Uncharted Waters

How the Maritime industry is both learning from and leading cybersecurity thinking

Paul Dorey

Sponsored by Inmarsat

Contents

Executive Summary

Cybersecurity is the hot topic in the world of Maritime digitalisation. Compared with other industry sectors, Maritime is coming to cybersecurity relatively late, but the specific challenges in digital shipping are right at the forefront of leading-edge technology and the world of the Internet of Things (IoT). I think that emerging IoT cybersecurity guidelines will have particular relevance to systems on ships.

In the maritime industry we should also look carefully at where critical interdependencies lie, particularly where a network or ship's system connects to, depends on and trusts the integrity of a system that is outside of the ship.

Ship control systems are 'turnkey' and so manufacturers of digital systems for ships are fundamental to the design of security capabilities and so should engage in dialogue now to help define how cybersecurity will be managed. Systems manufacturers should also be creative and open to adopting solutions which could become interoperable standards.

Ship operators and managers need to identify and address the level of cybersecurity awareness, training and capabilities that will be required on ships, plus define the additional services they will need delivered or supported from beyond the ship, by the operating company or by third party providers. Whilst giving attention to the requirements for new build, vessels operators also need to cover the cybersecurity of existing systems and particularly watch out for changes to risk from the adoption of new networks and systems.

Introduction

Over the past year I have had the pleasure of working with the Maritime industry in cybersecurity and I am recognising a number of common themes that I have previously seen in the energy sector, and even in financial services.

I am also seeing fundamental differences, and the start of some industry-leading thinking that I think will have broader applicability.

The purpose of this paper is to share these insights, which I hope will be useful and will prompt further conversation. I am grateful for the ideas and guidance given to me by professionals working in the industry, although the views stated here are my own.

1. How do you know that you are secure?

The challenge of answering the question "Are you secure?" starts with fundamentally understanding what components make up a system and what is their configuration and security status. As in process industries such as the energy sector or industrial manufacturing, the use of digital systems in Maritime goes beyond office Information Technology (IT) to include Operational Technology (OT). OT consists of that hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events. There are numerous examples of these type of systems on ships, (see Figure 1) and even in port facilities:

Types of Operational Technology (OT)
Bridge Systems including ECDIS, AIS
Propulsion, machinery management and power control systems e.g. engine rooms
Access control systems to ensure physical security
Cargo management systems, including critical cargo pressure and temperature, cargo tracking, ballast water etc.

Figure 1: Examples of Operational Technology Systems

For IT the identification of systems on a network is usually achieved using scanning tools or software agents. As discussed later, OT control systems may be vulnerable to common IT administrative tools, such as simple network scans and so several industries have found OT asset identification to be difficult, both because of fragility, but also because the segregation and isolation of OT networks may be part of their security architecture.

Knowing that something is secure is also a moving target, requiring assessment to keep up with changing vulnerabilities (new vulnerability disclosures) and changing threats (new attacks). When considering the limited resources available on a ship, it is unlikely that each ship will be able to track its own cybersecurity threats and newly discovered vulnerabilities, and instead will need to take information from some authorised onshore service, ideally one that has been specifically tuned for the systems on a particular vessel. Furthermore, recognising that ship systems have deviated from a known good configuration would be of immense benefit to operators.

Knowing that ship systems are at greater risk, then requires a decision on when to intervene to fix vulnerabilities and how this can be done when a vessel is in live operation. Some in-shore process plants find this decision particularly difficult and have found they need to carefully design both processes and update solutions which support continued operation.

But security is not just about software patching and systems configuration, failures in processes and mistakes by people can present a significant security loophole and so awareness of good cybersecurity behaviour and training in good cybersecurity practices is a very important. Elsewhere[1], I have described the psychology of good and bad security behaviours and how to influence them.

Many of the cybersecurity standards describe this whole picture of behaviours, processes and technical requirements, and these should be reviewed when defining a security programme for an enterprise, site, or ship.

[1] The Weakest Link, Jeremy Swinfen Green & Paul Dorey, Bloomsbury (2016)

2. Which Standards should we use?

So if standards are key, which ones should you refer to?

Managers and engineers new to cybersecurity usually find this confusing and may struggle with the practicality of implementing particular security standards and practices. Just deciding which of the numerous standards to apply can be a challenge in itself. A quick recap of the history and evolution of cybersecurity may sound academic, but I hope will put structure around the problem and help show where people are coming from.

The connection of security and computer systems started with the wartime birth of computing, and therefore had a strong government focus on confidentiality, codes and code breaking. Protecting confidential information therefore often features as a dominant part of security, which is underpinned by data protection law and the all too frequent news of personal data breaches. However, in industries such as energy and Maritime, the accuracy and integrity of information and the continued availability of operational systems is a higher priority. Most security standards recognise the three aspects of confidentiality, integrity and availability, but may show historical bias towards confidentiality and the security measures that support it. Many standards therefore need careful thinking through when applied to operational technologies.

ISO/IEC 27001

Twenty five years ago the only security standards were either those that described specific detailed security functions and communications protocols, or were internal company standards within banks, telcos. and oil companies. Out of this mix arose a British standard[2] which eventually turned into the ISO/IEC 27000 series, which is frequently referenced as the key set of information security (cybersecurity) standard. These are very important standards defining how information security should be managed across an organisation when using information technology. However, they can take some navigating as there are now around 40 individual standards which go beyond the well-known and higher level 27001 and 27002 members of the family.

ISO/IEC 62443

The challenge for Maritime, and indeed for all companies with operational technologies, is to decide what should be done at the company level and what at the local site/ship level. In fact, engineers from industries with industrial control systems saw limitations and so established the International Society of Automation, ISA-99 standards group which has gone on to develop the ISA/IEC 62443 series of standards to specifically address the OT environment. However, even with OT specific guidance, the physical isolation and low manning levels on ships need special consideration on how security solutions can work in practice.

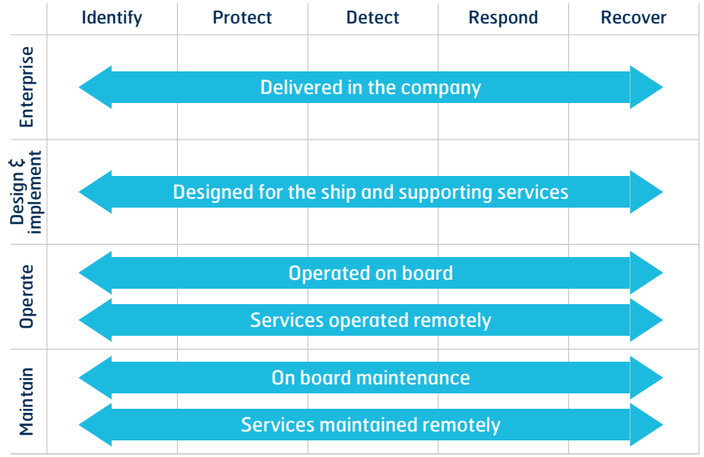


Figure 2: Mapping cyber security capability to different situations

Maritime technology standards themselves also have key security references such as IEC 61162-450 covering security in an Ethernet network for the navigation and communication on the bridge. and also IEC 61162-460 which adds safety and security to the ship network.

The recently updated industry "cybersecurity guidelines for ships[3]" provides a very helpful reference and references thinking from ISO 27000, ISO/IEC 62443 and other sources of best practice.

A useful approach when deciding which standards should be used is to map them to a capability framework - the International Maritime Organization (IMO) have been particularly helpful in their guidance[4] by directing Maritime organisations to consider cybersecurity under the specific headings of "Identify, Protect, Detect, Respond and Recover".

[2] BS7799

[3] The Guidelines on Cyber Security Onboard Ships, Version 2.0 (2017)

[4] MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management, International Maritime Organization

3. Operational Technology (OT) vs. Information Technology (IT)

As mentioned earlier, the majority of cybersecurity standards have been derived from the IT environment. The dynamics of OT and IT are different and this changes the way that they need to be managed, as illustrated in the following table[5]:

Information Technology	Operational Technology
Performance	
Non real-time	Real-time
Response must be reliable	Response is time critical
High throughput demanded	Modest throughput acceptable
High delay and jitter accepted	High delay a serious concern
Reliability	
Scheduled operation	Continuous operation
Occasional failures tolerated	Outages intolerable
Beta testing in the field acceptable	Thorough QA testing expected
Modifications possible with little paperwork	Formal certification may be required after any change
Security Priorities	
Risk impact is loss of confidentiality, integrity and business operations	Risk impact can be environmental and safety related as well as business operations.
Recover by reboot	Fault tolerance essential

Figure 3: Operational Technology (OT) vs. Information Technology (IT)

Not only does OT have a different set of priorities from IT but OT systems cannot all be managed with the same security tools and processes as used for IT. For example, simple software running on OT may be far more fragile than corresponding IT systems which may have much more memory and processing power. A simple security vulnerability scan could therefore seriously impact an OT system and cause it to fail. Security additions such as anti-virus or firewalls also need careful accreditation by OT system vendors to provide assurance that processes will not be disrupted.

[5] Credit: Eric Byres, ICS Secure

4. Who is responsible for security?

Responsibility for security in operation always remains with the operator and this is no different in Maritime. Operators therefore need to be concerned about staff training and awareness, robust processes, security monitoring and security configurations and maintenance.

But OT control systems and embedded computers are not implemented in the same way as IT systems. The ship operator, or even the shipyard, does not buy computer processors, disk storage and software and then build them into a system. Instead they procure a complete "turnkey" system from the control systems manufacturer. This means that security design and configuration is much more in the hands of the system manufacturer than for standard IT builds. If security features and capabilities are not built into the systems then they are not available for use.

The manufacturer also needs to have an active participation in future security maintenance as updates will need to be accredited. Procurement is therefore a key stage for successful OT security, if it is not in the requirement it is not likely to appear in the product. Other industries are struggling with this dynamic, with cost often trumping security and procurement teams removing requirements during negotiation. OT vendors for these industries also rightly complained that security specifications can be ill-defined or unrealistic. Examples from one sector included saying that systems should use "encryption" without specifying what is to be encrypted, under what circumstances and why.

Several industry sectors therefore struggle with unclear definitions of cybersecurity which can be used in procurement. In the case of ships, we should have a better opportunity to bring clarity and harder-edged requirements through the classification requirements process which is currently examining cybersecurity recommendations through IACS. This opportunity does place the Maritime industry ahead of others in being able to more clearly define requirements but, as a result, there will have to be much more detailed thinking than other industries have had to do. We must also remember that internationally accepted cybersecurity requirements for ships do not apply across all of the Maritime industry and hence, for example, similar standardisation is unlikely to exist for port facilities.

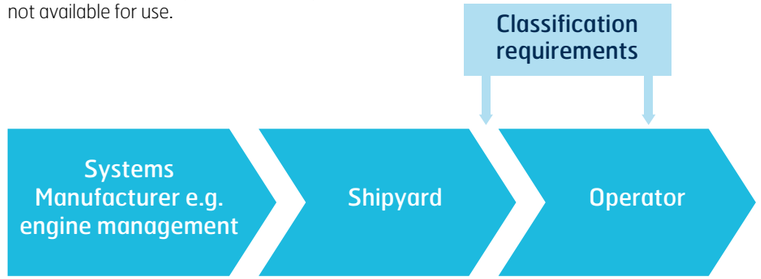


Figure 4: Security capabilities need to start with the manufacturer of individual ship systems. The target security recommendations/requirements are being developed by the Classification Societies with industry consultation.

5. Skills, staffing and automation – The Internet of Things

The low-level of staffing on a ship presents a particular challenge which brings Maritime cybersecurity to the forefront of innovation. The majority of IT security standards have an assumption of support being provided by a significant IT team and a corresponding set of cybersecurity specialists. These are not available on a vessel which may not even have any dedicated IT expertise in the crew. The philosophy here is closer to that of the Internet of Things, where systems need to be self-managing, remotely updated and supported by automated security. This brings the shipping industry clearly into the leading edge of emerging security thinking.

Detection of anomalies such as deviation from 'known good' configuration and detection of security attacks need to happen as automatically as possible and not require expert staff. Systems need to be built with the ability to be securely updated, even during operation, and have safe rollback. Rather than assuming no IT skills exist, it is more appropriate to assume that engineers with self-taught home IT skills will be available and can do some level of IT support, but they will not be cybersecurity specialists. So some specialist functions such as a deep analysis of alerts or security forensics will need to be delivered remotely or by visiting cybersecurity service providers.

The Internet of Things has a greater need for automation, and self-management than typically expected for IT and OT and so can resemble a ship. The following table gives some examples of functional requirements that I am involved with which are taken from the IoT Security Compliance Framework of the IoT Security Foundation[6].

Examples from the compliance framework:

Example area	Example requirements
Device Hardware and Physical Security – assume devices will not be in data centres	Protection of communication ports, and against physical tampering, secure boot
Device Software Application – devices will be distributed and may not have physical access to manage them	Prevention of loading unauthorised (unauthenticated) software, remote software update (and secure roll-back), design to fail safely, no back door access
Device Operating System – devices will be distributed and may not have physical access to manage them	Least privilege, ability to have latest updates, security features enabled, no unnecessary services or functions, no back door access
Device Wired and Wireless Interfaces - may not be part of a secure and managed network.	Secure protocols and only actually needed protocols active, good security on connections.
Authentication and Authorisation - device has its own identity and personalisation	Unique tamperproof identifiers, proper password security discipline
Encryption and Key Management for Hardware – encryption used to manage and protect over untrusted networks	Follows industry good practice
Cloud, Web User Interface and Mobile Applications – goes beyond a corporate IT network etc.	Web part of the service and any mobile application will have similarly robust and well-designed security and will not provide a weakest link.

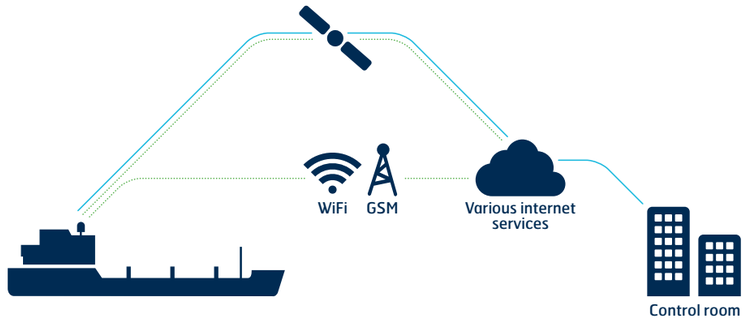
Figure 5: Examples of functional requirements taken from the IoT Security Compliance Framework of the IoT Security Foundation

[6] IoT Security Compliance Framework, Release 1.0, IoT Security Foundation (2016), https://iotsecurityfoundation.org/

6. Mobility and connectivity – a challenge of scope

Other industries have learnt the hard way that properly defining the scope of the cybersecurity problem is key. Security teams tend to focus on the technologies directly managed by their own internal corporate organisation (usually IT). So when smart phones or third party cloud web services start to be used by their business, the security risk does not always get picked up immediately. A security team focusing on IT servers and the corporate network can forget to look at mobile apps and web services. However, security risk does not respect any organisation. If critical services and data storage are used by a company then their security will matter wherever they are located.

In the Maritime industry we should look carefully at where critical interdependencies lie, particularly where a network or ship system connects to and trusts the integrity of a system running outside of the ship. Inherent trust is already appearing in the context of ship networks,[7] including onshore services monitoring and adjusting ship systems, some of which even reside in the Internet cloud. There are also ad hoc connections of systems and portable devices to those on the ship, including connecting dockyard cranes to ballast systems or visiting devices carried onto the ship by maintenance engineers, pilots or other test and service providers.



Managed Networks
In some new examples of digitalisation such as engine or battery performance management, on-shore facilities may be capable of monitoring or even adjusting the performance of systems on-board the ship.

Unmanaged Networks
As it is not managed end-to-end with a defined security model, general network connectivity to the ship should be considered to be untrusted.

Figure 6: Diagram of a managed and unmanaged network

[7] See almost any issue of "Digital Ship" and similar industry publications for relevant articles and advertisements

7. Risk and Resilience

Good security comes as a result of having the right level of capability to manage the risk to which systems are exposed. Risk comes from the motivation of attackers, their capability and skill and the opportunities they have to carry out their attack. Much of this is not easy to know and often the fact that an attack which would cause a serious impact could happen, is sufficient to justify security protection being put in place. However, a key element of cybersecurity is the ability of a system not just to resist attack but also to be able to detect, respond and recover from it. It is not possible to protect against all possible future attacks as attackers are creative and will devise new approaches. Well thought-out recovery is therefore a good strategy because one approach can mitigate multiple causes.

Within Maritime there is continued discussion on the importance of having manual alternatives to digital systems as part of resilience and recovery. Manual systems not only have the advantage of avoiding digital attacks, but can also take advantage of physical intervention by people who have greater flexibility than systems when placed in unusual circumstances.

But we should not be complacent, as other industries have seen an inexorable trend towards both automation and connectivity which may not always have an alternative. For example, land-based industrial plants have seen a trend in designs where emergency shutdown systems are placed onto the same digital network as the control system itself. This is an efficient design concept, but one which significantly reduces resilience to a cyber-attack on the network. Maritime engineers need to keep a wary eye on similar pressures and insist on designs and architectural patterns that either support manual recovery or provide resilience,[8] such as through diversity and redundancy.

[8] "Cyber Resiliency Design Principles", Deborah Bodeau & Richard Graubart, The Mitre Corporation (2017)

Conclusions and next steps

For cybersecurity in the Maritime industry to make good progress we need joined- up and consistent thinking across a whole range of different stakeholders, and as yet, not all of these conversations are happening.

- For classification societies and ship builders there needs to be clarity over the cybersecurity recommendations and requirements which are to apply. IACS should be commended on engaging the wider industry through a joint working group, as standards for ships on their own cannot be considered without taking into account cybersecurity activities in operation.
- Manufacturers of digital systems for ships, and those who are designing digital management capabilities into their systems should engage in dialogue now to help define how cybersecurity will be managed. They should also be creative and open to adopting solutions which could become interoperable standards.
- Operators need to look at the real cybersecurity awareness, training and capability requirements that will be required on ships. Where they see limitations, they should define the services they will need to have delivered or supported from beyond the ship by the operating company or third party providers. Whilst giving attention to the requirements for new build, vessels operators also need to examine the cybersecurity of existing systems and particularly watch out for risk changes from adding on new networks and systems.
- Ports should evaluate their own cybersecurity and cyber awareness and take particular care over the security of systems and networks which connect to ships.
- Support services such as pilots, maintenance engineers and test services should take care of what they bring onto ships and the security obligations when connecting to ship systems.
- Should promote cybersecurity awareness[9] amongst their members and look for the training and development opportunities.

Collectively – the industry should do more to promote sharing of alerts about incidents and share best practices, as well as learn from other industries, especially others who use operational technologies. Because of the special nature of maritime technology, the industry would also do well to participate in work to enhance the security for the Internet of Things as this should deliver low maintenance solutions suitable for the Maritime industry.

[9] Such as: https://www.becyberawareatsea.com/guidance

Prof Paul Dorey

PhD., CISM, F.Inst.ISP

Prof. Paul Dorey, is well known for his strategic thought leadership in cybersecurity including being Founder Chairman of the Institute of Information Security Professionals and now Chairman of the Internet of Things Security Foundation. His award winning career in Cybersecurity Risk Management includes Executive leadership roles at Deutsche Bank/Morgan Grenfell, Barclays Bank and BP.

Now a Visiting Professor in Information Security at Royal Holloway, University of London, he works with companies and government departments in developing their long term cybersecurity strategies, their security capabilities and leadership. He recently contributed to the January 2017 World Economic Forum guidance 'Advancing Cyber Resilience: Principles and Tools for Boards' and produced an introduction to Securing the Internet of Things published by Springer International Publishing[10]. He can be contacted at: paul.dorey@csoconfidential.com

[10] P. Dorey, "Securing the Internet of Things" p445-468 in K. Mayes and K. Markantonakis (eds.), Smart Cards, Tokens, Security and Applications, Springer International Publishing AG (2017)

inmarsat.com/maritime

While the information in this document has been prepared in good faith, no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability (howsoever arising) is or will be accepted by the Inmarsat group or any of its officers, employees or agents in relation to the adequacy, accuracy, completeness, reasonableness or fitness for purpose of the information in this document. All and any such responsibility and liability is expressly disclaimed and excluded to the maximum extent permitted by applicable law. INMARSAT is a trademark owned by the International Mobile Satellite Organisation, the Inmarsat LOGO is a trademark owned by Inmarsat (IP) Company Limited. Both trademarks are licensed to Inmarsat Global Limited. All other Inmarsat trade marks in this document are owned by Inmarsat Global Limited. © Inmarsat Global Limited 2017. All rights reserved. Cybersecurity Insight Paper September 2017.