Santtu Erich

Cyber Security Framework for NAPA Onboard Products

Metropolia University of Applied Sciences

Master of Engineering

Information Technology
Thesis

06.05.2021

Preface

This thesis was born in a situation, where NAPA as a company was in urgent need of improving Cyber Security capabilities of provided systems, products and the processes used to deliver them. So far, these have been tackled in organized manner regarding the software development procedures and our cloud services security.

However, the IMO regulations now dictate, that all shipping companies must include cyber security in their safety management system by the end of 2021, and that this must audited as well.
Thus, the aim of the thesis is to provide holistic view to product deliveries to customers ships and how to handle cyber security requirements regarding that.

Also, there was a great need to move from reactive response to proactive and planned Cyber Security Management for NAPA ship deliveries.

The undersigned has worked on initiatives for improving the security enhancements of NAPA systems, famously even before joining NAPA Ltd as an employee. Before my employment at NAPA, I worked as a Ship IT Manager on a tanker company where NAPA products were used.
On occasion, I was involved with Cyber Security issues when evaluating products we purchased, included but not limited to NAPA.

The scope of Cyber Security field is so wide, that even many of our customers are many times confused and challenged on what to require from software and systems provider.

Purpose of the thesis is to provide information for Sales, Development and Delivery, of the requirements and offered certifications from Class Society point of view. The view is selected as such, because all ships have a nominated Class Society and they are the entity that ensures the vessels compliance on any regulation.

I would like to thank and acknowledge advisory from Kana Dohi, Mikko Lehto, Mika Väkiparta and Tommi Vihavainen, who provided vital information from development point of view and regulations and on processes related to Cyber Security.

Author Title Number of Pages Date	Santtu Erich Cyber Security Framework for NAPA Onboard Products 74 pages + 2 appendices 6 May 2021
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Lecturer Sami Sainio, D.Sc. (Tech) Development coach Tommi Vihavainen, Napa Oy

NAPA as a maritime software and system provider needs to ensure proven cyber security capabilities before, during and after a system delivery to a ship.

Ship owners need to select a classification society for each ship, for insurance purposes. Each Class Society has their own requirements for cyber security compliance, which are based on top level the recommendations and guidelines: Those result in what is called a class notation. These can be used as a framework for NAPA to achieve regulatory compliance.

In the study, for Onboard Cyber Security of NAPA, main Class Society's and corresponding notations are studied and documented for relevancy, necessary documentation from NAPA and for the general procedure of the achievement of the class notation:

Classification Society	Class notation name
ABS	CyberSafetyTM
Bureau Veritas	Cyber Managed and Cyber Secure
CCS	Cyber Security (P,S)
ClassNK	CybR-G
ClassNK	Digital Smartship
DNV	Cyber Secure
Lloyd's	ShipRight

Keywords	Maritime cyber security, IMO, IACS

YEAR 2021: THE YEAR OF CYBER SECURITY IN MARITIME INDUSTRY

Abbreviations

- ABS: American Bureau of Shipping (a classification society)
- BIMCO: Baltic an International Maritime council
- CCS: China Classification Society
- CIA: Confidentiality, Integrity, Availability model
- ClassNK: Nippon Kaiji Kyokai, (a classification society)
- CSMS: Cyber Security Management System
- DCS: Distributed Control System
- DNV: Den Norske Veritas (a classification society)
- ENISA: The European Union Agency for Cybersecurity
- FAL: Facilitation Committee (IMO)
- IACS: Industrial Automation and Control System
- IACS: International Association of Classification Societies
- IEC: International Electrotechnical Commission
- IEEE: Institute of Electrical and Electronics Engineers Standards Association
- IMO: International Maritime Organization (under UN)
- IOT: Internet Of Things
- IT: Information technology
- MARPOL: The International Convention for the Prevention of Pollution from Ships
- MSC: Maritime Safety Committee (IMO)
- NIST: National Institute of Standards and Technology
- OT: Operational technology
- RP: Recommended Practice
- SC: Steering Committee (IACS)
- SCADA: Supervisory control and data acquisition system
- Suc: System under consideration
- SIEM: Security Information & Event Management
- UI: Unified Interpretations (IACS)
- UN: United Nations
- UR: Unified Requirements (IACS)

Preface

Abstract

Abbreviations

1 Introduction ... 8

1.1 Cyber Security and maritime IT and OT systems ... 8

1.2 Maritime industry and digitalization ... 13

1.3 Role of classification societies ... 16

1.4 Onboard Cyber Security and NAPA ... 17

2 Standards, relations and compliance requirements ... 18

2.1 Maritime ... 18

2.2 Non - maritime ... 18

2.3 FR - Fundamental requirements of IEC 62443-3-3 ... 19

2.4 NIST Framework for Improving Critical Infrastructure Cyber security ... 20

2.5 ANSSI Agence nationale de la securite des systems d'information ... 20

3 System under consideration: NAPA ... 21

3.1 Napa basic onboard parts ... 22

3.2 NAPA workstations ... 23

3.3 Other workstation software modules ... 26

3.4 NAPA servers ... 29

3.5 Services modules ... 29

3.6 Example installation ... 31

4 Frameworks offered by Classification societies ... 32

4.1 Common features ... 32

4.2 Relevance with NAPA ... 33

5 IACS ... 34

5.1 Introduction ... 34

5.2 Relevancy with NAPA ... 34

5.3 Required documentation from NAPA ... 36

5.4 Corresponding standards and regulations ... 36

5.5 Required additional certifications to be acquired by NAPA. ... 36

5.6 *Conclusions* ... 36
6 American Bureau of Shipping ... **37**
6.1 *Introduction* ... 37
6.2 *Relevancy with NAPA* ... 39
6.3 *Required documentation from NAPA* ... 39
6.4 *Corresponding standards* ... 39
6.5 *Required additional certifications to be acquired by NAPA.* ... 43
6.6 *Conclusions* ... 43
7 BIMCO ... **44**
7.1 *Introduction* ... 44
7.2 *Relevancy with NAPA* ... 46
7.3 *Required documentation from NAPA* ... 46
7.4 *Corresponding standards and regulations* ... 46
7.5 *Required additional certifications to be acquired by NAPA.* ... 46
7.6 *Conclusions* ... 47
8 Bureau veritas ... **48**
8.1 *Introduction* ... 48
8.2 *Relevancy with NAPA* ... 49
8.3 *Required documentation from NAPA* ... 49
8.4 *Corresponding standards and regulations* ... 50
8.5 *Required additional certifications to be acquired by NAPA.* ... 51
8.6 *Conclusions* ... 52
9 China Classification Society ... **53**
9.1 *Introduction* ... 53
9.2 *Relevancy with NAPA* ... 55
9.3 *Corresponding standards and regulations* ... 55
9.4 *Required documentation from NAPA* ... 56
9.5 *Required additional certifications to be acquired by NAPA.* ... 58
9.6 *Conclusions* ... 58
10 ClassNK ... **59**

10.1 Introduction ... *59*
10.2 Relevancy with NAPA ... *61*
10.3 Required documentation from NAPA ... *61*
10.4 Corresponding standards and regulations ... *61*
10.5 Required additional certifications to be acquired by NAPA. ... *62*
10.6 Conclusions ... *62*
11 DNV ... **63**
11.1 Introduction ... *63*
11.2 Type Approval DNVGL-CP-0231: ... *65*
11.3 Relevancy with NAPA ... *66*
11.4 Required documentation from NAPA ... *66*
11.5 Corresponding standards and regulations ... *67*
11.6 Required additional certifications to be acquired by NAPA. ... *67*
11.7 Conclusions ... *67*
12 Lloyd's ... **68**
12.1 Introduction ... *68*
12.2 Relevancy with NAPA ... *69*
12.3 Required documentation from NAPA ... *70*
12.4 Corresponding standards and regulations ... *71*
12.5 Required additional certifications to be acquired by NAPA. ... *71*
12.6 Conclusions ... *71*
13 End conclusions ... **72**
14 References: ... **73**
Appendix 1. Maritime Cyber Security for NAPA onboard ... **75**
Appendix 2 Definitions ... **76**

1 Introduction

NAPA Ltd is a maritime software and IT systems provider, based in Finland and other countries.
This thesis is a study of Onboard Cyber Security for NAPA, using class notations of a vessel and other class certifications as a framework (see definitions and abbreviations). In resulting pages, each major Classification Society and corresponding requirements for notation are studied and referenced for compatible NAPA products. As a result, we have a framework how to show compliance on a vessel and for the Classification Society selected for this ship. This will lead to faster commissioning, acceptance and further certifications and of course provide measures for the resilience for networked systems onboard against cyber-related risks, vulnerabilities and threats.

In general, the technical security requirements for onboard networked systems are based on the normative reference IEC 62443-3-3 (Industrial communication networks Network and system security Part 3-3: System security requirements and security levels)

This study excludes the use of ISO 9001:2015 Quality management and ISO 27000 information security standards, as the thesis handles onboard commissioning cyber security assessment only.
The two above mentioned are taken into account on shore side and supplier office and software development assessments, amongst others.

1.1 Cyber Security and maritime IT and OT systems

Most regulations and approval processes in commercial ship environments consider OT, as they include systems which directly affect critical control functions of the vessel.

Increased usage of onboard and onboard to shore integrated IT systems have changed the scenario and top-level regulations aim to address this challenge:

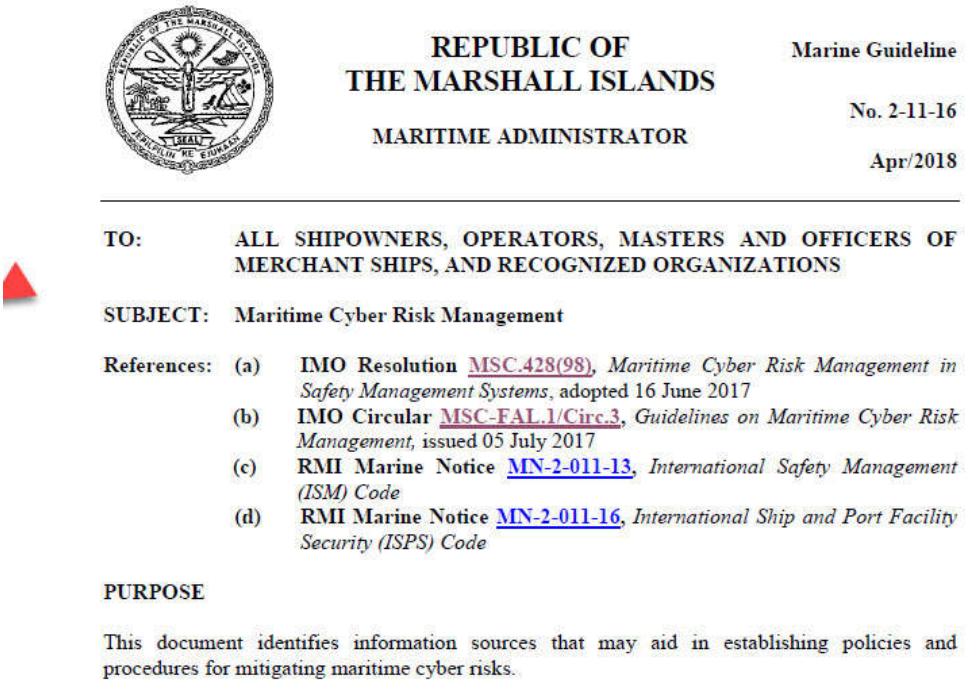
International Maritime Organization (IMO) Maritime Safety Council Resolution (MSC) MSC.428(98)
MSC-FAL.1-Circ.3 GUIDELINES ON MARITIME CYBER RISK MANAGEMENT
IACS UR E22, On Board Use and Application of Computer Based Systems
IACS Rec.166, Recommendation on Cyber Resilience

Table 1. International top-level regulations of maritime cyber security

According to IMO guidelines, distinction between information technology and operational technology systems should be considered [1]. Ship owners / operators approved safety management system address cyber risk management as a part of their safety

management system (SMS) latest after the first annual verification of the company's Document of Compliance after 1 January 2021 [2].

This makes the year 2021, the year of Cyber Security onboard



REPUBLIC OF THE MARSHALL ISLANDS

MARITIME ADMINISTRATOR

Marine Guideline

No. 2-11-16

Apr/2018

TO: **ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS, AND RECOGNIZED ORGANIZATIONS**

SUBJECT: **Maritime Cyber Risk Management**

References:
(a) **IMO Resolution** MSC.428(98), *Maritime Cyber Risk Management in Safety Management Systems*, adopted 16 June 2017
(b) **IMO Circular** MSC-FAL.1/Circ.3, *Guidelines on Maritime Cyber Risk Management*, issued 05 July 2017
(c) **RMI Marine Notice** MN-2-011-13, *International Safety Management (ISM) Code*
(d) **RMI Marine Notice** MN-2-011-16, *International Ship and Port Facility Security (ISPS) Code*

PURPOSE

This document identifies information sources that may aid in establishing policies and procedures for mitigating maritime cyber risks.

Figure 1.1. Marshall Island Maritime Administrator Guideline 2018 on Marine Cyber Risk Management

IT and OT systems onboard are also increasingly connected to each other. A good example of that is a NAPA system (IT), which reads data from a DCS (OT system). In some cases, our system can also send data to DCS.

Typical OT systems onboard could include:

- Cargo handling systems
- Propulsion and machinery handling systems
- Distributed Control Systems (DCS), which distribute networked control and monitoring stations to all manning stations around the ship

Typical IT systems onboard could include

- Email and VOIP communication
- Shore integrated ERP systems, handling e.g. procurement and maintenance processes
- Electronic logbooks
- Passenger management systems

Whereas IT systems manage data and support business functions, OT is the hardware and software that directly monitors/controls physical devices and processes and as such are an integral part of the ship and must function independently of the IT systems onboard [3].

The systems can, however, be connected to the IT network for performance monitoring, control and remote support. Such systems are sometimes referred to as belonging to the Industrial Internet of Things (IIOT). It is imperative that the process control systems or cyber-physical systems, be protected both physically and logically.

CIA model on IT and OT

CIA stands for:

- Confidentiality: Authentication of users and giving them an authorized access to a resource or to deny the forementioned
- Integrity: Ensuring that information is correct and not tampered with or erroneously recorded
- Availability: The used resource must be available and usable, otherwise it would be useless to invest in the system providing the resource

When considering IT and OT, there are differences when prioritizing the three factors of CIA - model:

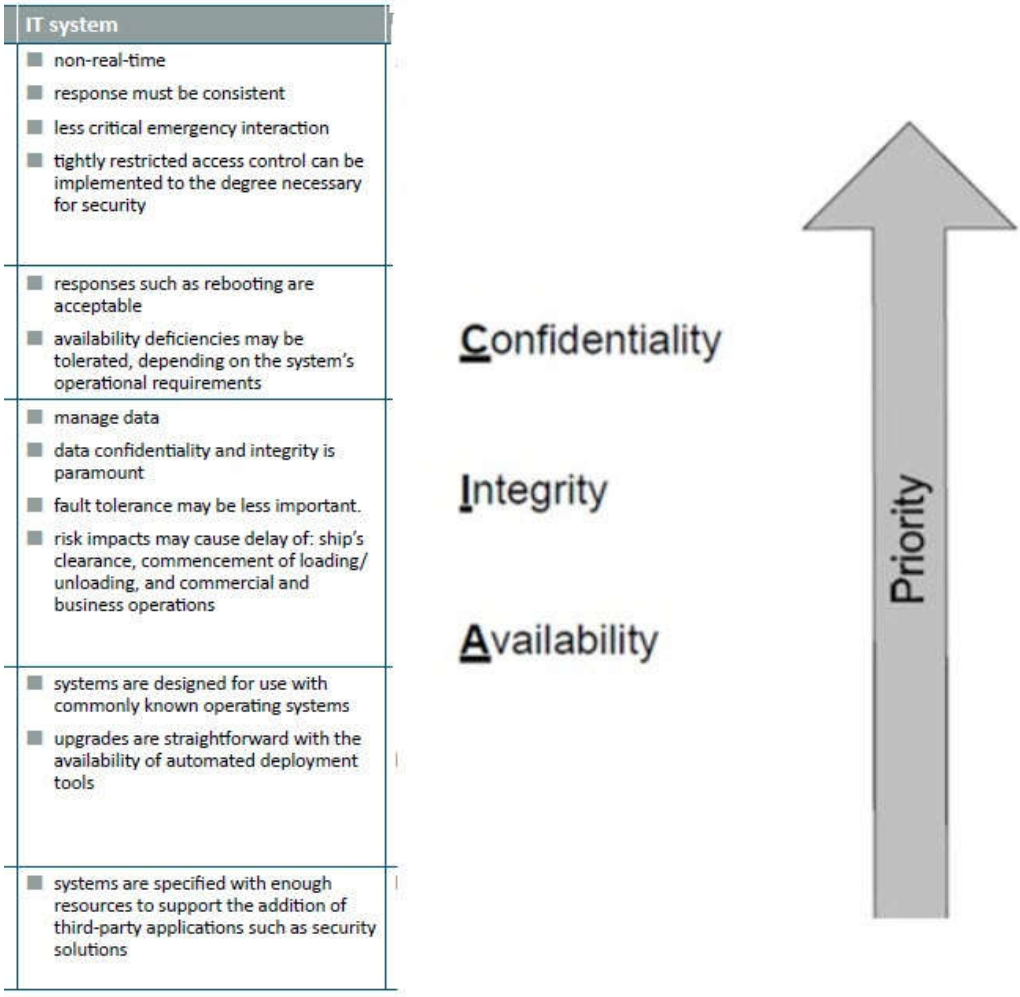


Figure 1.2. IT priority. IT considers confidentiality first, as it controls data.

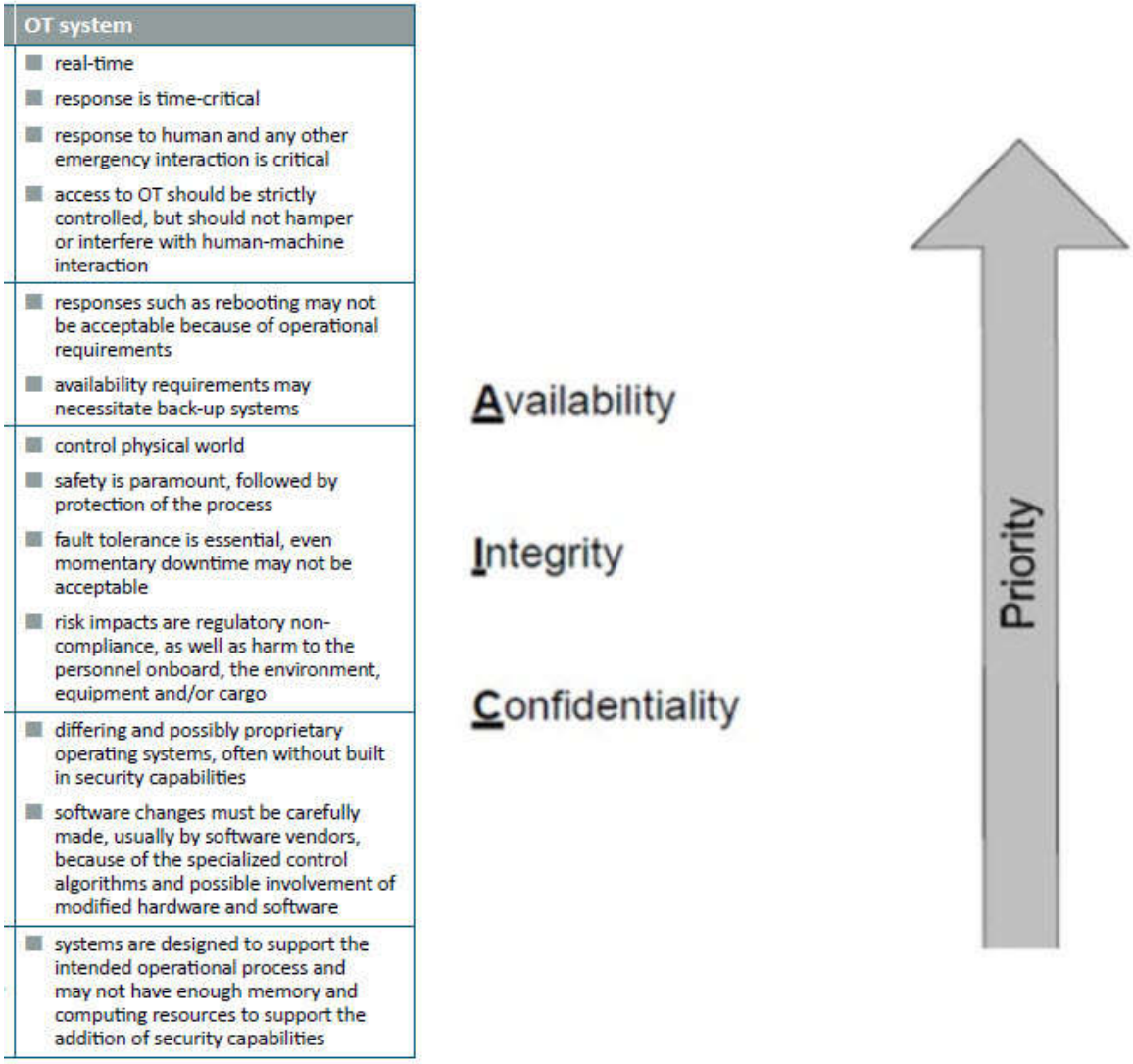


Figure 1.3. OT priority. OT Considers real time availability first since it controls physical world.

1.2 Maritime industry and digitalization

As all fields of maritime industry are aiming for digitalized era, this presents an enormous increase in requirements for cyber security [4].

Everything from ship design to operations are in the process of being "digitalized" in unprecedented scale.

This means more integrated data in datacenters, whereas data was before hidden or separated in paper documents.

It also means more data transported by internet and much more IOT on vessels.

OT systems control the physical world and IT systems manage data. OT systems differ from traditional IT systems. OT is hardware and software that directly monitors/controls physical devices and processes. IT covers the spectrum of technologies for information processing, including software, hardware and communication technologies Traditionally OT and IT have been separated, but with the internet, OT and IT are coming closer as historically stand-alone systems are becoming integrated. Disruption of the operation of OT systems may impose significant risk to the safety of onboard personnel, cargo, damage to the marine environment, and impede the ships operations [3].

Both increased IOT and merging IT and OT increase the attack surface quite substantially:

Maersk Bogor container ship approaches Middle East terminal (Source: Maersk)

State-sponsored criminals accused of Maersk IT cyber attack

Figure 1.4. Maersk Cyber Attack

Merchant marine ships are increasingly complex entities, using integrated and separate automation and IOT networked systems. Nowadays, separate systems on board, are not only connected to each other, but to the open internet as well. This has been made possible by high speed satellite-based internet connection systems, that have brought previously isolated ships to nearly shore side system internet connectivity [5].

Naturally, this has increased cyber security threat level onboard, with some high-profile incidents, bringing huge ships to a halt. Requirements in the Class rules aim to ensure that sufficient and correctly performed cyber security barriers are established to prevent, mitigate and respond to cyber-attacks. The barriers are a combination of technical, organizational and behavioral measures implemented onboard the vessel. Cyber security barriers for onshore facilities and organization are not covered in these rules [6].

For the asset owner/ asset operating organization to have a complete approach to cyber security, the onshore facilities and land organization should also be addressed. For such a purpose, it is recommended that e.g. ISO 27000 or IEC 62443 series or similar is applied. If the asset owner/ asset operating organization holds a valid ISO 27000 certificate, the requirements in these rules are intended to be a subset adapted for a single vessel.
However, the evaluation of onshore organization sis out of the scope of this study.

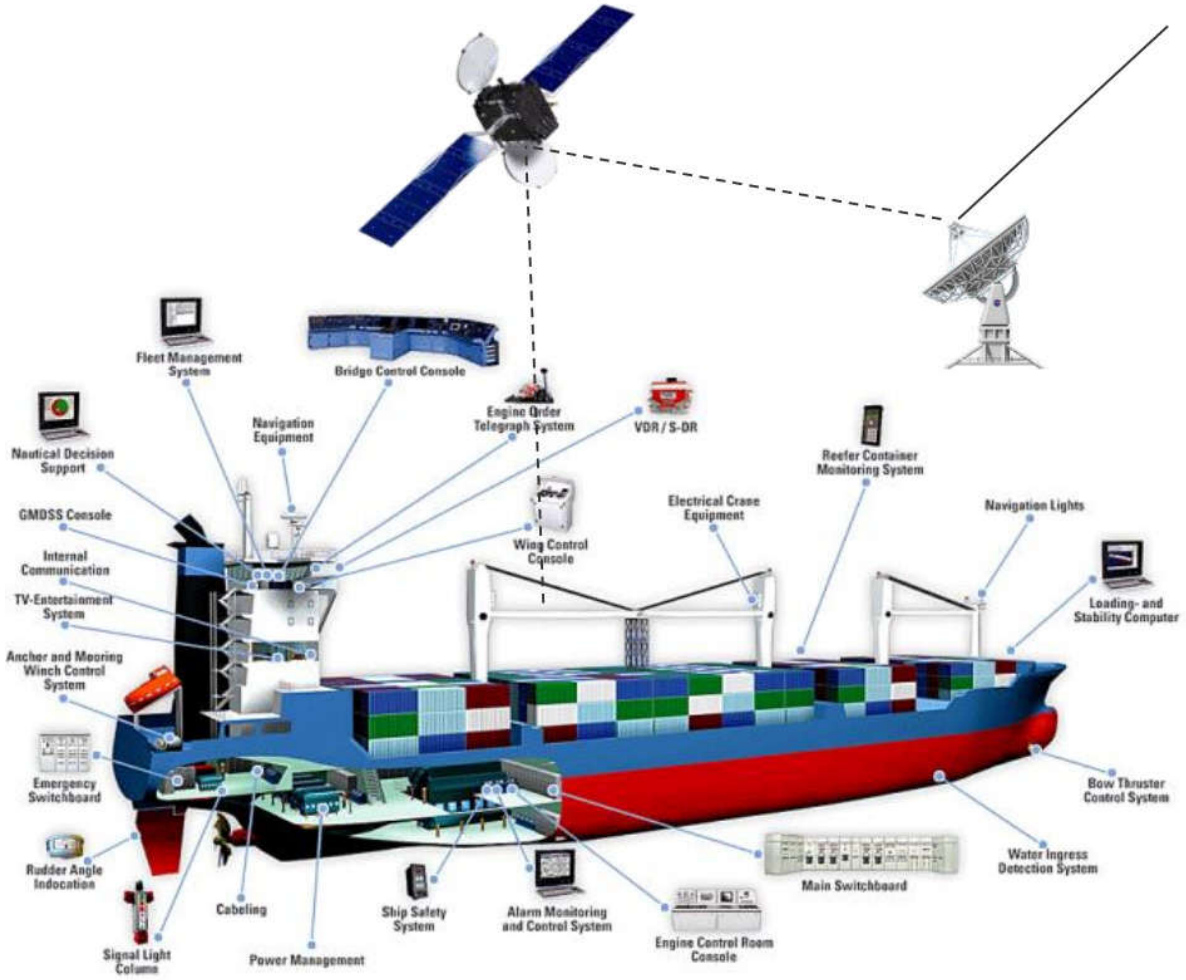


Figure 1.4. Multi-integrated environment of a modern merchant ship

1.3 Role of classification societies

For ships, the classification societies help to assess this situation by providing "class notations" where achieved cyber security capability is documented and verified.

These could include:

- ABS, CyberSafetyTM notation
- Bureau Veritas Cyber Managed and Cyber Secure notations
- CCS, Cyber Security (P, S) notation
- ClassNK, class notation "CybR-G"
- ClassNK, Digital Smartship notation
- DNV, additional class notation "Cyber Secure"
- Lloyd's Shipright Cyber Security notation

Class notations are mentioned in the certificate of class document of the vessel, provided by the classification society. They describe if the ship is compliant with the required standards for achieving the notation.

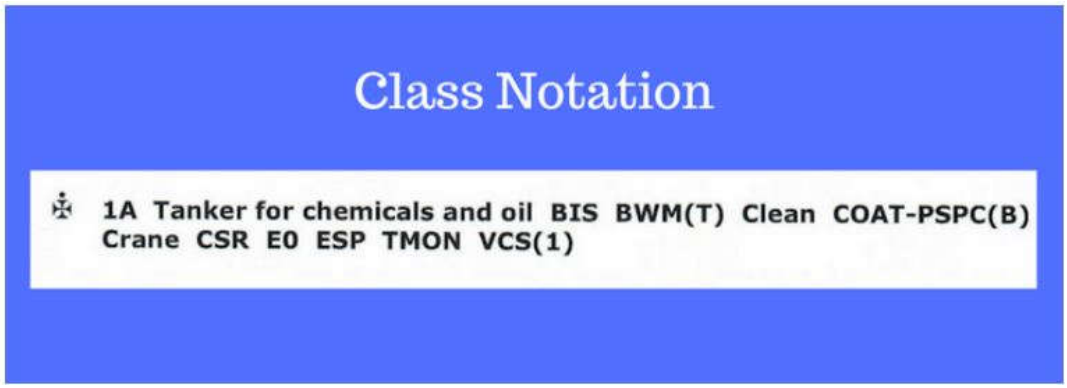


Figure 1.5. Another example of a Class Notation

Other approvals / certifications by Class societies are:

- Type Approvals for a specific product
- Class Society Specific Cyber Security Certificates

Above the classification societies, exists IMO (International Maritime Organization under UN), IACS (International Association of classification Societies) and Bimco (Baltic an International Maritime council) which is an organization which aims to assist ship owners and operators. IMO and IACS rules are referenced in this study when they from a basis for Class Rules. Bimco is studied as reference in chapter 9 since they do provide extensive Cyber Security advice although they are not a classification society.

1.4 Onboard Cyber Security and NAPA

The facilities where NAPA products are used, are not static production sites, but moving vessels which trade and transport globally.

While trivial cyber security enhancements are easier to achieve, getting certified or accepted to a Class Notation is a highly complex matter. With trivial enhancements we mean security improvements by using anti-malware software, limited privileges, encryption and system hardening.

Class notation requirements usually are relevant to essential and critical systems only, and many times NAPA products do not fall straight into this category. E.g. Loading computers (see chapter 5) are many times excluded, but still the owners would require that NAPA systems as a whole are included in "certification" of some kind e.g. ClassNK Smarts Ship notation.

Thus, for NAPA one of the biggest challenges is that while many Class requirements exempt NAPA systems, because they are not purely critical Operational Technology products controlling ships vital functions. This line is vague, since e.g. NAPA Loading Computer does have a mandatory function on ensuring stability on board, while not being exactly a SCADA device. NAPA Online is connected to OT but is only rarely used for more than reading data, while having a capability of sending data as well but not control commands.

For other certifications, challenge is that so far we have lacked holistic view on cyber security on our ship installations. Focus has been on individual settings and isolated issues on certain products. There has been significant improvement during last couple of years and we do have a certification for our monitoring product and a type approval for our loading computer.

More on NAPA product details in chapter 3. System under consideration.

This thesis is an applied research, which aims to answer mentioned challenges and to create systematic policies from sales to development ad onboard commissioning which will pave the way for better cyber security onboard when NAPA products are used.

2 Standards, relations and compliance requirements

Cyber Security standards, maritime and non - maritime [7]

2.1 Maritime

- IMO FAL.1/Circ.3 2017-07-05
- IACS UR E22
- IACS recommendations
- BIMCO Guidelines on Cyber Security Onboard Ships Version 3, 2018
- IEC 61162 Standard: "Digital interfaces for navigational equipment within a ship"
- ISO 16425:2013 Standard: Guidelines for the installation of ship communication networks for shipboard equipment and systems

2.2 Non - maritime

- NIST 800 Cyber Security Framework
- ISO27001/2 Specification for an information security management system (ISMS)
- ISO/IEC 62443 Standards for network and system security, especially:
- **IEC 62443-3-3 Industrial communication networks. Network and system security requirements and security levels**
- ANSSI “Agence nationale de la securite des systems d'information “
- And others, software development related

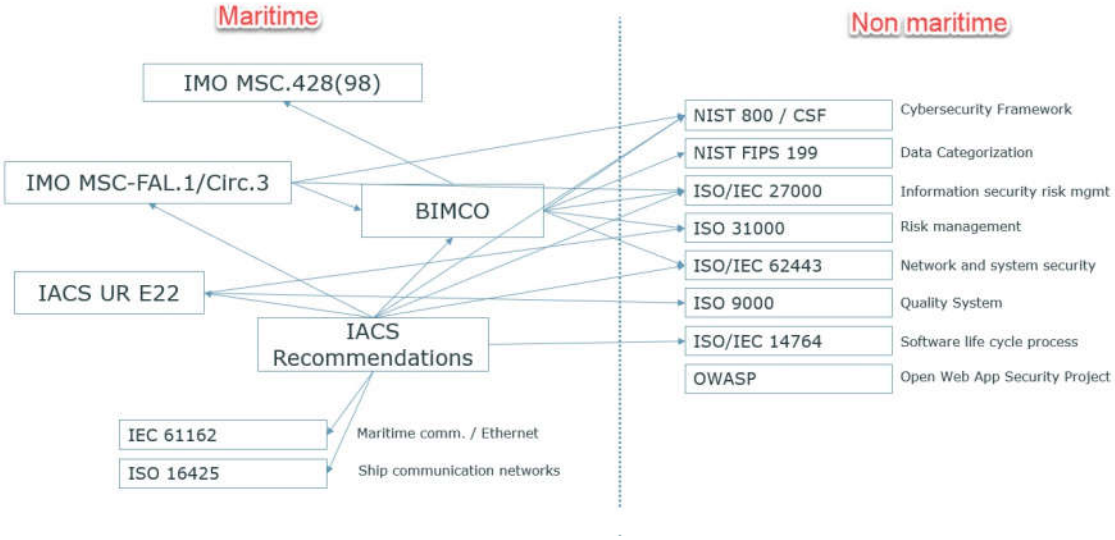


Figure 2.1. Maritime and non-Maritime standards and regulations [7]

2.3 FR - Fundamental requirements of IEC 62443-3-3

Especially the IEC 62443-3-3 is often refenced in requirements, since the cyber security assessed systems are always networked.

Table 1. IEC-62443-3-3 Fundamental Requirements for cyber security (FR)

FR	Description	Explanation	Customer Requirement example
FR1	Identification and authentication control	Identification and authentication of human users, software applications	2.7.2.1 Implementation of access control, Authentication and session-management
FR2	Use control	Assignment and control of privileges and authorizations for the identified user	2.7.2.1 Implementation of access control, Authentication and session-management
FR3	System integrity	Protection of the integrity of components or systems	
FR4	Data confidentiality	Protection of data	
FR5	Restricted data flow	Segmentation of the control system. Refer to the concept of zones and conduits	
FR6	Timely response to events	Monitoring, recording and reporting of security incidents	
FR7	Resource availability	Availability of the component and its applications	

2.4 NIST Framework for Improving Critical Infrastructure Cyber security

The NIST framework, is not directly Maritime related, but it gives the following core framework for all Cyber Security [8]:

- Identify: System inventories, management databases and installation drawings, risk assessments
- Protect: Used protective measures and safeguards against Cyber Security events
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- Recover: Recover Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

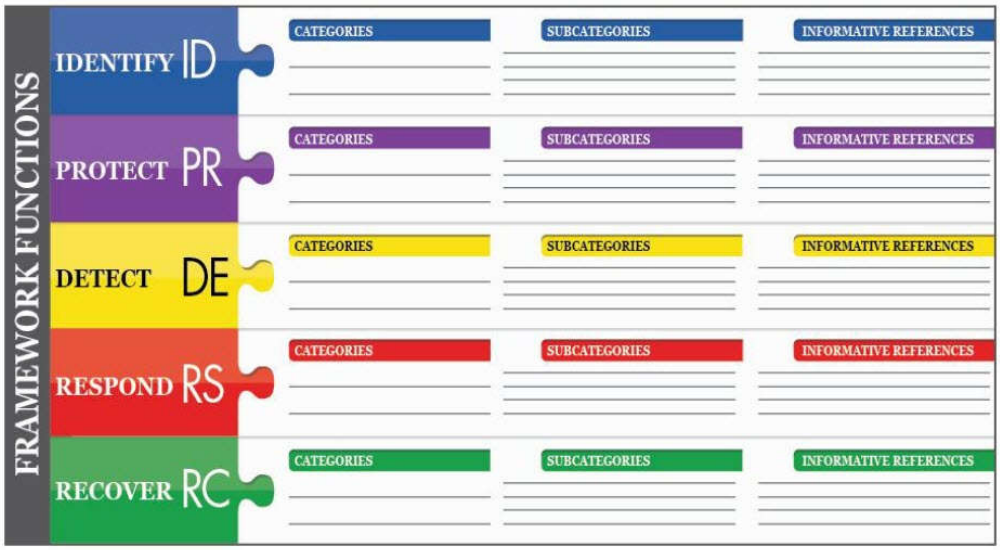


Figure 2.2 NIST Framework

2.5 ANSSI Agence nationale de la securite des systems d'information

The “Agence nationale de la securite des systems d'information (ANSSI; English: French National Cybersecurity Agency) is a French service created on 7 July 2009 with responsibility for computer security. ANSSI is used as a normative reference in Bureau Veritas additional class notations.

3 System under consideration: NAPA

In an order to get an idea what actually needs to be evaluated for compliance and cyber security, in this chapter we will describe the systems under consideration (Suc). System under consideration (Suc) signifies the cyber-physical systems to be secured [9].

Napa Onboard solutions are combination of hardware-modules and solutions, which are sold under different brands.

Cyber Security requirements apply to the software and hardware supporting the software [10].

For following components, NAPA is considered as SUPPLIER. The Supplier is the contracted or subcontracted provider of system components or software [10].

Since these are networked computer devices, following base standards apply, regardless of the classification society:

- IEC 62443-3-3 Industrial communication networks. Network and system security requirements and security levels
- NIST 800 Cyber Security Framework

3.1 Napa basic onboard parts

Windows hosts

- Marine approved HP computers (Model G6 at the time of writing) [11]
- Same model is used as workstations, servers and so called "communication PC"
- NAPA Workstation: For running NAPA client software, when workstations delivered by NAPA (If agreed, they can also be provided by customer)
- NAPA Server: A HP G5 model used as a server machine
- NAPA Communication PC: For running software which integrate with physical devices, such IACS, DCS and navigational equipment for measurement reading
- NAPA EC Server: Server computer to serve NAPA Emergency computer.
- Windows operating system: The operating system version must be the latest NAPA supported Windows version at the time of delivery, hardened according to NAPA Onboard Solution Cyber Security Hardening Guidelines [12]

3.2 NAPA workstations

NAPA Loading Computer / NAPA Stability

Ships equipped with a Loading Computer aka Stability computer must have it approved by the ships Class. Loading computers typically do have integration with automation / DCS systems, which makes them part of any cyber security assessment, even though stability computers exclusively are often excluded.

Figure 3.1. Loading Computer

Loading Computer consists of:

- Approved Marine PC
- Windows Operating system
- Loading computer / NAPA Stability Software

There are currently four types of stability software, all of which have varying levels of capability.

- Type 1 has software that only calculates intact stability.
- Type 2 can calculate intact stability and check damage stability based on a limit curve (e.g. for vessels applicable to SOLAS Part B-1 damage stability calculations).
- Type 3 calculates intact and damage stability by direct application of pre-programmed damage cases by reference to the relevant Conventions and/or Codes for each loading condition.
- Type 4 is the most advanced of them all. It calculates damage stability associated with an actual loading condition and/or actual flooding cases, by using the direct application of user or sensor defined damage to enable a safe return to port (SRtP).

Since the start of 2020, all passenger-carrying new buildings have been required to have a Type 4 Loading Computer installed. Passenger ships constructed before 1 January 2014 must also comply with this requirement no later than the first renewal survey after 1 January 2025.

NAPA Emergency computer

Emergency computer runs a software which automatically detects the vessels vulnerability and survivability.

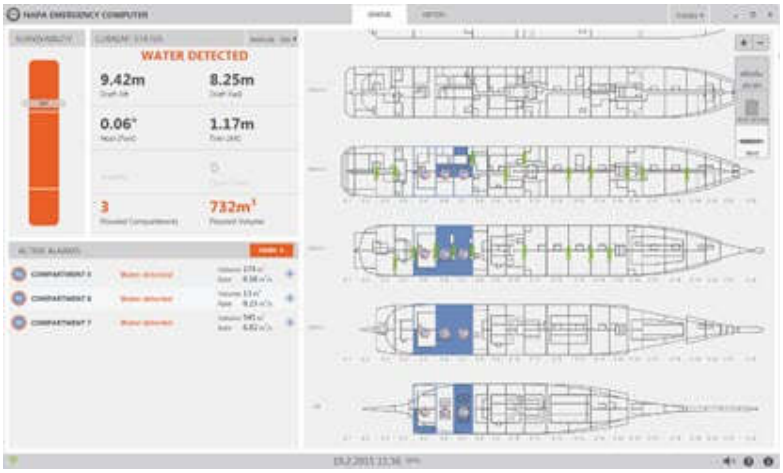


Figure 3.2. Emergency Computer

Emergency computer needs data from NAPA Server, which is connected to the ship DCS / IAS systems and other data sources.

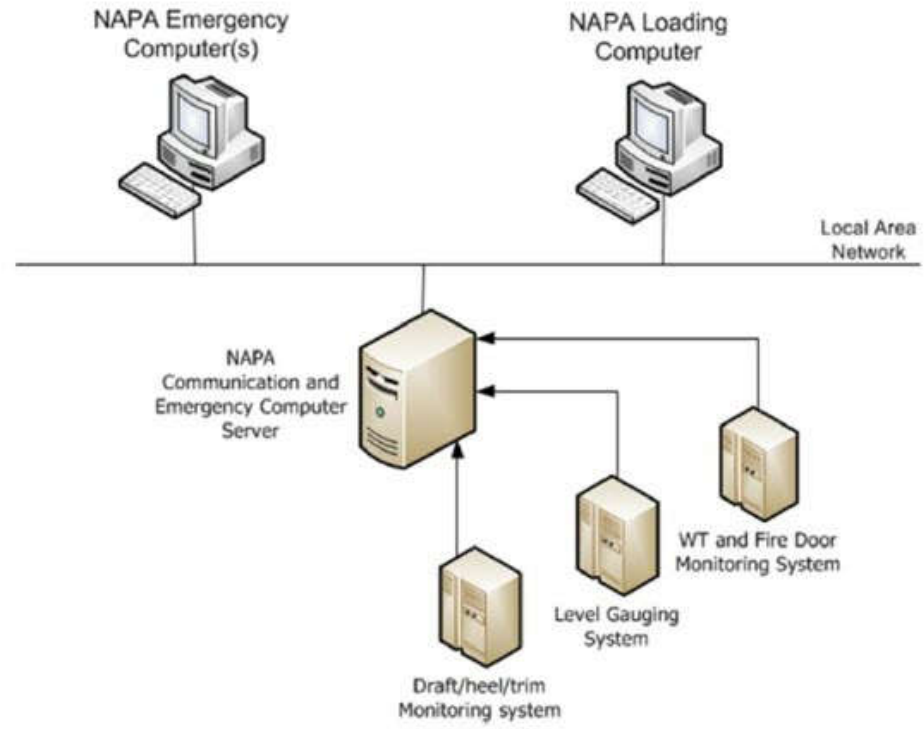


Figure 3.3. Emergency Computer in network

General NAPA workstation

- A marine approved windows computer, which can run any combination of NAPA client software

3.3 Other workstation software modules

NAPA Electronic Logbook

NAPA Logbook client software works as a replacement for paper logbooks. On many modern ships, logbooks are so large and complex, that using paper logbooks is not a viable option anymore.

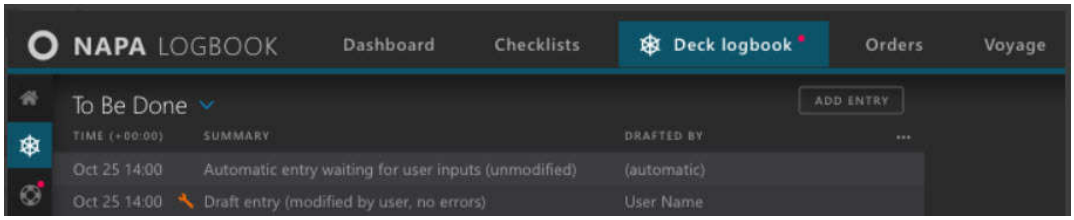


Figure 3.4. NAPA Logbook

NAPA Real Time Monitoring

NAPA Real Time Monitoring is an awareness tool for the crew, where all data can be shown in configurable displays and status boards.

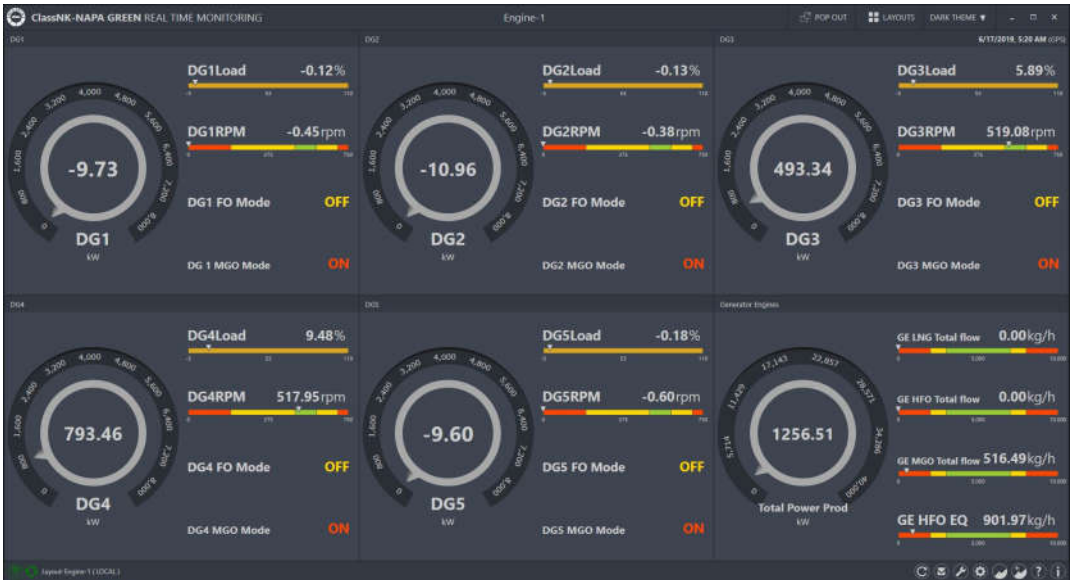


Figure 3.5. NAPA Real Time Monitoring

Cloud based software onboard

NAPA Fleet intelligence: Cloud based software which does not require interfacing This is a data driven software, which takes information from publicly available sources and combines it with NAPA collected data when available.

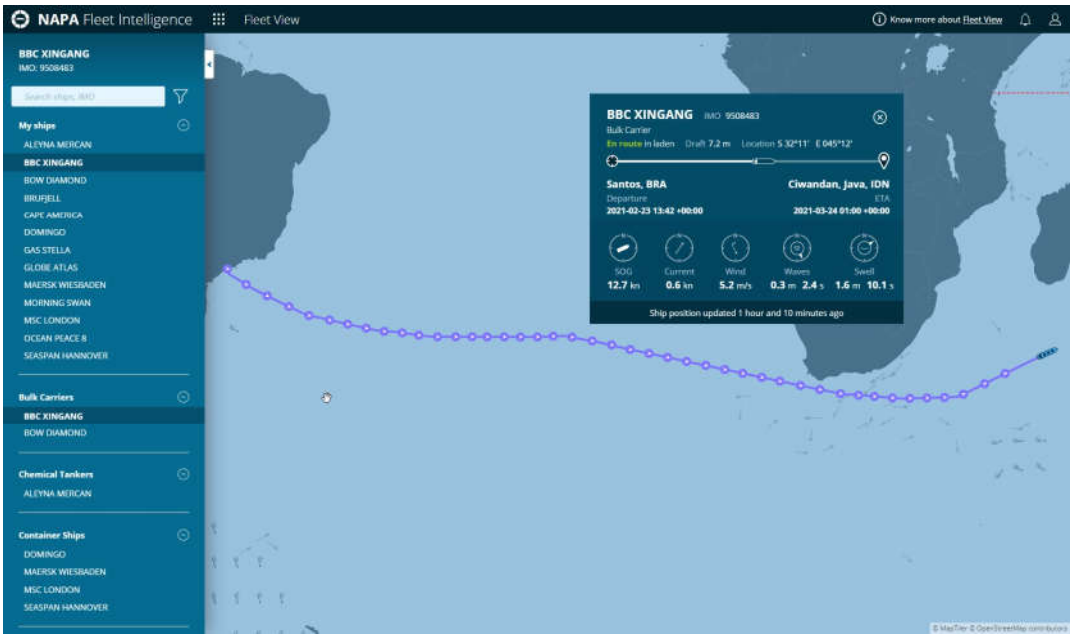


Figure 3.6. Fleet Intelligence

3.4 NAPA servers

Communication PC

Communication PC is a workstation, which handles interfaces to third party instruments, devices and sensors. It also handles data transfer for collected data to our cloud service, using ship satellite internet. This might be combined with the Log server.

Log server

Runs the NAPA Logbook server service. Can be run on the communication PC or a separate machine. Need a relational database (MS-SQL or PostgreSQL) installed as well. Database service can be run on a dedicated server if client has one available.

3.5 Services modules

Different windows service modules are run in NAPA Server, Communication PC or Workstation depending of the installation requirements onboard.

NAPA Bus

- An ActiveMQ messaging server for interconnected NAPA Modules communication
- All modules mentioned below and client software use NAPA Bus to communicate with each other

NAPA Calculation module

- Internal module for "trim efficiency calculation"

NAPA Datatransfer

- Reads messages to be sent to NAPA Office cloud service and receives them as well
- Used vessel satellite internet connection system to communicate with open internet

NAPA Log

- NAPA Electronic Logbook service
- Requires a relational database. Either PostgreSQL or MS-SQL server
- Acts as data storage, and message creator for NAPA Data transfer

NAPA Online

- Online reads and writes data to physical devices connected to the NAPA host, where it is running
- Connections could include SCADA, IACS and navigational systems, e.g. GPS for reading vessel position
- Online supports various general and proprietary communication protocols as Modbus, ModbusTCP, NMEA, OPC etc
- Online is almost Operational Technology (OT):

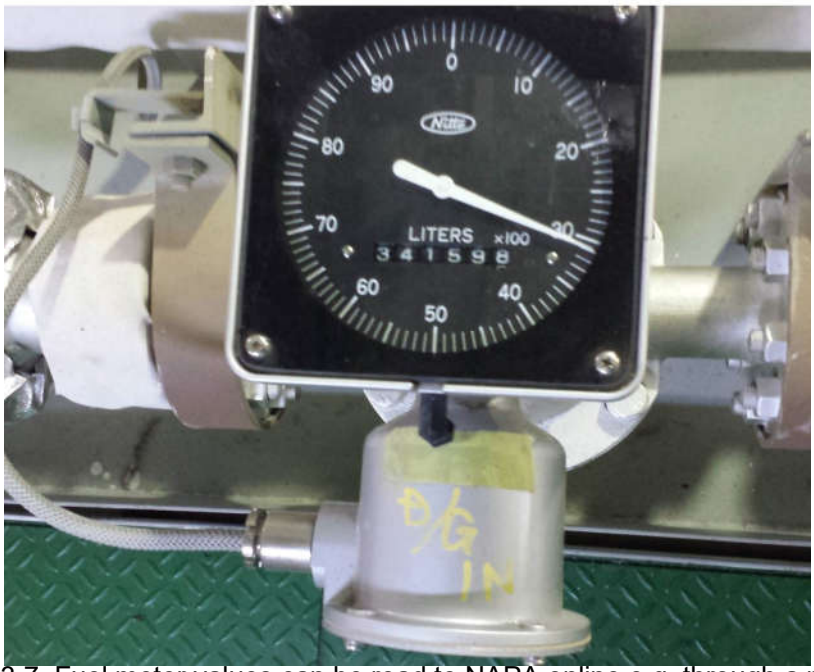


Figure 3.7. Fuel meter values can be read to NAPA online e.g. through a modbus PLC connection or as part of DCS interface.

NAPA System Monitoring View

- Small applet monitoring service modules
- Graphical interface, which warns user if modules malfunctioning

NAPA VCR

- Vessel configuration repository
- For centrally managing configuration files for different NAPA hosts from the server

3.6 Example installation

Figure shows a typical cargo ship installation, with network segmentation, serial SCADA connections and a satellite connection to internet.

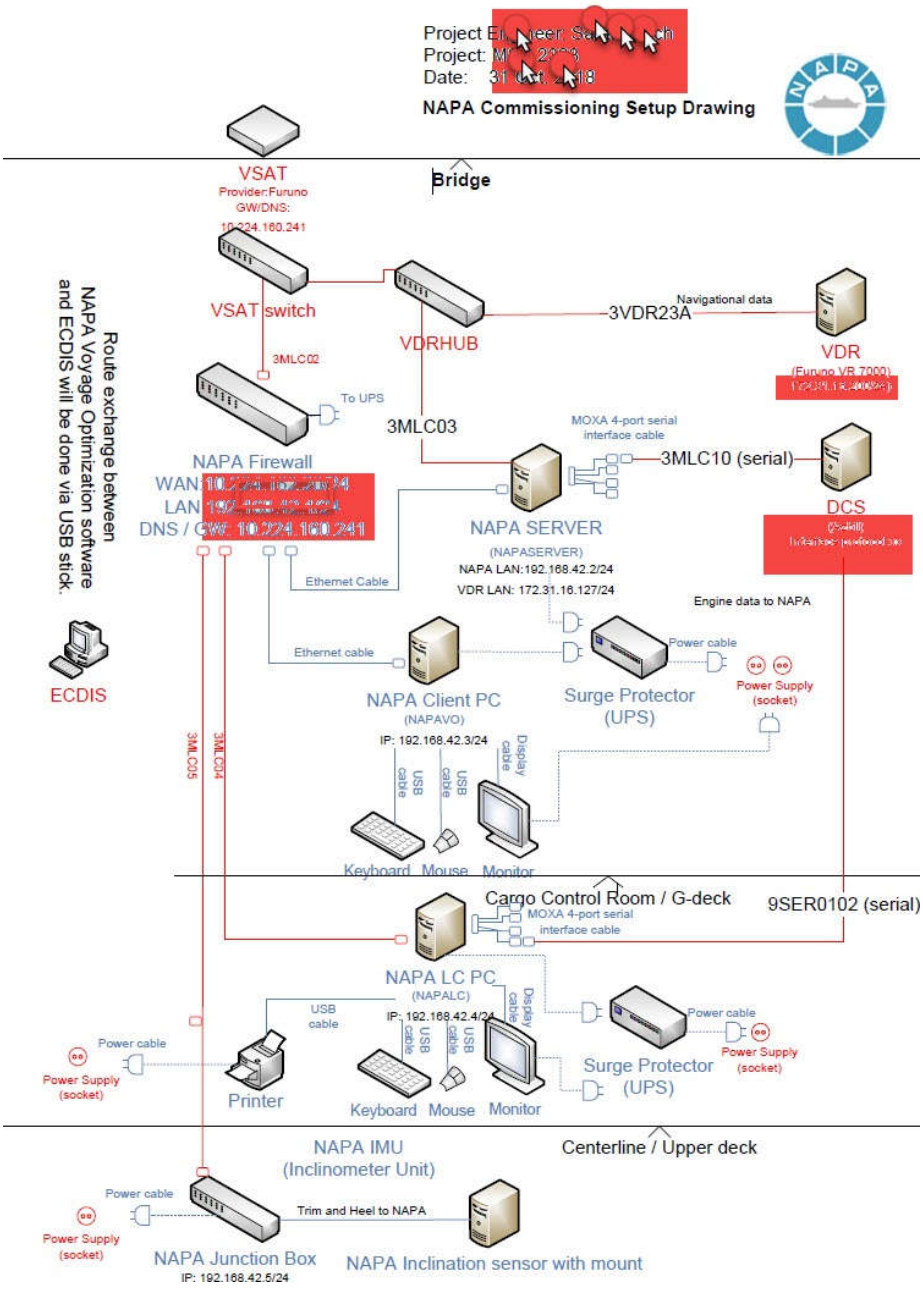


Figure 3.8. Typical cargo ship installation (some data redacted with red color)

4 Frameworks offered by Classification societies

4.1 Common features

In following chapters, we will assess the frameworks offered by major classification societies and maritime entities, and how they can be used to assess cybersecurity on ships where different NAPA products are used.

The notation frameworks have certain common features:

- They are based on class best practices, class programmes, class guidance and class rules published by the classification society
- Above mentioned are based on standards and requirements, e.g. "ISA/IEC 62443 Security for Industrial Automation and Control Systems"
- They aim to cover IMO MSC.428(98) and MSC-FAL.1-Circ.3 - "Guidelines On Maritime Cyber Risk Management" requirements and IACS URE22 “On Board Use and Application of Computer based systems”
- An inventory of Cyber Assessed System is done
- Zones and conduits are defined in an order to describe segregated network zones
- Cyber Security Consequence - Likelihood matrix (how bad - how often) is provided
- Levels of Cyber Security targets are defined based on the CS matrix

4.2 Relevance with NAPA

For each classification society, we inspect the following:

- Relevance with NAPA
- Required documentation from NAPA
- Corresponding standards and requirements
- Required additional certifications to be acquired by NAPA.
- Conclusions

Certificate No. 18 -SSQ-002

NIPPON KAIJI KYOKAI
ClassNK
Founded 1899

Certificate
of
Compliance

THIS IS TO CERTIFY that the below-mentioned software has successfully validated the

Software Security Quality

Of

ClassNK-NAPA GREEN Monitoring
Version D

developed by

NAPA
Tammasaarenkatu 3 FI-00181 Helsinki, Finland

Figure 4.1. Certificate of compliance by ClassNK

5 IACS

5.1 Introduction

International Association of Classification Societies:

IACS rules (RU), unified requirements (UR) and recommendations form a basis for the individual Classification Society class notation rules for Cyber Security. For this reason, the basis of those are described here.

IACS rules and recommendations:

1. IACS UR E22, "On Board Use and Application of Computer Based Systems"
2. IACS Rec.166, "Recommendation on Cyber Resilience"
3. IACS UR L5, "Computer Software for Onboard Stability Calculations"

5.2 Relevancy with NAPA

Sometimes owners refer directly to UR E22 AND IACS REC 166, bypassing the class notation or certifications.

IACS UR E22 On Board Use and Application of Computer based systems

These requirements apply to design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions. The requirements focus on the functionality of the software and on the hardware supporting the software. These requirements apply to the use of computer-based systems which provide control, alarm, monitoring, safety or internal communication functions which are subject to classification requirements. Since UR E22 concerns only systems under classification requirements, this excludes our monitoring software. Logbook, when used as official Electronic Logbook falls under this category.

- Exclusion: Navigation systems required by SOLAS Chapter V, Radiocommunication systems required by SOLAS Chapter IV, and vessel loading instrument/stability computer are not in the scope of this requirement [10]

IACS Rec 48. considers NAPA Loading Computer or Stability Computer.

IACS REC 166 Recommendation on Cyber Resilience

The Recommendation is based on the application of IACS UR E22 and is a kind of abbreviated explanation of the UR E22. The recommendation applies to onboard OT systems and other systems which are connected to onboard OT systems in a way that may affect their operation. The recommendation was formed in April 2020 and amended in July 2020 and is to be translated into a Unified Requirements of IACA members and later to be incorporated into the members mandatory class rules.

System Categories (I, II, III): System categories based on their effects on system functionality, which are defined in IACS UR E22.

- 'I. Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
- 'II. Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
- 'III. Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Category	Effects	System functionality	Confidentiality	Integrity	Availability
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Monitoring function for informational / administrative tasks	Low	Moderate	Low
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Alarm and monitoring functions Control functions which are necessary to maintain the ship in its normal operational and habitable conditions	Moderate	High	Moderate
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Control functions for maintaining the vessel's propulsion and steering Safety functions	Moderate	High	High

Figure 5.1 IACS Categories

5.3 Required documentation from NAPA

- Inventory of provided products, system drawings
- Risk assessment, respond and recovery plan

5.4 Corresponding standards and regulations

Name	**Description**
IMO MSC-FAL.1/Circ.3	Guidelines on Maritime Cyber Risk Management, July 2017
BIMCO	The Guidelines on Cyber Security Onboard Ships, version 3.0, 1.1 2018

5.5 Required additional certifications to be acquired by NAPA.

- N/A

5.6 Conclusions

While UR E22 specifically targets products that require Class Approval, it specifically excludes Loading / Stability Computer, which has an approval procedure of its own.

In reality all customers will be requiring that we are compliant with UR E22, starting from 2021.

6 American Bureau of Shipping

6.1 Introduction

American Bureau of Shipping (ABS), is American maritime classification society is established in 1862, with headquarters in Houston Texas.

The Class Notation CS is based on ABS FCI Cyber Risk Model.

The notation is assigned to ships and offshore assets that comply with ABS requirements contained in the **ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries ABS CyberSafetyTM Volume 2** and is available for all classed vessels complying with the IMO International Safety Management (ISM) Code [13].

Compliance with the procedures and criteria given in this Guide may result in issuance of a:

- CyberSafety Management System Certificate (CMSC)

Or:

- Certificate of Cyber Compliance (CCC) for the Company's examined Facility or vessel under construction [14]

Or:

- A class Notation CS1, CS2, CS3, to an ABS classed ship or offshore asset upon request. Ships and offshore assets not classed by ABS can be issued a Statement of Fact when they are in conformance with the requirements of this Guide

The CS notation may be assigned as follows:

- CS1 Informed Cybersecurity Implementation (Basic)
- CS2 Rigorous and Repeatable Cybersecurity Implementation (Developed)
- CS3 Adaptive Cybersecurity Implementation (Highest level of Readiness) (Integrated)
- The + CS Notation may itself be annotated in the case of a Company that certifies a facility or facilities in addition to vessel(s). The Notation would thereby reflect as CS1+, CS2+, or CS3+. This is expected in cases of advanced vessels that will link control systems between vessel and onload/offload facility to regulate cargo or hazardous operations through cyber-enabled systems.

The intent of the CS Notation series is to define boundaries of critical systems in the shipboard networked environment. Primary Essential Services, as defined by Integrity Levels and criticality to human, asset or environmental safety, are to be protected for a vessel or unit to be eligible for the CS notation, within the defined system boundaries [14].

FIGURE 1
Cybersecurity Notation Hierarchy

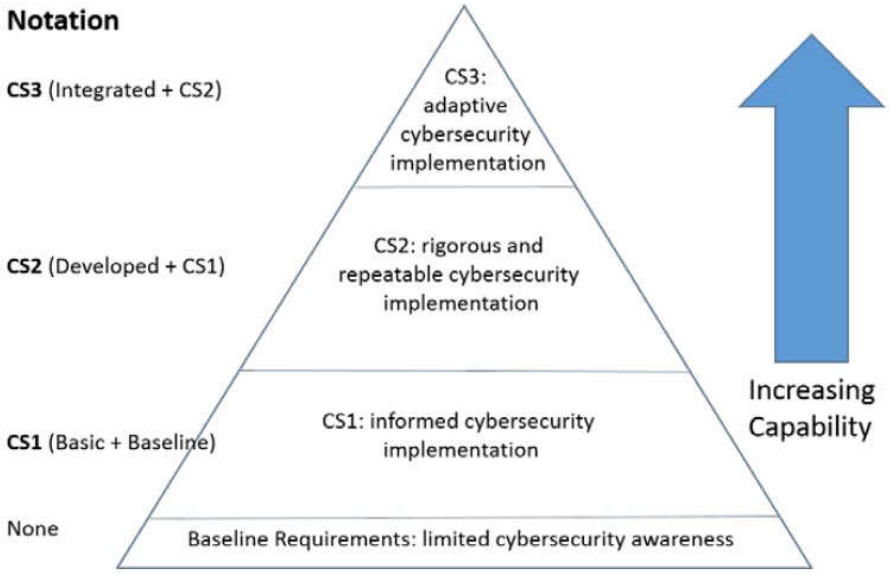


Figure 6.1.ABS CyberSecurity Notation Hierarchy

6.2 Relevancy with NAPA

New buildings and companies, which have ABS as Classification Society. ABS cyber-security implementation for the marine and offshore industries aims to have Cyber Security Assessment nowadays always included, and we need to be able to answer building yard requirements, which are based on ABS, when a Cyber Security Class Notation is prepared for the ship.

At the time of writing of this thesis we do have several hundred product deliveries onboard ships with ABS as classification society. Products include the whole portfolio from safety to monitoring systems.

6.3 Required documentation from NAPA

- Functional Description Document
- Risk Analysis document
- System Architecture: Line drawings of the control system, network topology, interface information, communication protocols information, new or unproven technology, and software version.

6.4 Corresponding standards

Standard	**Description**
IEEE Std 14764-2006	Software Engineering Software Life Cycle Processes Maintenance, Second edition 2006-09-01
IEEE Std 12207-2008	Second edition, 2008-02-01
IEEE Std 730-2002	IEEE Standard for Software Quality Assurance Plans
IEEE Std 1012-2004	IEEE Standard for Software Verification and Validation

IEEE Std 1016-1998	IEEE Recommended Practice for Software Design Descriptions
IEEE Std 1219-1998	IEEE Standard for Software Maintenance
IEEE Std 1362-1998 (R2007)	IEEE Guide for Information Technology System Definition Concept of Operations (ConOps) Document
IEEE SWEBOK 2004	Software Engineering Body of Knowledge
IEC 61508-0 (2005-01)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 0: Functional safety and IEC
IEC 61508-1 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
IEC 61508-2 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electri-
IEC 61508-3 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements
IEC 61508-4 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbrevia-
IEC 61508-5 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 5: Examples of methods for
IEC 61508-6 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the appli-

IEC 61508-7 (2010-04)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 7: Overview of techniques
IEC 61511-1 (2003-01)	Functional safety Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system,
IEC 61511-2 (2003-07)	Functional safety Safety instrumented systems for the process industry sector, Part 2: Guidelines for the application of
IEC 61511-3 (2003-03)	Functional safety Safety instrumented systems for the process industry sector, Part 3: Guidance for the determination of
IEC 62351	Power systems management and associated information exchange - Data and communications security
ISA/IEC 62443	Industrial Automation and Control Systems Security) Standard of Good Practice for Information Security (Published by the
ISO 17894-2005	General principles for the development and use of programmable electronic systems in marine applications
ISO/IEC 9126-1:2001	Software engineering Product quality Part 1: Quality model
ISO 9001:2015	Quality Management Systems Requirements
ISO/IEC 20000-1:2011	Information Technology Service Management - Part 1: Service management system requirements
ISO/IEC 27001:2013	Information Technology - Security techniques - Information security management systems Requirements

ISO/IEC 27002:2013	Information Technology - Security techniques - Code of practice for information security controls
ISO 28001:2007	Security management systems for the supply chain; Best practices for implementing supply chain security, assessments and
ISO 31000:2009	Risk management Principles and guidelines
ANSI/ISA-84.00.01-2004	Part 2 (IEC 61511-2 Mod) Functional Safety: Safety Instrumented Systems for the Process Industry Sector Part 2:
National Institute for Science and Tech-	Framework for Improving Critical Infrastructure Cybersecurity Feb 2014.
Software Engineering Institute	The Capability Maturity Model: Guidelines for Improving the Software Process Reading
American Petroleum Institution (API)	Specification 16D Third Edition Draft: Control Systems for Drilling Well Control Equipment and Control Systems for Diverter
NERC CIP Standards (North American Elec-	Critical Infrastructure Protection (CIP)) - Targeted at the energy sector

6.5 Required additional certifications to be acquired by NAPA.

No mandatory additional certifications.
ABS offers product Design Assessment (PDA) and Service Provider approval certification solution [15].

ABS CyberSafety PDA

- Vulnerability Assessment of:
- Functional description
- List of components and software versions
- Vulnerability Analysis (includes remote and wireless vulnerabilities and controls installed)
- OEM and user access requirements
- Topology drawing to identify control system boundaries for protective equipment (routers, firewalls, etc.)
- Sub-supplier information
- OEM and sub-supplier installed cybersecurity protective equipment (routers, firewalls, etc.)

ABS CyberSafety Service Provider Approval

- Cyber Security Office
- Cybersecurity policies & procedures
- Risk management
- Change management
- Cybersecurity training programs
- External-facing incident responses team procedures

6.6 Conclusions

Especially new buildings under ABS Classification will be relevant when the owner aims to have the CS Notation in the ships Class Certificate. Vessels shall be assessed on an annual basis, when there are major cyber-enabled, safety-related networked system configuration changes, or with multi-year Class survey events when no major system configurations are changed.

7 BIMCO

7.1 Introduction

BIMCO guidelines on cyber security onboard ships:

BIMCO is the world's largest direct-membership organization for shipowners, charterers, shipbrokers and agents. The above are usually referred as "Shipping Companies", which is a broad term.

In total, around 60% of the world's merchant fleet is a BIMCO member, measured by tonnage.

Bimco requires that shipping companies should evaluate and include the physical security and cyber risk management processes of service providers in supplier agreements and contracts [16].

To facilitate this, Bimco provides "Guidelines on Cyber Security Onboard Ships" manual for shipping companies to use:

The Guidelines on Cyber Security Onboard Ships, version 3.0, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, WSC and IUMI, 2018

This Guidance gives shipowners and operators procedures and actions to maintain the security of cyber systems in the company and onboard the ships. The guidelines are not intended to provide a basis for, and should not be interpreted as, calling for external auditing or vetting the individual company's and ships approach to cyber risk management.

According to Bimco, processes evaluated during supplier vetting and included in contract requirements may include:

- security management including management of sub-suppliers
- manufacturing/operational security
- software engineering and architecture
- asset and cyber incident management
- personnel security
- data and information protection

Figure 7.1. Bimco Cyber risk management approach

7.2 Relevancy with NAPA

Our customers might be direct members of Bimco, so the they could potentially use the guidelines mentioned here.

7.3 Required documentation from NAPA

- See additional certifications

7.4 Corresponding standards and regulations

IMO resolutions	Maritime Safety Council Resolution (MSC) MSC.428(98)
NIST Framework	Improving Critical Infrastructure Cybersecurity Version 1.1, April 16 2018
IACS ur-e22	On Board Use and Application of Computer based systems rev2

- IMO resolutions
- NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 April 16, 2018
- IACS ur-e22 On Board Use and Application of Computer based systems rev2

7.5 Required additional certifications to be acquired by NAPA.

- ISO 9001:2015
- ISO 27001

7.6 Conclusions

Major shipping companies and oil majors can base their own supplier assessment or vetting procedures to Bimco Guidelines or NIST. No direct implication to onboard system deliveries:

Assessments are done prior to that.

8 Bureau veritas

8.1 Introduction

Bureau Veritas is a company specialized in the testing, inspection and certification founded in 1828 and operating worldwide from Paris. It operates in a variety of sectors not only as a maritime classification society. Its historical foundation is in ship classification, as originally ir provided insurers with information that enabled them to assess the reliability of ships and equipment.

Bureau veritas has two different notations in use [17].

Cyber Managed and Cyber secure:

- CYBER MANAGED for cyber security risk management
- CYBER SECURE for cyber security by design
- Both notations also have a version applicable to yards (CYBER MANAGED PREPARED & CYBER SECURE PREPARED)

The additional class notations CYBER MANAGED PREPARED, and CYBER SECURE PREPARED, may be assigned to new building only, on shipyard level. The additional class notations CYBER MANAGED and CYBER SECURE may be assigned to new building or to ships in-service.

Cyber Managed Prepared:

The additional class notation CYBER MANAGED PREPARED is assigned to a ship in order to reflect that a set of procedures including periodical and corrective maintenance, as well as periodical and occasional inspections of information systems or equipment and DCS or equipment, are in line with the design of the vessel and the inherent cyber security threats. The assignment of the notation implies that requirements for assignment of CYBER MANAGED PREPARED notation have been fulfilled in accordance with the following:

- Equipment are identified, inventoried, categorized in basic repository inventory
- Criticality, incident impact and cyber-attack likelihood of each equipment is assessed
- On board to on shore connections, vessel networks and operational technologies interconnections are designed in accordance to on board to on shore connections plan, vessel network plan and operational technologies interconnections plan
- Surfaces of attack and cyber resilience are assessed
- Monitoring, maintenance and incident response procedures are delivered in accordance of Bureau veritas Cyber Handbook [18]

Cyber Managed:

Applied primarily to in-service vessels, this new class notation aims to support ship owners in developing an approach to cyber risk management using safety standards similar to those already used onboard. In practice, this means that CYBER MANAGED employs a risk-based methodology and standardized framework to assess and protect ships from cyber risks [17].

With this notation, owners can be sure that their IT and OT systems have been detailed evaluated, the safety procedures are in place and also the crew members and personnel have the expertise needed, after being properly trained. Ship owners and contractors are requested to develop a complete map of IT and OT systems (Cyber Repository), high-level management principles (Cyber Policy) and detailed on-board procedures (Cyber Handbook).

Cyber Secure Prepared:

As Cyber Managed Prepared, for new buildings. Applies to newbuild vessels and provides a detailed, automated onboard and onshore cyber protection measures. This notation is in line with Cyber Managed notation and provides owners with additional security measures, concerning automatic digital updates, procedures and system checks. For manufacturers with sufficient equipment hardening, Bureau Veritas can provide a CYBER SECURE Type Approve Certificate.

Cyber Secure:

Cyber Secure class notation aims to provide support to shipyards and ship owners to understand and address the complexity of their cyber systems and the eco-system within.

8.2 Relevancy with NAPA

At the time of writing of this thesis we do have several hundred product deliveries onboard ships with Bureau Veritas as classification society, mostly loading computers.

8.3 Required documentation from NAPA

- Cyber Repository document (a dedicated document for information gathering regarding assets, systems and equipment and to be enforced by equipment suppliers for systems or equipment seeking Type Approved Certificate)

8.4 Corresponding standards and regulations

Name	Description
Bureau Veritas NR 659	RULES ON CYBER SECURITY design, construction, com-missioning and maintenance of computer-based systems
Bureau Veritas NR 642	Cybersecurity Requirements for Products to be In-stalled On-Board Naval Ships
ANSSI Cybersecurity for Industrial Control	Classification + Detailed Measures
ANSSI EBIOS	Expression des Besoins et Identification des Objectifs de Securite
ANSSI-DAT-NT-003-EN/ANSSI/SDE/NP	Recommendations for securing networks with IPsec
ANSSI-PA-046	Cartographie du systeme de information
BV-SW-200 / 20170609	Bureau Veritas LIST CEA Tech,Cybersecurity Guide-lines for Software Development & Assessment
CIS-Benchmarks	Centre for Internet Security guidelines to protect systems & platforms
ENISA Port Security	Good practices for cybersecurity in maritime
IACS UR E22	International Association of Classification Societies, on board use and application of computer-based systems - Rev.2 June
IACS Rec. No. 166	Recommendation on Cyber Resilience

IEC 62443	Industrial communication networks, Network and system security
IMO Resolution MSC.428(98)	Maritime Cyber Risk Management in Safety Management Systems
IMO MSC-FAL.1	International Marine Organization, Guidelines on Maritime Cyber Risk Management, Circ.3 - 5 July 2017
ISO/IEC 27005:2008	Information security risk management
ISO/IEC 15408	Common Criteria for Information Technology
ISO/IEC 27001	Information Security Standard
NIST SP 800-39	Managing Information Security Risk
NIST 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations as part of a di-
Information Security Management Act	(FISMA)

8.5 Required additional certifications to be acquired by NAPA.

- N/A

8.6 Conclusions

Comprehensive, but quite complicated procedure. As an outcome, a ship specific Cyber manual will be produced.

9 China Classification Society

9.1 Introduction

China Classification Society (CCS; 中國船級社) is a classification society of ships, started in 1956 as a non-profit making entity in the People's Republic of China.

China Classification Society guidelines and rules are based on their proprietary "Rules for classification of a Sea-going Steel Ships" [19].

A ship, when applied for assessment and qualified in drawing review and assessment by CCS, will be granted with the following additional notation:

Cyber Security (P, S), where P indicates meeting basic requirements and S meeting higher requirement.

For Cyber Security Notation P, network redundancy, intrusion prevention system and network monitoring are not required (refer to picture on next page).

Technical Requirements of Class Notation Cyber Security (P)

	Clauses	Description	Class-P
Physical security	3.2.1	Physical location requirements	√
	3.2.2	Physical access control	√
	3.2.3	Device installation	√
Cyber architecture	3.3.1	Network redundancy	-
	3.3.2	Network segregation and segmentation	√
	3.3.3	Communication security	√
	3.3.4	Wireless network	√
	3.3.5	Assets List	√
	3.3.6	Network testing	√
Region boundary	3.4.1	Boundary protection	√
	3.4.2	Malicious code prevention	√
	3.4.3	Intrusion prevention	-
	3.4.4	Monitoring and alarming	-
	3.4.5	Remote operation and maintenance (if applicable)	√
	3.4.6	Access control	√
Computing environment	3.5.1	Identity authentication	√
	3.5.2	Data security	√
	3.5.3	System installation and update	√
	3.5.4	Accident response and recovery	√
	3.5.5	Backup	√
Security	3.6.1	Configuration requirement	√

Figure 9.1. Technical requirements

9.2 Relevancy with NAPA

NAPA regularly provides loading computers and sometimes monitoring systems to ships with CCS as classification society. Ships built in People's Republic of China, do not however always have CCS as classification society, as this choice is made by the ship owner which might reside in some other country. CCS cyber security regulations almost specifically refer to new buildings, and all NAPA deliveries so far under CCS are new builds.

9.3 Corresponding standards and regulations

Name	**Description**
CCS Rules	Classification of Sea-going Steel Ships and its modification notification
IACS UR E22	On Board Use and Application of Computer Based Systems
IEC 62443-2-1	Industrial communication networks Network and system security: Establishing an industrial automation and control system security
IEC 62443-3-3	Industrial communication networks -Network and system security: Requirements and security levels

9.4 Required documentation from NAPA

Documentation relies heavily on the shipyard, which needs to develop a security construction management system.
Required System Specification (Product Technical Specifications) from NAPA:

System Specifications:
Requirements for environmental conditions of the product: The requirements for working conditions (including electromagnetic compatibility) stipulated in the Rules for Classification of Sea-going Steel Ships shall be met. Detailed description of product functions: including system configuration, scope of application of the product, detailed description of implementable control and monitoring functions of the product and implementation methods, detailed description of the security status of each function implemented, features of the system under various operating conditions (including emergency and fault conditions) and the instructions under normal and abnormal conditions
Detailed description of redundant settings and conversion mechanism
Detailed description of fault monitoring and identification functions
Detailed description of data security and user security level -List of control and monitoring items: List of all I/O signals of the system (service description, instrumentation, system, signal type, range and limited setting range)
Hardware Specifications:
List of technical specifications of hardware and external device
System chart: The connections among all major components (software and hardware units, modules) of the system and the interfaces with other systems are described
Detailed description of main hardware configuration of the product
Details of I/O devices
Details of power supply unit
Specification of network transmission medium and maximum data transmission traffic
Main communication protocol standard adopted by the network transmission medium
Basic parameters of access network device, such as transmission port, subnet mask, gateway address, accepted communication protocol, etc.
Specification of storage medium
Software Specifications:
List of software installed on the system and version numbers
Description of basic software installed in each hardware unit
Description of communication software installed in the network node
Description of application software: maintain the information of the system modules that must operate for the functions and the information of its dependence on other sys-

tems, maintain the relations between the software modules that must operate for each function, and the data flow and control flow between software modules
Software configuration, including priority scheme
Switching mechanism between redundant systems
User manual for each software:
Description of the function allocation of each workstation and operation station and the control conversion between the stations
Description of functions assigned to each input device
I/O devices layout, dimensions and necessary physical pictures
User input interfaces description and menu description
Topology of the Cyber System:
Network topology, which can clearly show the connections and access relations of network transmission medium with the access systems and devices
Layout of routers, and the network zones connected thereto
Layout and access modes of system firewalls, and the zoned security protection area
Layout and access modes of on-board work stations and servers
Systems and devices accessed to the network, such as the communication navigation system, cabin status monitoring system and display control unit connected via a router or directly accessed to the network
Layout and access modes of intrusion detection and intrusion prevention system (where applicable)
The power supply modes of inside and outside of the system and the units
Configuration System Files:
List of devices and systems accessed to the network, including the basic information of version numbers, installation and maintenance dates and the identification names in the cyber system
Network data traffic limit
Open ports in the devices after the system is put into operation
Users permitted to access the network and the conferred authorities
The system's settings of restricted access addresses, such as the system white list
Remote user access authority (where applicable)
Locations where configuration files are stored and backed up
Necessary measures taken to protect system configuration files from malicious reading or tampering
System Operation and Test Procedures:
Test items

Test methods
Result evaluation criteria
Referenced standards.
Cyber System Hardware Installation Instructions:
Installation locations and methods of router, firewall, workstations, servers, etc.
Necessary measures taken to protect hardware devices from physical damages (where applicable)
Requirements of devices installed in special areas for environmental conditions (temperature, pressure)
Operation Manual (incl. Troubleshooting Instructions):
It shall at least include system start-up, functions recovery, maintenance and routine test, data security and data backup, user authority limits, software re-installation and system recovery, fault location and shooting, system update and other matters that users need to pay attention to
Software maintenance and instructions (incl. necessary procedures for software and hardware alteration management)
Software verification evidences:
Verification evidence of software modules in line with software programming standards (detection and correction of software errors)
Test evidence of programmable device functions for software modules, subsystems and system levels

9.5 Required additional certifications to be acquired by NAPA.

N/A

9.6 Conclusions

Although a major classification society, not our main concern, when compared with numbers of installed products. Even for many vessels built in China, they have another classification society selected, as this is the owners choice. However, CCS cyber security provides a comprehensive and interesting documentation and checking list as can be noted from above. Interestingly, this list is not based on NIST framework, but solely on CCS own and IEC 62443. Even more interestingly it notes the physical conditions of where the systems are installed.

10 ClassNK

10.1 Introduction

Nippon Kaiji Kyokai (日本海事協会), AKA ClassNK offers guidelines for holistic approach, covering design, owners and operators and system vendors of a commercial ship:

1. Guidelines for Digital Smart Ships, August 2020 and edition 1.1 in March 2021
2. Guidelines for Designing Cyber Security Onboard Ships, July 2020
3. Guidelines for Software Security, May 2019 (second edition suspended for now, as new IACS rules coming)
4. Guidelines Cyber Security Management System for Ships April 2019

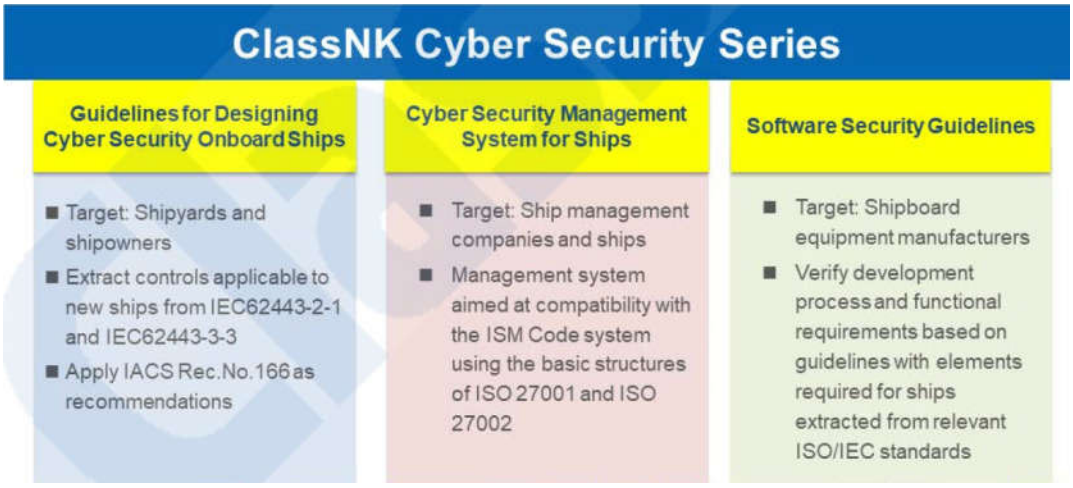


Figure 10.1. ClassNK Cyber Security Series

CybR-G notation

A class notation "CybR-G" applies to ships that have taken cyber security measures in accordance with "Class Guidelines for Designing Cyber Security Onboard Ships" and to this end, the audit requirements for its registration and maintenance have been set out in chapter 3. of "Class Guidelines for Designing Cyber Security Onboard Ships" [20]. This means that the owner and yard have taken to verify cyber security already in design and building phase.

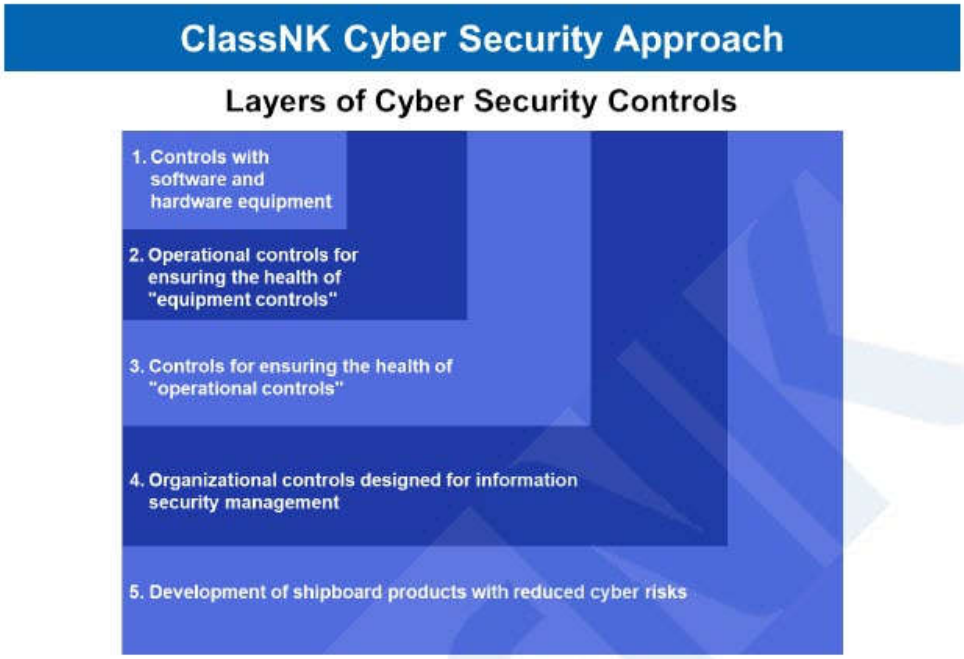


Figure 10.2. ClassNK Cyber Security Approach

Digital Smart Ship (DSS(XX)) notation

ClassNK describes a ship, which applies digital technologies such as various types of monitoring and autonomous navigation systems as "Digital Smart Ship" (DSS). A Digital Smart Ship notation can be affixed to the classification characters of the ship in accordance of the requirements of "Guidelines for Digital Smart Ships" [21].
Abbreviation DSS(XX), indicates subcategories of the notation as follows:

- Digital Smart Ship (Energy Efficiency) (DSS(EE))
- Digital Smart Ship (Hull Monitoring)(DSS(HM))
- Digital Smart Ship (Sloshing) (DSS(SLOSH))
- Digital Smart Ship (Machinery Monitoring) (DSS(MM))
- Digital Smart Ship (Connected Ship) (DSS(CNC))
- Digital Smart Ship (Navigation)(DSS(NAV))
- Digital Smart Ship (Shore Monitoring)(DSS(SM))
- Digital Smart Ship (Onboard Local Area Network) (DSS(LAN))
- Digital Smart Ship (Refrigerated Cargo Shore Monitoring)(DSS(RCSM))

10.2 Relevancy with NAPA

- A ship in construction which applies for CybR-G class notation and has procured NAPA systems, will have NAPA involved in the building phase already
- A ship equipped with ClassNK - NAPA Green Monitoring system is considered a "Digital Smart Ship", and categories Digital Smart Ship (Energy Efficiency) (DSS(EE)) and Digital Smart Ship (Connected Ship) (DSS(CNC)) apply
- ClassNK Software Security Guidelines are targeted for shipboard equipment manufacturers, and NAPA applies as a software vendor who provides specific computers for NAPA systems (Loading / Stability Computer mainly)
- Hundreds of NAPA monitoring product deliveries to ships which have ClassNK as classification society
- Considerable amount of those ships have a DSS(EE) and DSS(CNC) notation

10.3 Required documentation from NAPA

- System description, DSS (EE)
- Installation (Commissioning setup) drawing, with wiring diagram, DSS (CNS)
- User manuals, DSS (EE)
- Service agreements if any, DSS(EE)

10.4 Corresponding standards and regulations

- IACS recommendations No. 166

- IEC62443-2-1 and IEC62443-3-3
- ISO 27001 and 27002

10.5 Required additional certifications to be acquired by NAPA.

Depending of the commissioned product, a separate type approval might be needed.

10.6 Conclusions

Especially in Asian market, our clients will aim for DSS notation for their ships. Possibly CybR-G notation from yards is sought also, which means we will be involved from the beginning at least when a Loading Computer, Stability Computer or Emergency Computer is included.

11 DNV

11.1 Introduction

DNV, Den Norske Veritas (formerly DNV GL) is an international accredited registrar and classification society headquartered in Hvik, Norway.

DNV Cyber Security program refers to two main documents:

1: **Class Guidance, DNVGLCG0325: Cyber secure**

The Class Guidance can be applied to guide owners, yards, manufacturers and surveyors to implement DNV GL class rules for the Class Notation Cyber Secure and to describe the content of their Cyber Security Management System (CSMS).

2: RULES FOR CLASSIFICATION Part 6 Additional class notations Chapter 5 Equipment and design features

Section 21 handless cyber security with the objective of achieving the additional class notation "Cyber Secure" in an order to introduce measures aimed at setting up barriers to prevent, mitigate and respond to cyber security threats. Vessels constructed and tested in accordance with the requirements in these rules may be assigned the class notation "Cyber secure" [22].

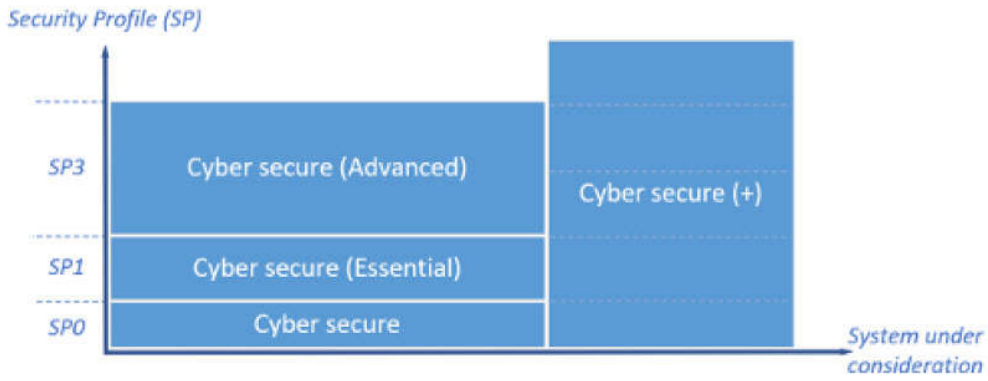


Figure 11.1.DNV Cyber Secure Notations and Security Profiles

DNV bases its notation heavily with IEC 62443 standards [23].

This does not always concern NAPA directly, although NAPA Online module does have OT features when used to send data to DCS systems. DNV Rules are however based on ISO/IEC 27001 and 27002, which NAPA is compliant with.

The security level (SL) concept is introduced in the IEC 62443 standard to align the requirements with cyber risk reduction. For DNV add notation, Security Profiles (SP) are intended to tailor the selection of requirements to their need. DNV GL has defined five incremental security profiles (SP0 to SP4) and the highest security profile represents the greatest risk reduction.

- Security profile SP0 (Cyber Secure):
  Provides an initial level of risk reduction. It focuses on the most prominent security threats and barriers and is considered to meet the intention of MSC.428(98). This security profile is mandatory for class notation Cyber secur. It is a common baseline requirement for systems inventoried and divided to zones and conduits. Baseline requirements comply with IEC 62443-3-3 fundamental requirements (FR)
- IEC 62443 security level 1:
  Security profile SP1 (Cyber Secure (Essential)) provides protection against casual or coincidental cyber threats. This security profile is mandatory for Cyber secure (Essential) notation and may be selected for Cyber secure (+).
- IEC 62443 security level 2:
  Security profile SP2 (Cyber Secure (+)) provides protection against intentional violation by threat actors possessing low resources and low motivation. This security profile may be selected for Cyber secure(+) notation.
- IEC 62443 security level 3:
  Security profile SP3 (Cyber Secure (Advanced)) provides protection against intentional violation by threat actors possessing moderate resources and specific OT-system skills. This security profile is mandatory for Cyber secure (Advanced) notation and may be selected for Cyber secure (+).
- IEC 62443 security level 4:
  Security profile SP4 is based on and provides protection against intentional violation by threat actors possessing extended resources, high motivation and specific OT-system skills. This security profile may be selected for class notation Cyber secure (+).

A threat assessment matrix based on Security Profiles (SP), which come from IEC 62443-3-3 security levels and the actual notation is given on four different types of notations:

- Cyber Secure, SP0. Common baseline requirements for systems inventoried and divided to zones and conduits. Baseline requirements comply with IEC 62443-3-3 fundamental requirements (FR)
- Cyber Secure (Essential), SP1. Additional technical security requirements are based on IEC 6244333 security level 1 profiled for the maritime industry.
- Cyber Secure (Advanced), SP3. Additional technical security requirements are based on IEC 6244333 security level 2 profiled for the maritime industry.
- Cyber Secure (+), SP2. Class notation Cyber secure (+) intends to offer flexibility with respect to risk reduction level (security profile) and SuC. The notation may be used as a 'stand-alone' notation or may be combined with qualifier Essential or Advanced. NAPA Systems fall into this category, since they are not listed in Essential and important functions list by DNV

DNV GL security profile (SP)	*IEC 62443 security level (SL)*
SP0. Common requirements	Not applicable (IMO MSC.428(98) compliance).
SP1. Required for **Cyber secure(Essential)**	SL1. Protection against casual or coincidental violation.
SP2.	SL2. Protection against intentional violation using simple means with low resources, generic skills, low motivation.
SP3. Required for **Cyber secure(Advanced)**	SL3. Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills, moderate motivation.
SP4.	SL4 Protection against intentional violation using sophisticated means with extended resources, IACS specific skills, high motivation.

Figure 11.2. IEC Security levels and DNV Security profiles

11.2 Type Approval DNVGL-CP-0231:

If type approval for a product is achieved, then only onboard check required to ensure that the type approved capabilities are correctly configured [22].

11.3 Relevancy with NAPA

Our number one classification society, when it comes to number of installed products onboard. When performing the cyber security risk assessment of the vessel, other systems than the 11 pre-selected may be considered as important for the cyber risk. Such systems should be added in the scope by using Cyber secure(+). NAPA falls into the category of Cyber Secure+ usually.

11.4 Required documentation from NAPA

Object	*Documentation type*	*Additional description*	*Info*	*Required for*
Vessel system subject for cyber security assessment	I020 - System function description	A textual description with necessary supporting drawings, diagrams and figures to cover: — cyber security configuration and arrangement for system — scope of supply — cyber security diagnostics and alarming functionalities — safe states for cyber security incidents — implementation of requirements in design philosophy.	AP	— **Cyber secure(Essential)** — **Cyber secure(Advanced)** — **Cyber secure(+)**
	I030 - System block diagram (topology)	Schematic drawing(s) showing arrangement of systems to be addressed for cyber security. This should include: — local and remote control for individual systems — integration into logical zone model — system interfaces — connection outside of vessel (if any) — physical location.	AP	— **Cyber secure(Essential)** — **Cyber secure(Advanced)** — **Cyber secure(+)**
	I150 - Circuit diagram	Detailed drawing showing electrical and communication wiring complying with requirements in the design philosophy.	AP	— **Cyber secure(Essential)** — **Cyber secure(Advanced)** — **Cyber secure(+)**
	I320 - Software change handling procedure	A procedure describing how software changes to the system are proposed, evaluated and implemented using a standardized, systematic approach that ensures traceability, consistency and quality and that proposed changes are evaluated in terms of their anticipated impact on the entire vessel system. See [5.4].	FI	— **Cyber secure(Essential)** — **Cyber secure(Advanced)** — **Cyber secure(+)**
AP=For Approval; **FI**=For information				

Figure 11.3 Required Documentation

11.5 Corresponding standards and regulations

Name	Description
IEC 61162-460	(Maritime navigation and radiocommunication equipment and systems Digital interfaces Part 460: Multiple talkers and multiple listeners Ether-net interconnection Safety and security)
IEC 62443-2-1	(Industrial communication networks Network and system security Part 21: Establishing an industrial automation and control system security pro-gram -IEC 62443-3-3 (Industrial communication networks Network and system security Part 33: System security requirements and security levels)
IEC 62443-4-2	(Industrial communication networks Network and system security Part 42: Technical security requirements for IACS components)

11.6 Required additional certifications to be acquired by NAPA.

No mandatory certifications, but individual systems can have separate type approval: Type approval DNVGL CP0-231.Objective of the TA scheme is to offer an alternative to case by case design approval for systems or components intended for vessels with class notation Cyber secure.

11.7 Conclusions

As our biggest classification society by numbers of installed products onboard, DNV cannot be omitted. DNV also gives a profound mapping of FR (Fundamental Require-ments) of IEC 62443, SR (System Requirements), RE (Requirement Enhancements) to different notation SP (Security Profiles). These can be used as base evaluation regard-less of classification society used.

12 Lloyd's

12.1 Introduction

Lloyd's Register Group Limited (LR) is a technical and business services organization and a maritime classification society, wholly owned by the Lloyds Register Foundation, a UK charity dedicated to research and education in science and engineering.
The organization dates to year 1760.

ShipRight Cyber Security Procedure

ShipRight procedures are a comprehensive system of procedures aimed at ensuring high standards of safety, quality and reliability at the design stage and during ship construction [24].

For Cyber Security there are two procedures which are referenced in this overview which cover both the design and build requirements, as well as the operational requirements, of securing the safety of a vessel against cyber-attacks [25].

Lloyds ShipRight Cyber Security Procedure is a set of requirements, which are used together with Lloyds Cyber Security Framework system. The LR Cyber Security Framework system is a strategic tool for ship owners, thus out of scope of this study. Descriptive notes are issued as per vessel, not as per system, i.e. a vessel is inspected as a whole.

Pic 12.1 Lloyds Framework.jpg

There are two procedures which are referenced in this overview which cover both the design and build requirements, as well as the operational requirements, of securing the safety of a vessel against cyber-attacks.

LR Cyber Security ShipRight (Design & Build) Procedures

LR Cyber Security ShipRight (Operations) Procedures

Assessment of these requirements will result to the issue of a Cyber Security Descriptive Note (DN).

Descriptive note Format:

- Cyber SECURITY Capability (1:Established - 4:Optimised), Maturity (1:Established - 4:Optimised) (xxx yyyyyyy)

Example:

- Cyber SECURITY Capability (3: Accomplished), Maturity (2:Established), (SOU 1400145)

12.2 Relevancy with NAPA

Our number two classification society, when it comes to number of installed products onboard.

12.3 Required documentation from NAPA

Asset and data management:

- Asset inventory: Identification of critical assets, asset classification, functional description
- Maintenance plan
- Network design (installation drawing, network segregation and security controls)

Authentication & Authorization

- Privileged access rights are defined and documented for each system and/or process.

Remote use:

- A secure design for remote access must be documented, agreed and followed.
- All 3rd parties that have any responsibility over anything in scope systems must be documented.

Risk Management:

- Penetration test reports
- Risk assessment documentation
- cyber security policy documentation

Delivery:

- Delivery and handover notes and checklists
- Configuration and settings documentation
- System management guide

12.4 Corresponding standards and regulations

ISO 27002	Information technology – Security techniques – Code of practice for information security controls-
NIST 800-53	Cyber Resiliency
IACS rules and recommendations	ur-e22 On Board Use and Application of Computer based systemsrec166 Recommendation on Cyber Resilience
IEC-62443-3-3	Network and system security – Part 3-3: System security requirements and security levels

12.5 Required additional certifications to be acquired by NAPA.

- N/A regarding cyber security

12.6 Conclusions

Lloyds offers the most conclusive mapping list of cyber security risk areas (domains in Lloyds vocabulary) that it can be used as a reference or checklist regardless if the ship has Lloyds as classification society or not.

Also, the mapping of cyber security risk areas to standards and regulations is the most comprehensive and well listed for both new buildings and retrofit installations to ships already in operation.

13 End conclusions

A customer of NAPA will most likely send a cyber security assessment questionnaire of their own, in the beginning or sales phase of a project. Since all ships have a classification society, the items and question are most likely based on the framework of that Class Society.

All classification societies follow the IACS rules and recommendations and IEC 62443 standard, but in addition they have their own classification for cyber security risk areas and refer to additional standards and regulations.

Any and all onboard assessments, including but not limited to additional class notation regarding cyber security, will follow the requirement and procedures of the corresponding Class.

For this reason, for NAPA, a documented and up to date understanding of the cyber security certification and notation procedures of different certification societies is necessary.

This documentation is available for sales people, who can then determine the scope of required work for cyber security compliance, by choosing the lists for corresponding class society.
As the amount of referred standards, and required documentation from NAPA, vary a lot, this has to be taken into account on delivery pricing when class notation is sought. For actual onboard commissioning, the China Classification Society documentation list is the most practical one (and not based on non-maritime NIST framework).

Additional NAPA specified cyber security certifications and type approvals provided by Class, likely to be needed as well.

At the moment IACS separates IT and OT, but this is likely to be changed as the border between them gets vague. Loading computer is also excluded from IACS cyber requirements, but this also likely to be changed as well as the loading computers will also be connected to OT and to other IT systems onboard.

As a final note, while this study will serve as a beginning of a holistic onboard cyber security management program for NAPA deliveries, this kind of program has a start, but no end, as it is a continuously improving process.

14 References:

[1] IMO, April 2017. IMO MSC-FAL.1-Circ.3 - Guidelines On Maritime Cyber Risk Management. p. 2.

[2] IMO, June 2017, IMO resolution MSC.428(98), p. 1.

[3] BIMCO, 2018, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, p 5.

[4] NAPA Oy, October 2020. NAPA and Digitalization in shipping, p. 10.

[5] Digital Ship, April 2011. Development underway on Inmarsats Global Xpress, p.1-2.

[6] DNV GL AS, February 2020. RULES FOR CLASSIFICATION, Part 6 Additional class notations Chapter 5 Equipment and design features SECTION 21 CYBER SECURITY , p. 288

[7] Mikko Lehto , Sept 2020. NAPA Cyber Security for developers, p. 3.

[8] NIST, April 2018. Framework for Improving Critical Infrastructure Cybersecurity, p. 13.

[9] DNVGL, February 2020, Glass Guideline DNVGL-CG-0325, p. 9.

[10] IACS, June 2016. E22 On Board Use and Application of Computer based systems, p. 1-2.

[11] Mariner Systems UK Ltd, April 2020. Approvals. Available from: http://www.marinersystems.co.uk/welcome.htm [accessed 29-Dec-2020]

[12] NAPA Ltd, October 2020. NAPA Onboard Solution Cyber Security Hardening Guidelines, p. 1.

[13] ABS, February 2020, ABS Notations and Symbols, p. 24.

[14] ABS, June 2018, CYBERSECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES ABS CyberSafetyTM VOLUME 2, p. 9.

[15] Eagle.org, ABS CYBERSAFETY SERVICES FOR EQUIPMENT. Available from: https://ww2.eagle.org/en/Products-and-Services/type-approval/abs-cybersafety-for-equipment.html [Accessed 16.02.2021]

[16] BIMCO, 2018, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, p. 8.

[17] Bureau Veritas, July 2020. Technology Report: Cyber Managed & Cyber Secure, p.3.

[18] Bureau Veritas, September 2020. Rules on Cyber Security for the Classification of Marine Units, p.64.

[19] CCS, March 2020. CCS Guidelines for Requirement and Security Assessment of Ship Cyber System 2020 , p. 5.

[20] ClassNK, July 2020. Guidelines for Designing Cyber Security Oboard Ships, p. 10.

[21] ClassNK, August 2020, Guidelines for Digital Smart Ships, p. 1.

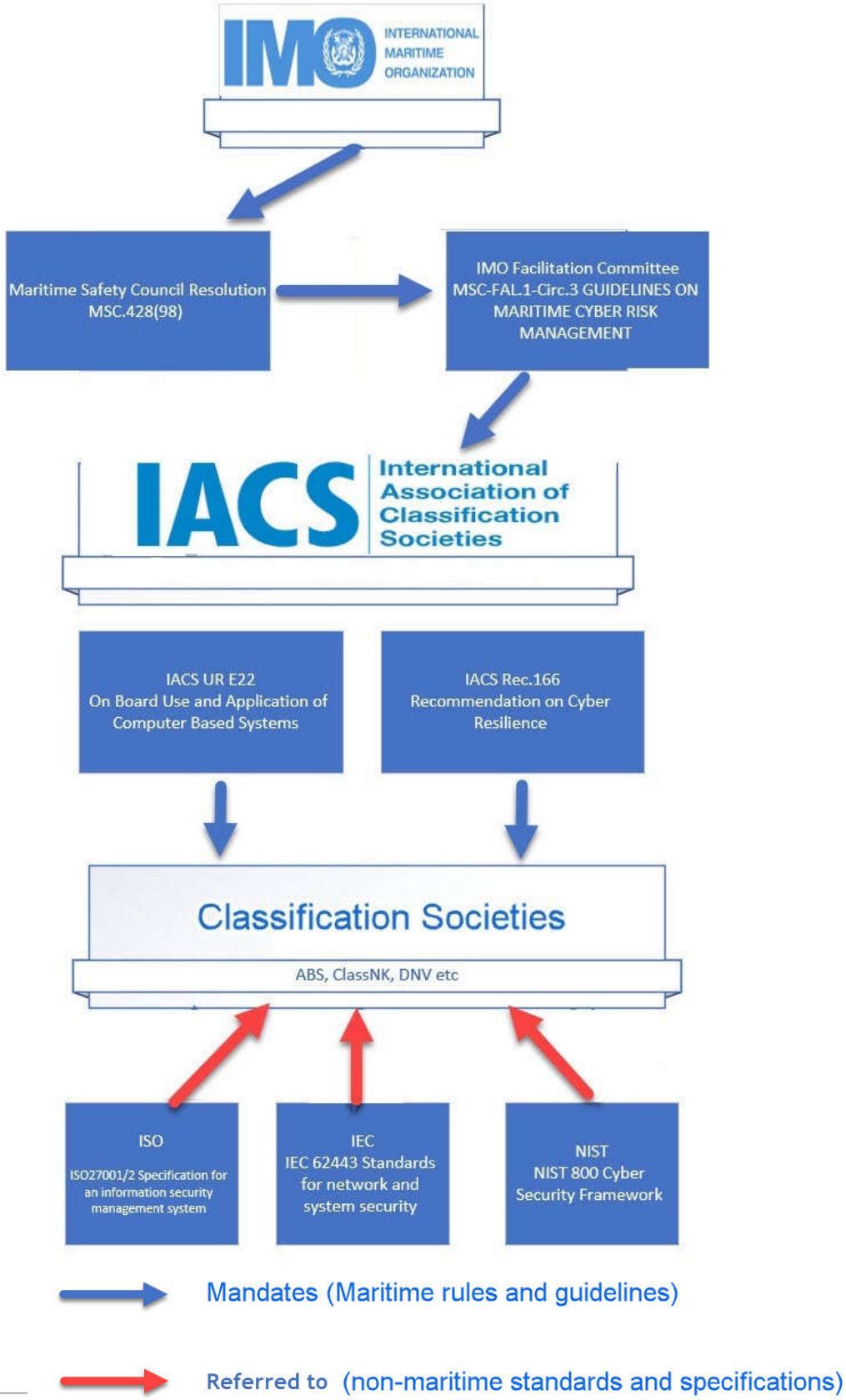
[22] DNV GL AS, February 2020. RULES FOR CLASSIFICATION, Part 6 Additional class notations Chapter 5 Equipment and design features SECTION 21 CYBER SECURITY , p. 289-290.

[23] DNV GL AS, September 2017. RECOMMENDED PRACTICE DNVGL-RP-G108 Cyber security in the oil and gas industry based on IEC 62443, p. 7.

[24] Lloyds, ShipRight procedures, Available from: https://www.lr.org/en/shipright-procedures/ [Accessed 18.02.2021]

[25] Lloyd's Nettitude, October 2020. Overview and Guidance for ShipRight CyberSecurity Procedures, p. 2.

Appendix 1. Maritime Cyber Security for NAPA onboard



Appendix 2 Definitions

IMO - The International Maritime Organization

IMO is a specialized agency of the United Nations responsible for regulating shipping industry. IMO's primary purpose is to develop and maintain a comprehensive regulatory framework for shipping including safety, environmental concerns, legal matters, technical co-operation, maritime security and the efficiency of shipping.

IMO convention SOLAS (Safety of Life at Sea) is United Nations Convention regarding safeguarding human life at sea. SOLAS itself incorporates the International Safety Management Code (ISM) as one it's key elements. ISM in turn defines the International safety management (ISM) code, which details all the important policies, practices, and procedures that are to be followed in order to ensure safe functioning of ships at the sea.

IMO resolution MSC.428(98) from June 2017, mandates that all shipping companies should include cyber risks addressed in safety management systems (SMS) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

In an order to accomplish this, the following guidelines from IMO Facilitation Committee must be followed and included in the shipping company safety management system (SMS).

IMO MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management, July 2017

These guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

IACS - International Association of Classification Societies

IACS is a top organization for classification societies, and it provides high level requirements and recommendations for Class Societies to use on ther own notation requirements. See Chapter 7. IACS.

Classification Societies

So called classification societies, work on registering and classifying private ships on marine trade and ensuring technical standards are followed on the construction and operation of ships and offshore structures.

Classification societies have also entered into the Cyber Security field of private marine operations, by providing cyber security certificates and notations on marine IT systems and / or ship systems as a whole.

Main classification societies in alphabetical order:

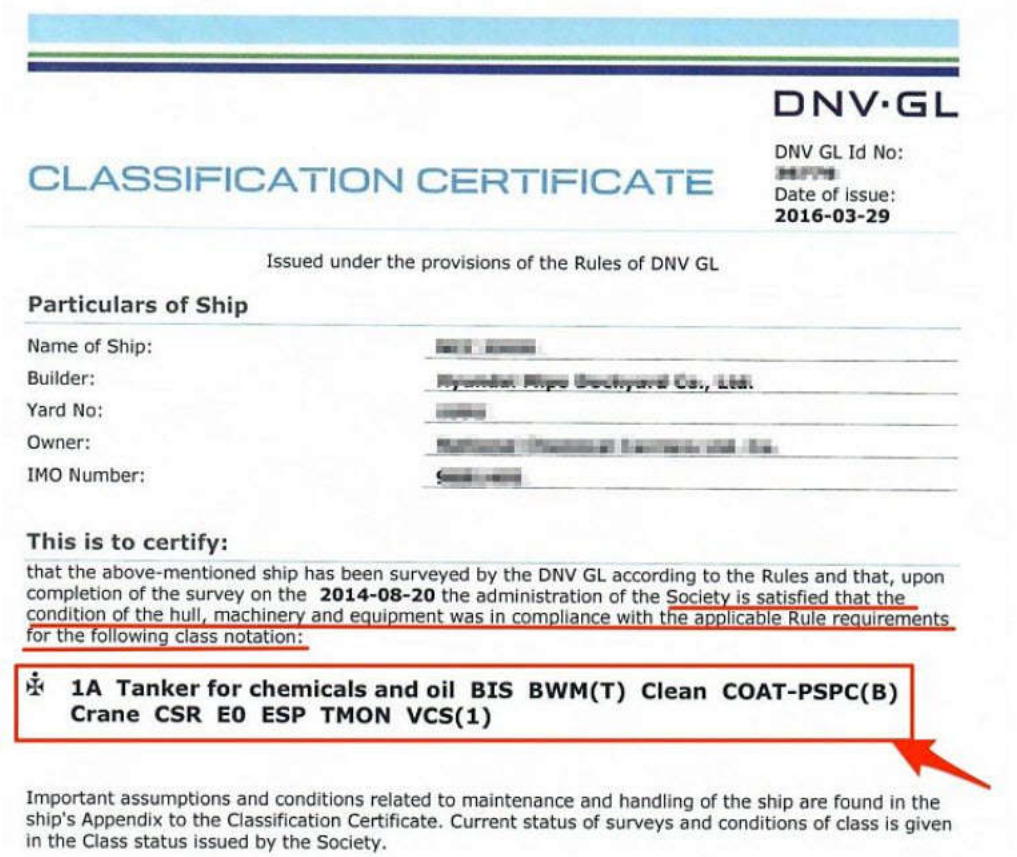
- ABS, American Bureau of Shipping
- Bureau Veritas
- CCS, China Classification Society
- ClassNK, Nippon Kaiji Kyokai
- DNV: Den Norske Veritas, world’s largest classification society
- Lloyd's: Lloyd's Register of Shipping

Classification certificate

Issued by a classification society recognized by the proposed ship register is required for a ship's owner to be able to register the ship and to obtain marine insurance on the ship, and may be required to be produced before a ship's entry into some ports or waterways.

Class notation

- Class notations are mentioned in the certificate of class of the vessel. These notations are the symbols that signify the standards to which the ship is built.
- These could include "ice class", "cyber secure" and other notations.



DNV·GL

CLASSIFICATION CERTIFICATE

DNV GL Id No: [redacted]
Date of issue: **2016-03-29**

Issued under the provisions of the Rules of DNV GL

Particulars of Ship

Name of Ship: [redacted]
Builder: [redacted]
Yard No: [redacted]
Owner: [redacted]
IMO Number: [redacted]

This is to certify:

that the above-mentioned ship has been surveyed by the DNV GL according to the Rules and that, upon completion of the survey on the **2014-08-20** the administration of the Society is satisfied that the condition of the hull, machinery and equipment was in compliance with the applicable Rule requirements for the following class notation:

1A Tanker for chemicals and oil BIS BWM(T) Clean COAT-PSPC(B) Crane CSR E0 ESP TMON VCS(1)

Important assumptions and conditions related to maintenance and handling of the ship are found in the ship's Appendix to the Classification Certificate. Current status of surveys and conditions of class is given in the Class status issued by the Society.

Figure: Class Notations of a ship

Type approval

Type approval of a product confirms that manufacturer has been found in compliance with international standards, regulations or the corresponding classification rules. This provides the company with proof of high quality and safety standards.

DNV·GL

Certificate No:
A-13890
File No:
780.90
Job Id:
262.1-017982-1

TYPE APPROVAL CERTIFICATE

This is to certify:

That the Loading Computer System

with type designation(s)
NAPA Loading Computer Version D

Issued to
Onboard-Napa Ltd.
HELSINKI, Finland

is found to comply with
Det Norske Veritas' Rules for Classification of Ships and Det Norske Veritas' Offshore Standards

Application :

Type approved for calculation and control of loading conditions with respect to requirements for:
Control of Shear Force and Bending Moments against Limit Curves* Correction of Shear Force for Tanker * Intact and Damage Stability

Figure: Type approval

Cyber Security

Cybersecurity is the application of security methods and controls to provide for, and to verify, deterministic behavior of cyber-enabled systems.
It differs from information security as it is aimed to protect exclusively digital data and systems providing it.

A cybersecurity program is meant to safeguard assets, guide personnel and their actions, and allow freedom of action and of decision making within the boundaries of the system, free of interference from both internal and external influences.
The cybersecurity process has a beginning but has no practical end short of decommissioning of the cyber-enabled asset or system.

Other terminology related to cyber security assessment

Conduit:

- Logical grouping of communication channels, connecting two or more zones, that share common security requirements.

Essential function:

- Function or capability that is required to maintain health, safety, the environment and availability for the equipment under control (HSE)

Non-Repudiation:

- Ability to prove the occurrence of a claimed event or action and its originating entities

System integrator:

- Person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

Zone:

Grouping of logical or physical assets that share common security requirements