, workstations, sensors/actuators) Check backup network Check undeclared protocols in control segments
Host	<ul style="list-style-type: none"> Endpoints (HMIs, engineering/operator workstations, ICS clients, etc.) Embedded computer/controller (flow computer, PLC, RTU, DCS controllers, etc.) Field devices (RTU, HART devices, ModBus devices, IED) Workstation accounts and administrator privileges, including review of security levels (privilege creep) Access via wireless and remote access technologies OT interaction with external systems ICS internet connectivity
Application	<ul style="list-style-type: none"> Application and interface vulnerability assessment Do vulnerabilities allow to pivot through to critical services Level of antivirus protection Use of third-party or pirated software
Data	<ul style="list-style-type: none"> Network traffic analysis, find data leaks, plain text transmissions

4.7.5. Technical security solutions

Policies require technical implementations to be monitored and enforced. For example, locks and security cameras protect equipment from unauthorised access and use. Secure network devices configuration separates parts of the network to prevent the direct exposure of SSS to the internet. Further examples of technical security solutions on board are outlined below:

- Firewalls and intrusion prevention systems monitor and block the data traffic as it leaves and enters the ship’s IT network.
- The dataflow between all nodes on the network, including ICS traffic and satellite and radio communications, should be mapped out and encrypted, e.g. by using a VPN. This way, even if signals were intercepted, the adversary could not easily read the message.

- Network hardening refers to the secure configuration of hardware and software and the deactivation of unused features and accounts. It applies to firewalls, routers, switches, servers, voice communication equipment, and any other device on the network.
- Hardening includes disabling unused ports and services but also managing and installing updates, patches and bugfixes.
- Default usernames and passwords must be changed where possible. The use of complex passwords protects against automated port-scan and dictionary-based login attempts, for example on the VSAT terminal.
- Access control systems should be configured and audited regularly to only allow users the access rights they need to perform their job.
- X.509 certificate-based authentication can secure the access to the ship’s wireless network for authorised crew members and guests.
- It is recommended to create a separate wireless network (Virtual Local Area Network – VLAN) for guests to allow only minimal access to resources on the network.
- The usage of secure communications protocols like ssh, https, and sftp should be implemented and enforced where it is possible. Multi-Factor Authentication (MFA) can provide an additional layer of access security to sensitive systems and applications.
- Application whitelisting prevents staff from installing unapproved and potentially malicious programs.
- The threat of intentional or accidental data leakage can be mitigated with data-loss-prevention software

(Mertens, 2014; Shoultz, 2017; Soullie, 2014a).

4.8. Summary

To keep up with the incredible fast pace of technology development, vendors typically favor a fast “time-to-market” over the appropriate design and implementation of security features in their products (e.g., Secure Software Development Lifecycle – SSDLC). This does not encounter any opposition from consumers, since their primary concerns are performance, up-time, real-time control, and ease of use – but not security.

The impending manifestation of the IoS will expose an entire new economy to IT and OT cybersecurity threats. An early shift of ideology and awareness-culture is the most critical factor to counter these emerging threats. The complex supply-chain connectivity is an uncharted territory for most maritime stakeholders, but the methods used by cyber criminals are similar. They only need to adapt to the new opportunities and learn a few new skills.

The current passive approach is highly unlikely to withstand a determined attempt to interfere with the technology on smart ships and the weak links within the supply chain. Humans are still the most important cause and target for network intrusions and must be educated, guided and

penalised accordingly. Work procedures should be examined to address weaknesses and inform policies.

These policies should be clearly communicated and understood. Crew members should receive regular training on cybersecurity awareness and learn how to protect themselves and the technology on board. Security policies and procedures must be ingrained in the organisational culture to best ensure the resilience against cyber-crime. The fusion of traditional IT and OT and the resulting vulnerabilities must also be addressed with high priority. Engineers on both sides must learn to understand the differences in priorities and how to align them with the mutual goal of a secure vessel.

5. Conclusion

The current state of technology allows shipping companies to participate in the global digital economy on an entirely new scale. The maritime domain can benefit from terrestrial-like economics to enhance safety, efficiency and convenience for passengers and crew members (Bhatia, 2007). Modern satellite systems (HTS – High-Throughput Satellites) can provide download speeds of more than 100 Gbps nearly anywhere in the world (Vasavada, Gopal, Ravishankar, Zakaria, & BenAmmar, 2015). Even though these speeds exceed most current requirements, satellite broadband internet will soon be the norm on vessels – supporting applications from remote maintenance and environmental monitoring to social media, streaming and video conferencing. Satellite-Internet- and hardware-providers market their products aggressively and attract customers with affordable products and flexible plans. Many satcom devices like VSATs have a small footprint and a great range of functionality.

However, with great opportunity comes great risk, and as this research has shown –there is no device or system that has been tested and is completely free of cybersecurity issues. New technologies are developed at such rapid pace that manufacturers routinely disregard standards and best practices in order to get to the market quick. This turns into a burden for the consumer and operator who must spend the extra time and resources to outside of their regular business to understand and protect these technologies.

This dissertation has explored two complex layers of maritime technology – the shipborne systems and the maritime cyber ecosystem.

“Smart” devices with wireless connectivity play a great role to enable the maritime digital transformation and manifest the need for vessels to be “online” at all times. Visibility and connectivity are keys for centralised and remote management, and to that end systems and subsystems must be integrated to exchange data with each other. And with increasingly merging IT and OT environments increases the complexity and difficulty to configure these networks and protect it from unauthorised access.

Smart Ship Systems are characterised by the combination of different technology-paradigms and the critical dependence on real-time data for applications that enable safe navigation, communication, and control. Research has demonstrated that manipulated real-time data like PNT can remain undetected and result in Hazardously Misleading Information, which can lead to catastrophic accidents.

Unfortunately, the digital transformation comprises many unknown factors, including novel attack techniques and the behaviour of smart ships under cyber-attack. All “traditional” IT and OT security issues (e.g., malware, phishing, DoS and remote backdoors) are now available offshore. Fortunately, existing land-based cybersecurity models and methods for IT and OT apply just as much at sea. Existing work has shown that the divide between IT and OT knowledge and skills is large and that bridging this divide is vital to minimising the risk of outages, malfunctions, and attacks.

Future Work

While this research shows that there is substantial work to be done to address the many security concerns in IoS and SSS, there is also an increasing appetite for maritime stakeholders to be informed and educated. The cybersecurity industry puts a lot of emphasis on technical solutions for security problems. But it is even more time-critical to ingrain a positive cybersecurity mentality into the maritime community and offer training and awareness programs that are tailored to different IoS service domains and the different roles of an organisation.

It is particularly important to bring both experts from IT and OT departments together to build a common language, understanding, and objective to enable the benefits and minimise the risk of digital integration. Both must be trained to appreciate the different priorities of their environments and the requirements for any data exchange. Neither IT nor OT engineers are security professionals by trade, and therefore simply having more meetings with each other will not improve the organisation's cybersecurity posture alone.

When the organisation's leadership team understands the key areas of concern, it can make informed strategic decisions and embed cybersecurity policy into its governance framework, similar to the policies and processes related to occupational health and safety. This inclusion is important to a) justify resources to mitigate cyber-risk; b) to have a plan in place to respond to incidents; and c) to enforce security rules across the organisation.

In addition to training on technology and security, and a large aspect of future work is to be focussed on incident reporting and sharing. There is nothing of more value than previous experience (e.g. Indicators of Compromise – IoC) to prevent similar attacks in other environments. The perception is that the disclosure of incident data will cause reputational damage, but many organisations are either unsure of their options for responsible, secure disclosure, or simply have no way of knowing whether they were compromised at all. As outlined above, secure reporting platforms exist – and they can only increase in value when more stakeholders are actively contributing.

References

- Abaimov, S., & Ingram, P. (2017). *Hacking UK Trident: A Growing Threat*. Retrieved from <https://basicint.org/portfolio/hacking-uk-trident-a-growing-threat-2/>
- Acil Allen Consulting. (2017). *Australian Space Industry Capability - A Review*. Retrieved from https://www.industry.gov.au/sites/default/files/June%202018/document/extra/australian_space_industry_capability_-_a_review.pdf
- Allianz Global Corporate & Specialty. (2017). *Safety and Shipping Review 2017*. Retrieved from http://www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Safety_Shipping_Review_2017.pdf
- American Bureau of Shipping. (2016a). The Application of Cybersecurity Principles to Marine and Offshore Operations. In *ABS CyberSafety VOLUME 1*. Houston, TX 77060 USA.
- American Bureau of Shipping. (2016b). Cybersecurity Implementation for the Marine and Offshore Industry. In *ABS CyberSafety VOLUME 2*. Houston, TX 77060 USA.
- Attorney-General's Department. (2017). Trusted Information Sharing Network for Critical Infrastructure Resilience. Retrieved from <https://www.tisn.gov.au/Pages/default.aspx>
- Australian Government Space Coordination Committee. (2018). *2017 State of Space Report*. Retrieved from https://www.industry.gov.au/sites/default/files/June%202018/document/pdf/state_of_space_report_2017.pdf?acsf_files_redirect
- Australian Logistics Council. (2010). *Future Freight Networks - The ALC Yearbook 2010* (978 1 921345 16 6). Retrieved from <https://www.austlogistics.com.au/wp-content/pdf/publications/Final-ALC-Year-Book-Future-Freight-Networks-August-2010.pdf>
- Australian Maritime Safety Authority. Automatic Identification System (AIS). Retrieved from <https://www.amsa.gov.au/navigation/services/ais/>
- Australian Maritime Safety Authority. (2013). *Australian Global Maritime Distress and Safety System (GMDSS) Handbook*.
- Australian Maritime Safety Authority. (2017). *Marine Order 63 (Vessel reporting systems) 2015*. Retrieved from <https://www.legislation.gov.au/Details/F2017C00975>
- Australian Maritime Safety Authority. (2018). Automatic Identification System (AIS). Retrieved from <https://www.amsa.gov.au/safety-navigation/navigation-systems/about-automatic-identification-system>
- Australian Maritime Safety Authority. (2019). How distress beacons work. Retrieved from <https://beacons.amsa.gov.au/about/how-they-work.asp>
- Babicz, J. (2015). Wartsila Encyclopedia of Ship Technology. *Wartsila Corporation*, 393. doi:10.1007/978-1-4614-9610-6
- Bai, Y., & Bai, Q. (2019). 4 - Subsea Surveying, Positioning, and Foundation. In Y. Bai & Q. Bai (Eds.), *Subsea Engineering Handbook (Second Edition)* (pp. 81-121). Boston: Gulf Professional Publishing.
- Balduzzi, M., Wihoit, K., & Pasta, A. (2013). *Hey captain, where's your ship? attacking vessel tracking systems for fun and profit*. Paper presented at the Hack in the Box (HITB) Security Conference in Asia.
- Baltic and International Maritime Council. (2017). *The Guidelines on Cyber Security Onboard Ships*. Retrieved from <https://www.bimco.org/-/media/bimco/news-and-trends/news/security/cyber-security/2017/industry-guidelines-cyber-security---june-2017.ashx>
- Bensing, R. (2009). *An Assessment of Vulnerabilities for Ship-based Control Systems*. Naval Postgraduate School, Monterey, California. Retrieved from <http://www.dtic.mil/dtic/tr/fulltext/u2/a508895.pdf>
- Bhatia, S. (2007). *Understanding High Throughput Satellite (HTS) Technology*. Retrieved from http://www.intelsat.com/wp-content/uploads/2013/06/HTStechology_bhartia.pdf
- Bhatti, J., & Humphreys, T. E. (2017). Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation, Journal of the Institute of Navigation*, 64, 51-66. doi:10.1002/navi.183

- Boyens, J., Paulsen, C., Moorthy, R., Bartol, N., & Shankles, S. A. (2014). Supply chain risk management practices for federal information systems and organizations. *NIST Special Publication, 800(161)*, 1. Retrieved from <http://dx.doi.org/10.6028/NIST.SP.800-161>
- Boyes, H., & Isbell, R. (2017). *Code of Practice Cyber Security for Ships*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf
- Bureau of Safety and Environmental Enforcement. (2014). *Assessment of Real-Time Data Monitoring Systems - Presentation of Findings*. Retrieved from <https://www.bsee.gov/sites/bsee.gov/files/tap-technical-assessment-program/707ab.pdf>
- Byres, E., & Cusimano, J. (2012). *7 Steps to ICS and SCADA Security*. Retrieved from <https://www.tofinosecurity.com/professional/7-steps-wp>
- Caparra, G., Wullems, C., Ceccato, S., Sturaro, S., Laurenti, N., Pozzobon, O., . . . Crisci, M. (2016). *Design Drivers for Navigation Message Authentication Schemes for GNSS Systems*. Retrieved from <https://pdfs.semanticscholar.org/1bc8/a37331f3008360c32dd8c07f877bbc926083.pdf>
- Choy, S., Kuckartz, J., & Dempster, A. G. (2016). *GNSS Satellite - Based Augmentation Systems for Australia*.
- Cimpean, D., Meire, J., Bouckaert, V., Vande Castele, S., Pelle, A., & Hellebooge, L. (2011). *Analysis of Cyber Security Aspects in the Maritime Sector*. Retrieved from https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport
- Comsys. (2017). *The comsys VSAT Report - 14th edition*. Retrieved from http://www.comsys.co.uk/wvr_stat.htm
- Comtech Systems Inc. (2014). *Communication Links for Offshore Platforms*. Retrieved from <https://www.comtechsystems.com/wp-content/uploads/2014/05/Communication-Links-for-Offshore-Platforms-2012.pdf>
- Crandal, J. (2018). Cybersecurity and Offshore Oil: The Next Big Threat. *Oil and Gas, Natural Resources, and Energy Journal*, 4, 703.
- CyberKeel. (2015). *Maritime Cyber Risks - Virtual Pirates at large on the Cyber Seas*. Retrieved from https://docs.wixstatic.com/ugd/2d153e_46bd931729324d4b81723567d9e7d288.pdf
- Dechow, N., & Mouritsen, J. (2005). Enterprise Resource Planning Systems, Management Control and the Quest for Integration. *Accounting, Organizations and Society*, 30, 691-733. doi:10.1016/j.aos.2004.11.004
- Deloitte. (2017). *Cyber Security in the Shipping Industry*. Retrieved from <http://forums.capitallink.com/shipping/2017cyprus/ppt/ioannides.pdf>
- Dinning, M. (2014). *Strategies for Maritime Cyber Security – Leveraging the Other Modes, Innovative Technologies for a Resilient Marine Transportation System*. Retrieved from <http://onlinepubs.trb.org/onlinepubs/conferences/2014/MTS2014/Dinning.pdf>
- DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015, 6-8 July 2015). *The little-known challenge of maritime cyber security*. Paper presented at the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA).
- Dobryakova, L., Lemieszewski, Ł., & Ochyn, E. (2014). The main scenarios of GNSS spoofing and corresponding spoofing detection algorithms. *Logistyka*, 4, 2751-2761.
- Dyryavyy, Y. (2014). *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*. Retrieved from <https://www.nccgroup.com/en/learning-and-research-centre/white-papers/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/>
- Easton, R. D. (2013). *GPS Declassified*: Potomac Books, Inc.
- Edgar, T. W., & Manz, D. O. (2017). *Research Methods for Cyber Security*: Syngress.
- Effendi, A. (2015). Managing Cyber Security Across the Enterprise. In N. T. I. S. S. Association (Ed.).
- Eisenhauer, J., Donnelly, P., Ellis, M., & O'Brien, M. (2006). *Roadmap to Secure Control Systems in the Energy Sector*. Retrieved from Columbia, Maryland, US: <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf>
- El-Rabbany, A. (2002). *Introduction to GPS - The Global Positioning System*: Artech House.

- European GNSS Agency. (2016). *GNSS User Technology Report* (9789292060299). Retrieved from https://www.gsa.europa.eu/system/files/reports/gnss_user_technology_report_webb.pdf
- Falliere, N., Murchu, L., & Chien, E. (2011). *W32.Stuxnet Dossier*. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. In: Lancaster University.
- Furuno. (2006). *Operator's Manual - Model VR3000 and VR3000s*. Retrieved from http://haidang.vn/files/news/465/VR3000_VR3000S_Operator_s_Manual-F2.pdf
- Galliers, R. D. (1990). Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy. In H.-E. Nissen, H. K. Klein, & R. Hirschheim (Eds.), *Information Systems Research: Contemporary Approaches & Emergent Traditions*.
- Geoscience Australia. (2016). *National Positioning Infrastructure Capability*.
- Goel, S., Kiran, R., & Garg, D. (2012). Vulnerability Management for an Enterprise Resource Planning System. *arXiv preprint arXiv:1209.6484*.
- Gregory-Brown, B. (2017). *Securing Industrial Control Systems-2017*. Retrieved from <https://www.sans.org/reading-room/whitepapers/ICS/paper/37860>
- Gregory-Brown, B., & Harp, D. (2016). *Security in a Converging IT/OT World*. Retrieved from <https://www.sans.org/reading-room/whitepapers/analyst/security-converging-it-ot-world-37382>
- Hale, M. J. (2007). *Identifying And Addressing Management Issues For Australian State Sponsored CORS Networks*. (Master of Geomatic Engineering). The University of Melbourne,
- Healey, D., Meckler, S., Usen, A., & Cottle, E. (2016). *European Parliament - Cyber Security Strategy for the Energy Sector*. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU\(2016\)587333_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf)
- Hery, W., & Karri, R. (2010). *Cyber Security & the Smart Grid*. Retrieved from https://www.sallan.org/EventPix_slideshow_Smart-Grid/resources/W_Hery-R_Karri-Cyber_Security_and_the_Smart_Grid.pdf
- Høyve, G. K., Eriksen, T., Meland, B. J., & Narheim, B. T. (2008). Space-based AIS for global maritime traffic monitoring. *Acta Astronautica*, 62(2-3), 240-245.
- Hudson Analytix Inc. (2017). *Global Threats: Cybersecurity in Ports (Donald Duck, Daughters & Dollars)*. Paper presented at the Hemispheric Conference on Port Competitiveness & Security: Finding the Right Balance, University of Miami, Center for International Business Education & Research.
- Global Threats: Cybersecurity in Ports (Donald Duck, Daughters & Dollars), (2017).
- IBM Corporation. (2018). *Unleash digital intelligence with data and apps*. Retrieved from <https://www.ibm.com/cloud/smartpapers/data-governance-multicloud-integration.pdf>
- ICS-CERT. (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Retrieved from https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- IDirect. (2016). *The rising tide of Maritime VSAT*. Retrieved from <https://www.idirect.net/Applications/~media/Files/Maritime%20Campaign/Rising-Tide-Maritime-Final0092016.pdf>
- Ikeda, Y. (2017). *Smart Ship Application Platform - IoS-OP*. Retrieved from [https://www.jsmea.or.jp/ssap/assets/pdf/9c_SSAP_in_IMPA_LONDON\(20170912\).pdf](https://www.jsmea.or.jp/ssap/assets/pdf/9c_SSAP_in_IMPA_LONDON(20170912).pdf)
- Information Security Audit and Control Association. (2016). *The Merging of Cybersecurity and Operational Technology*. Retrieved from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Merging-of-Cybersecurity-and-Operational-Technology.aspx>
- INMARSAT. (2019). Our coverage. Retrieved from <https://www.inmarsat.com/about-us/our-satellites/our-coverage/>

- International Civil Aviation Organization. (2011). *EB 2011/56: "Interference to Global Navigation Satellite System (GNSS) Signals"*. Retrieved from https://www.skybrary.aero/index.php/Interference_to_GNSS_Signals
- International Hydrographic Organization. (2010). *Facts about Electronic Charts and Carriage Requirements*. Retrieved from <http://hydro.gov.au/prodserv/important-info/AA448300.pdf>
- International Hydrographic Organization. (2012). *IHO Data Protection Scheme*. Retrieved from https://www.iho.int/iho_pubs/standard/S-63/S-63_e1.1.1_EN_Apr12.pdf
- International Maritime Organisation. (2004). *MSC 79/25 - Report of the Maritime Safety Committee on its Seventy-Ninth Session*. Retrieved from
- International Maritime Organisation. (2017). *ECDIS - Guidance for Good Practice*.
- International Maritime Organization. (2008). *Sub-Committee on Radiocommunications and Search and Rescue - Report to the Maritime Safety Committee*. Retrieved from <http://www.mpa.gov.sg/web/wcm/connect/www/9a6e6065-a33b-4971-8cad-92aeb55fddea/cs12-15.pdf?MOD=AJPERES>
- International Maritime Organization. (2009). *International convention for the Safety of Life at Sea (SOLAS)", Chapter V "Safety of Navigation"*. Retrieved from <http://www.imo.org/en/OurWork/facilitation/documents/solas%20v%20on%20safety%20of%20navigation.pdf>
- International Maritime Organization. (2015). *Revised Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS)*. Retrieved from <http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Assembly/Documents/A.1106%2829%29.pdf>
- International Maritime Organization. (2016). *Measures to enhance Maritime Security: Report of the Working Group (MSC 96/WP.9)*. Retrieved from <http://12zc4845uhr73vbfjp3ubgkz.wpengine.netdna-cdn.com/wp-content/uploads/2016/05/Cyber-guidelines.pdf>
- International Risk Governance Council. (2011). *Risk Governance of Maritime Global Critical Infrastructure - The example of the Straits of Malacca and Singapore*. Retrieved from http://irgc.org/wp-content/uploads/2012/04/irgc_mgcireport_2011.pdf
- International Telecommunication Union. (2015). *Digital selective-calling system for use in the maritime mobile service (Recommendation ITU-R M.493-14 (09/2015))*. Retrieved from https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.493-11-200405-S!!PDF-E.pdf
- Ioseba Tena. (2011). *Automating ROV Operations in aid of the Oil & Gas Offshore Industry*. Retrieved from <https://www.unmannedsystemstechnology.com/wp-content/uploads/2013/10/White-Paper-Automating-ROV-Operations.pdf>
- Jensen, J. K. (2009). *Experience with AIS AtoN (Aids to Navigation) - Is there a future for electronic AtoN within e-Navigation?* (FRV-Rapport-2009-01). Retrieved from <https://imo.amsa.gov.au/iala-aism/anm/anm14/14-1.pdf>
- John A. Volpe National Transportation Systems Center. (2001). *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*. Retrieved from https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf
- Jones, M. (2017). Spoofing in the Black Sea: What really happened? *GPS World*. Retrieved from <https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>
- Jovanovic, A., Botteron, C., & Fariné, P. A. (2014). *Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers*. Paper presented at the Record - IEEE PLANS, Position Location and Navigation Symposium.
- Kaplan, E., & Hegarty, C. (2006). *Understanding GPS: Principles and Applications, Second Edition* (Second ed.).
- Kaspersky. (2013). *The 'Icefog' APT: A Tale of Cloak and Three Daggers*. Retrieved from <https://www.securelist.com/en/downloads/vlpdfs/icefog.pdf>
- Kok, M., Hol, J. D., & Schön, T. B. (2017). Using inertial sensors for position and orientation estimation. *Foundations and Trends in Signal Processing, Vol. 11: No. 1-2, pp 1-153*.

- Kongsberg. (n.d.). K-Bridge Conning System. Retrieved from <https://www.kongsberg.com/maritime/products/bridge-systems-and-control-centres/navigation-system/conning-display/>
- Lagouvardou, S. (2018). *Maritime Cyber Security: concepts, problems and models*. (Masters Thesis). Technical University of Denmark, Retrieved from https://orbit.dtu.dk/files/156025857/Lagouvardou_MScThesis_FINAL.pdf
- Lampe & Schwartze KG. (2015). *Look-Out 2016 - Maritime Domain Cyber: Risk, Threats and Future Perspectives*. Retrieved from http://www.dlr.de/dlr/Portaldata/1/Resources/documents/2015/Look-Out_2016_web.pdf
- Lara, M. (2015). *Secure Broadband IP over Satellite*. Retrieved from https://usgif.org/system/uploads/3908/original/Secure_Broadband_IP_over_Satellite_1_.pdf
- Li, X., Zhang, X., Ren, X., Fritsche, M., Wickert, J., & Schuh, H. (2015). Precise positioning with current multi-constellation Global Navigation Satellite Systems: GPS, GLONASS, Galileo and BeiDou. *Scientific reports*, 5, 8328. doi:10.1038/srep08328
- Liu, G., Perez, R., Muñoz, J. A., & Regueira, F. (2016). Internet of Ships: The Future Ahead. *World Journal of Engineering and Technology*. doi:10.4236/wjet.2016.43D027
- Liu, S., Xing, B., Li, B., & Gu, M. (2014). Ship information system: Overview and research trends. *International Journal of Naval Architecture and Ocean Engineering*, 6, 670-684. doi:10.2478/IJNAOE-2013-0204
- London Economics. (2017). *The economic impact on the UK of a disruption to GNSS*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf
- Magal S3. (2014). *New Cyber Frontiers (Antwerp Port Case study)*. Retrieved from
- Maral, G. (1995). *VSAT Networks*.
- Marine Handling & Logistics. (2018). Maersk first to test LiDAR on Container Ship. Retrieved from <https://www.mhlnews.com/technology-automation/maersk-first-test-lidar-container-ship>
- MarineTraffic. (2017). MarineTraffic: Global Ship Tracking Intelligence | AIS Marine Traffic. Retrieved from <https://www.marinetraffic.com>
- Marlink. (2018). The Complete Guide to VSAT. Retrieved from https://issuu.com/rivieramaritimemedia/docs/the_complete_guide_to_vsat_2018
- Marsh & McLennan, & Global Marine Practice. (2014). The Risk of Cyber Attack to the Maritime Sector. Retrieved from <https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Gap%20Insurance%20Cyber%20Risk%20Filling%20the%20Coverage%20Gap-07-2014.pdf>
- Masters, D. (2018). *Seizing Opportunity: Spire's CubeSat Constellation of GNSS, AIS, and ADS-B Sensors*. Paper presented at the Stanford PNT Symposium. http://web.stanford.edu/group/scpnt/pnt/PNT18/presentation_files/I07-Masters-Spire_GNSS_AIS_ADS-B.pdf
- Matherly, J. (2017). Shodan Ship Tracker. Retrieved from <https://shiptracker.shodan.io/>
- Mertens, M. (2014). Securing VSAT Terminals. Retrieved from <http://www.newtec.eu/article/article/securing-vsats-terminals>
- Mimoso, M. (2017). Maersk Shipping Reports \$300M Loss Stemming from NotPetya Attack. Retrieved from <https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/>
- Mirian, A., Ma, Z., Adrian, D., Tischer, M., Chuenchujit, T., Yardley, T., . . . Halderman, J. A. (2016). *An internet-wide view of ICS devices*. Paper presented at the 14th Annual Conference on Privacy, Security and Trust (PST), 2016
- Morse, J. (2017). Remotely hacking ships shouldn't be this easy, and yet ... Retrieved from <http://mashable.com/2017/07/18/hacking-boats-is-fun-and-easy/#mjW1KLCj6aqb>
- Moteff, J. (2005). *Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences*. Retrieved from <https://fas.org/sgp/crs/homsec/RL32561.pdf>

- Moxa Inc. (2017). Industrial Ethernet for In-ship Communication. Retrieved from https://www.moxa.com/event/Net/2010/Maritime_microsite/In-ship_solution.htm
- National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- National Institute of Standards and Technology. (2017). *Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1*. Retrieved from <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- National Oceanic and Atmospheric Administration. (2005). *ENC Data Encryption*. Retrieved from https://nauticalcharts.noaa.gov/h srp/archive/march2005/EncryptionPointPaper_final1.pdf
- National Oceanic and Atmospheric Administration. (2018). What is LiDAR? Retrieved from <https://oceanservice.noaa.gov/facts/lidar.html>
- Nicholson, M., Tutt, I., & Ward, N. (2015). *e-Navigation - The role of visual aids to navigation*. Retrieved from http://www.gla-rrnav.org/pdfs/enav_paper_iala_2010.pdf
- North P & I. (2016). Cyber Risks in Shipping - Loss Prevention Briefing. In.
- NSW Department of Primary Industries. (1981). *Echo Sounder, Sonar, Radar Operations, and Navigation Course - Final Report*. Retrieved from <http://www.frdc.com.au/Archived-Reports/FRDC%20Projects/1981-070-DLD.pdf>
- Online Trust Alliance. (2016). *Data Protection and Breach Readiness Guide*. Retrieved from <https://otalliance.org/Breach>
- Orbcomm. (2017). SCADA System Monitoring. Retrieved from <https://www.orbcomm.com/en/industries/natural-resources/scada-system-monitoring>
- Orolia Maritime. (2019). McMurdo SmartFind S5A AIS SART. Retrieved from <https://www.oroliamaritime.com/products/mcmurdo-smartfind-s5-ais-sart/>
- Pace, S., & Camacho, S. (2015). *Global Navigation Satellite System (GNSS) Spectrum Protection*. Retrieved from <https://www.gps.gov/governance/advisory/meetings/2015-10/pace-camacho.pdf>
- Paganini, P. (2017). Brutal Kangaroo is the CIA tool suite for hacking Air-Gapped Networks. Retrieved from <http://securityaffairs.co/wordpress/60322/hacking/brutal-kangaroo-cia.html>
- Panayides, P., & Song, D.-W. (2012). *Maritime Logistics : A Complete Guide to Effective Shipping and Port Management*.
- Parkinson, A. (2011, 12-14 Sept. 2011). *Space-based ADS-B: A small step for technology a giant leap for ATM?* Paper presented at the 2011 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles.
- Ponemon Institute LLC. (2017). *2017 Cost of Data Breach Study - Global Overview*. Retrieved from <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&>
- Port Technology. (2017). Airbus D&S Collaborates on Maritime Crime Fighting Tool. Retrieved from https://www.porttechnology.org/news/airbus_ds_collaborates_on_maritime_crime_fighting_tool
- Praetorius, G. (2014). *Vessel Traffic Service (VTS): a maritime information service or traffic control system? Understanding everyday performance and resilience in a socio-technical system under change*. Chalmers Institute of Technology,
- Radan, D. (2008). *Integrated control of marine electrical power systems*. Norwegian University of Science and Technology,
- Rødseth, Ø. J., Øgaard, O., & Hallset, J. O. (1992). *Integrated Ship Control and Open Systems (1474-6670)*. Retrieved from <http://www.mits-forum.org/resources/ifac92-proof.pdf>
- Rogers, J. D. (1989). *VSAT-an alternative communication network for fixed and mobile applications - IET Conference Publication*. Paper presented at the IEE Colloquium on VSATs - Trends and Technologies.

- Rolls-Royce. (2016). *Autonomous ships The next step*. Retrieved from <http://www.rolls-royce.com/~media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf>
- RTL-SDR. (2018). Using a HackRF to Spoof GPS Navigation in Cars and Divert Drivers. Retrieved from <https://www.rtl-sdr.com/tag/gps-spoofing/>
- SAFETY4SEA. (2017). SAFETY4SEA survey reveals industry's smart side. Retrieved from <https://www.safety4sea.com/safety4sea-survey-reveals-industrys-smart-side/>
- SAFETY4SEA. (2019). Britannia P&I considers the benefits of CCTV cameras on vessels. Retrieved from <https://safety4sea.com/britannia-pi-considers-the-benefits-of-cctv-cameras-on-vessels/>
- Santamarta, R. (2014a). SATCOM terminals: Hacking by air, sea, and land. In: IOActive Security Services.
- Santamarta, R. (2014b). *Technical White Paper: A Wake-up Call for SATCOM Security*. Retrieved from https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf
- Santamarta, R. (2014c). *Technical White Paper: SATCOM terminals: Hacking by air, sea, and land*. Retrieved from <https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf>
- Santamarta, R. (2015). Maritime Security: Hacking into a Voyage Data Recorder (VDR). Retrieved from <http://blog.ioactive.com/2015/12/maritime-security-hacking-into-voyage.html>
- SATCOM, C. (2013). *Sailor 900 VSAT: Technical manual*. Retrieved from <https://www.theastgroup.com/media/products/SAILOR%20900%3A%20Ku-Band%20VSAT%20Antenna/SAILOR%20900%20VSAT%20Tech%20Manual%202013.pdf>
- Shauk, Z. (2013). Malware offshore: Dangers lurk where the chips fail. Retrieved from <https://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/>
- Shenoi, R., Bowker, J., Dzielendziak, A., Lidtke, A., Zhu, G., Cheng, F., . . . Johnson, S. (2015). *Global marine technology trends 2030*. Retrieved from http://info.lr.org/l/12702/2015-09-04/2bxfbc/12702/131118/55046_LR2030_WEB_LR_25mb.pdf
- Shoultz, D. (2017). Securely Connected Vessels: Vessel Communications and Maritime Cybersecurity. *maritimeprofessional.com*. Retrieved from <https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communications-and-maritime-15176>
- Silverstein, A. (2016). *GPS Timing Challenges and Robustness Needs for Critical Infrastructures : Examples from Telecom , Broadcast and Power Delivery Industries*. Retrieved from <https://www.gps.gov/governance/advisory/meetings/2016-05/danielson-silverstein.pdf>
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*: Oxford University Press Inc. USA.
- Sistrunk, C. (2016). *How to Get into ICS Security*. Paper presented at the RSA Conference 2016, San Francisco, United States. <https://www.slideshare.net/chrisistrunk/how-to-get-into-ics-security>
- Skey, K. M. (2017). *Responsible Use of GPS for Critical Infrastructure*. Retrieved from <https://www.gps.gov/multimedia/presentations/2017/12/CIPRNA/skey.pdf>
- Skjong, E. (2017). *Optimization-based Control inShipboard Electric Systems*. Norwegian University of Science and Technology, Trondheim, Norway.
- Soloviev, A., & Venable, D. (2009). When GNSS Goes Blind. Retrieved from <https://insidegnss.com/auto/oct10-soloviev.pdf>
- Soullie, A. (2014a). *Pentesting PLCs 101*. Paper presented at the Blackhat Europe 2014.
- Soullie, A. (2014b). *Pentesting PLCs 101*. Paper presented at the Blackhat Europe Conference 2014. <https://www.blackhat.com/docs/eu-14/materials/eu-14-Soullie-Industrial-Control-Systems-Pentesting-PLCs-101.pdf>
- Stark Moore Macmillan. (2011). *VSAT: Present and Future A comprehensive survey of maritime VSAT*. Retrieved from <https://docplayer.net/20881325-Vsat-present-and-future.html>

- Symantec Security Response. (2017). Petya ransomware outbreak: Here's what you need to know. Retrieved from <https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know>
- The MUNIN Research Project. (2016). Research in Maritime Autonomous Systems - Project Results and Technology Potentials. Retrieved from <http://www.unmanned-ship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf>
- The Royal Institution of Naval Architects. (2017). The Internet of Ships: a new design for Smart Ships. *The Naval Architect*. Retrieved from <https://www.rina.org.uk/The Internet of Ships a new design for Smart Ships.html>
- Tokyo Keiki. (2017). *Electronic Chart Display and Information System (ECDIS) EC-8600/EC-8100*. Retrieved from https://www.tokyokeiki.jp/Portals/0/images/e/products/pdf/marine/ec8600_8100_e_201902.pdf
- Tollefsen, C. D., & Zedel, L. (2003). Evaluation of a Doppler sonar system for fisheries applications. *ICES Journal of Marine Science*, 60(3), 692-699.
- Torre, A. D., & Caporali, A. (2015). An analysis of intersystem biases for multi-GNSS positioning. *GPS Solutions*, 19. doi:10.1007/s10291-014-0388-2
- Transport Canada. (2016). *Understanding Cyber Risk: Best Practices for Canada's Maritime Sector*. Retrieved from <http://www.cosbc.ca/index.php/advocacy/files-downloads/transport-canada/455-understanding-cyber-risk/file>
- Transportation Research Board. (2015). *Application of Real-Time Monitoring of Offshore Oil and Gas Operations - Workshop Report*. Retrieved from <https://www.nap.edu/read/22082/chapter/1>
- U.S. Department of Homeland Security. (2013). *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*. Retrieved from <https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf>
- UK Government Office for Science. (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf
- UNCTAD. (2017). *Review of Maritime Transport 2017*. Retrieved from https://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf
- United States Coast Guard. (2015). *Cyber Risks in the Marine Transportation System - The U.S. Coast Guard Approach*. Retrieved from http://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/USCG_Paper_MTS_CyberRisks.pdf?ver=2017-07-19-070403-473
- United States Coast Guard. (2016). *Electronic Aids to Navigation*. Retrieved from <https://www.dhs.gov/sites/default/files/publications/United%20States%20Coast%20Guard%20-%20Electronic%20Aids%20to%20Navigation.pdf>
- United States Coast Guard. (2017). *Draft Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*. Washington, D.C. Retrieved from http://www.maritimedelriv.com/storage/app/media/Draft_Cyber_Risks_NVIC_7-12-17.pdf
- Vasavada, Y., Gopal, R., Ravishankar, C., Zakaria, G., & BenAmmar, N. (2015). Architectures for next generation high throughput satellite systems. *International Journal of Satellite Communications and Networking*, 28, 291-315. doi:10.1002/sat
- VesselFinder Ltd. (2017). Free AIS Ship Tracking of Marine Traffic - VesselFinder. Retrieved from <https://www.vesselfinder.com/>
- Wang, J., & Zhang, S. M. (2000). Management of human error in shipping operations. *Professional Safety*, 45(10), 23-28. Retrieved from <http://aeasseincludes.asse.org/professionalsafety/pastissues/045/10/012659ul.pdf>
- Wang, L., Li, Z., Ge, M., Neitzel, F., Wang, Z., & Yuan, H. (2018). Validation and assessment of multi-GNSS real-time precise point positioning in simulated kinematic mode using IGS real-time service. *Remote Sensing*, 10. doi:10.3390/rs10020337

- Williamson, G. (2015). OT, ICS, SCADA – What’s the difference? Retrieved from <https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference>
- Wright, R. G. (2017). *Virtual aids to navigation*. World Maritime University
- Wu, X.-B., Sun, Z.-C., Wu, Z.-H., & Miao, X.-N. (2016). *Research in Security Architecture for Internet of Ships*. Paper presented at the 2016 Joint International Conference on Artificial Intelligence and Computer Engineering (AICE 2016) and International Conference on Network and Communication Security (NCS 2016).
- x0rz. (2017). Shodan now live tracking ships via VSAT antennas exposing web services. Retrieved from <https://twitter.com/x0rz/status/887238046172753920?lang=en>
- Zachhuber, P., Pinzón, I. D. H., Born, A., Hoppe, M., Burmisova, L., Heßelbarth, A., . . . Michler, O. (2013). PNT-data generation as basis for guidance systems in inland water traffic. *Inertial Sensors and Systems*.
- Zaghloul, M. S. (2014). Online Ship Control System Using Supervisory Control and Data Acquisition (SCADA). *International Journal of Computer Science and Application*. Retrieved from www.dpi-journals.com/index.php/IJCSA/article/download/780/648
- Zurich. (2014). *Beyond data breaches: global interconnections of cyber risk*. Retrieved from <https://www.jasadvisors.com/custom/uploads/2014/04/Risk-After-Next-Whitepaper.pdf>

Appendix A Maritime threat environment summary

