DNV·GL

RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

Cyber security resilience management for ships and mobile offshore units in operation

DNV GL AS

FOREWORD

DNV GL recommended practices contain sound engineering practice and guidance.

Any comments may be sent by e-mail to *rules@dnvgl.com*

CHANGES – CURRENT

This is a new document.

CONTENTS

SECTION 1 GENERAL

1.1 Introduction

… Safety management objectives of the Company should, inter alia […] assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards…

INTERNATIONAL SAFETY MANAGEMENT (ISM) CODE 1.2.2

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

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

…vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed…

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

INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT: IMO-MSC 1/CIRC 1526 June 1st 2016

In 2010, the Stuxnet virus revealed cyber security to be a new focus area in operational technology and industrial automation and control systems environments. With these technologies becoming increasingly software intensive and connected to onshore business supporting systems and 3rd parties, their exposure to cyber threats has increased, putting key assets and operations of an organisation at risk. At the same time, increasing sophistication of cyber-attacks is adding to the threats IT security organisations have to deal with – often without having the experience nor any suited cyber security solutions readily available. Cyber security related threats are increasing. Threats discussed in various research reports like vulnerabilities in ECDIS, manipulation of AIS, jamming and spoofing of GPS and other satellite based tracking systems (ref. /31/), indicate that the maritime and offshore industries are not sheltered. In fact, transportation and energy are perceived as being high up on the target list of possible attackers (ref. /38/).

This recommended practice (RP) guides owners, managers and operators of ships and mobile offshore units towards enhanced cyber security of their assets in operation. In addition, this RP is intended to help IT and industrial automation control system professionals to join their efforts towards building and maintaining cyber security resilience of the total set of the assets and processes employed to conduct the company's business. Following a risk based approach, the decisoins of what is critical and high priority is then left at the discretion of the organisation.

Different members of the management team might have different exposure and levels of responsibility towards cyber security. This RP provides practical solutions suited to their different needs, from quick, high level ([2.1]) to very technical in depth assessments ([2.3]). Improvements (Sec.3) as well as verification and validation activities (Sec.4) can be scaled accordingly.

1.2 Objective

Cyber security is becoming critical not only for data protection but also for safe and reliable operations. Stakeholder driven requirements are increasing, be it through concerns about critical infrastructure and public safety or from board members who push for risk reduction and towards securing business continuity. The ISPS/ISM (ref. /19/, /20/) regime outlines the respective formal requirements to safety and security management for ships and units in operation.

This RP goes further, builds on recognised guidelines as issued by BIMCO (BIMCO, CLIA, ICS INTERCARGO and INTERTANKO ref. /5/) and IMO (ref. /21/) and is intended to be a practical guideline for those

responsible for cyber security in their respective organisations who wish to assess risks, improve cyber security and verify that information security management systems are put in place.

1.3 Scope

In this RP cyber security threats to onshore and vessel systems are considered within the following categories:

- Unintentional infections / non-targeted threats:
  - Software infections stemming from malicious malware or ransomware: Spreading via unsuspecting and insufficiently trained users in combination with unsecured internet access or insufficiently protected use of portable storage devices like USB sticks, the infection thrives through automated replications aimed at infecting as many systems as possible. These non-targeted threats typically exploit known vulnerabilities in standard systems and networks.
  - Unintentional weaknesses in software: Typically stemming from misconfiguration of equipment and software as well as from software design or updates containing undetected weaknesses due to insufficient verification and validation of the software.
- Intended / targeted threats:
  - External attackers: Hackers, "hacktivists" as well as criminal attackers, employing a wide range of attack techniques and malicious software infections. These include phishing, social engineering, and exploitation of weaknesses in control systems, user authentication or lack of network segregation.
  - Insider threats: Originating from disgruntled employees or from employees that intend to sell or otherwise misuse data or system access. Their ability to circumvent physical access controls and their in depth knowledge of the systems makes them particularly difficult to defend against.

To counter this wide range of threats, a comprehensive response is required, with Cyber Security responsibilities to be shared by different participants of the value chain: Owners of the vessel or offshore assets, users of the different systems, respective suppliers as well as ship managers and the operators themselves. Within these organisations:

- Senior Management carries the overall responsibility and establishes the risk management policies
- IT and industrial automation management personnel are responsible for establishing the required operational procedures, securing assets, operational systems and information.
- Fleet management / crew / on shore staff should comply with these policies/procedures, secure awareness and training and report incidents or anomalies.

ASSESSMENT: A systematic assessment is the foundation of cyber security improvements. Due to the potentially substantial cost of conducting detailed assessments across all systems, data sets and organisational units, this RP recommends three different assessment levels, each serving a different need and using tailored methodologies.

- *High level assessment*: Senior management needs to quickly obtain an overview of the cyber security status of their organisation. This high level overview will focus on technical aspects, awareness, policies and enforcement mechanisms. The results will provide first indications of where to focus.
- *Focused assessment*: To assess the cyber security of specific systems and data sets, a focused assessment approach is recommended. This recommended assessment builds on the safety management methodologies developed in the offshore and maritime industries and focuses on barriers that help prevent possible cyber security incidents as well as on those that help reduce the undesired consequences of such incidents. Both types of barriers need to be identified, evaluated and then assessed for their resilience. The approach can be easily picked up by staff with basic IT and industrial automation control systems knowledge and understanding of risk management methodologies.
- *Comprehensive, in depth assessment*: To generate a comprehensive picture of the total cyber security risk of an organisation, an in depth assessment is recommended. In depth assessments build on the requirements of the ISO/IEC 27001 (ref. /7/) standard as well as on other standards that are widely accepted such as the "BSI Grundschutz" (ref. /14/, /15/) or the "IEC-62443-3-3" (ref. /22/) requirements. The in depth assessment is based on a detailed inventory of the IT and automated control related

processes. It is then recommended to determine the consequence of successful attacks for each of these concerning confidentiality, integrity, availability and authenticity security properties and rate their respective importance. Combining consequence with likelihood of an attack (measured by the ease of access) then leads to a detailed cyber security risk assessment.

IMPROVEMENT: Most of the activities required to improve cyber security can be directly derived from the above described assessments. They will typically fall into the following categories:

- *Awareness and competence building*: The vast majority of cyber security incidents are related to the human element. Increasing awareness about how certain behaviours can be exploited by external attackers or malware is critical, as is building competence on how to react in cases of cyber security breaches. Company specific requirements need to be understood and policies adhered to.
- *Technical improvements*: Technical solutions can provide solid barriers against attacks – be it from the in- or the outside. These solutions typically include hardened firewalls, authentication concepts and network segregation as well as more secure software design and implementation. They need to be scaled to meet specific cyber security requirements of a particular organisation.
- *Management system including organisational set-up, clarification of responsibilities and related processes:* Requirement standards like ISO/IEC 27001 form a good basis for continuing improvement efforts, and are recommended to be implemented by more cyber security mature organisations and those with a higher risk exposure. They need to be tailored to the company's specific operations. Organisational aspects of enhancing cyber security need to be considered.

VERIFICATION and VALIDATION: In order to obtain assurance of the achieved cyber security and to demonstrate compliance and progress towards external stakeholders and the company's board, cyber security resilience can be validated and verified. Two different approaches are recommended:

- Verification and testing of technical and procedural controls protecting the deployed systems or data sets. These tests can be conducted at system level, or at component level.
- Certification of the Information Security Management System (ISMS) to the international standard ISO/IEC 27001.

Cyber security resilience has many aspects in common with general quality management systems. Due to the changing nature of the risk picture, cyber security policies need to be implemented into operational procedures, communicated and audited within a continuous improvement Plan-Do-Check-Act (PDCA) cycle which complements the maritime and offshore industries' safety and security culture. Organisations following the approach proposed by this RP will find that managing cyber security is similar to managing other challenges, making cyber security part of a continuing effort to protect the company's assets, systems, data and operations to secure compliance with the requirements of regulators such as the ISM and ISPS codes and on board procedures.

1.4 Terms and definitions

Table 1-1 Definitions

Term	*Definition*
availability	the ability of the system to provide access to its resources in a timely manner for a specified duration [IEC IEV 191-02-05], alternatively, the time or proportion of time that the system is functioning as intended
access control	selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions [BIMCO]
assets	in the scope of this RP, assets refers to hardware, system and application software, software dependent systems, networks and databases
authenticity	property that an entity is what it claims to be [ISO 27000]

Term	*Definition*
availability	property of being accessible and usable upon demand by an authorised entity [ISO 27000]
CERTs	computer emergency response teams (expert groups that handle computer security incidents)
compromise	unauthorized use, disclosure, modification, or substitution, respectively, of data, programs or systems configuration, i.e., by and after intrusion [IEC/ISO 62443-3]
confidentiality	property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO 27000]
consequence (failure)	real or relative magnitude of the seriousness of the failure (business, environmental and safety)
corrective action	action to eliminate the cause of a nonconformity and to prevent recurrence [ISO 27000]
critical	any function or component whose failure could interfere significantly with the operation or activity under consideration
criticality	the degree of impact that a requirement, module, error, fault, failure, or other item has on the development or operation of a system [IEEE 610.12:1990]
cyber-attack	any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data [BIMCO] attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset [ISO 27000]
cyber security	practices, tools and concepts that protect: — the operational technology (OT) against the unintended consequences of a cyber incident; — information and communications systems and the information contained therein from damage, unauthorised use or modification, or exploitation; and/or — against interception of information when communicating and using the internet [BIMCO]
denial of service (attack)	an attempt to make a system or network resource unavailable to its intended users. A denial of service attack can be part of a larger attack scenario, e.g. by disabling an alarm or logging functionality
dependability	collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance see also RAMS, to which it adds Security [IEC IEV 191-02-03]
emergency response	action to safeguard the health and safety of persons on or near the unit or installation usually includes all actions through alarm, escape, muster, communications and control, evacuation and rescue
error	a discrepancy between a computed, observed or measured value and condition and the true, specified or theoretically correct value or condition [IEC 61508-4]
essential services	generally defined as a service which needs to be in continuous operation for maintaining the unit's manoeuvrability (if applicable), or whose loss or failure would create an immediate danger to the unit

Term	*Definition*
failure	the termination of the ability of a functional unit to perform a required function on demand *note:* a fault in a part of the system may lead to the failure of its function, itself leading to a fault in other linked parts or systems etc.
failure mode	a defined manner in which a failure can occur failure modes can be seen as scenarios for how a system can go wrong
fault tolerance	software fault tolerance is the ability of software to continue its normal operation despite the presence of system or hardware faults
firewall	a firewall (better designated security gateway) is a system of software and hardware technical components to interface IP networks secure (see security gateway) [BSI GS]
fuzz testing	a software testing technique that involves providing invalid, unexpected, or random data to the inputs of a cyber system
important services	generally defined as a service which needs not necessarily be in continuous operation but whose failure or non-availability would not create an immediate danger but impairs the unit's safety
integrated software dependent systems	integrated systems where the overall behaviour depends on the behaviour of the systems' software components [DNV-0S-D203]
integrity	property of accuracy and completeness [ISO 27000]
mitigation	limitation of any negative consequence of a particular event
nonconformity	non-fulfilment of a requirement [ISO 27000]
operational technology (OT)	includes devices, sensors, software and associated networking that monitor and control on-board systems [BIMCO]
penetration testing	systematic employment of methods that an attacker would use to gain access
pre-shared key	in cryptography, a PSK is a shared secret key previously exchanged between the two parties using a secure channel before using the key
probability	extent to which an event is likely to occur
protective measure	means used to reduce risk
recovery	refers to the activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term [BIMCO]
redundancy	the existence of more than one means for performing a required function or for representing Information [IEC 61508-4] redundancy prevents the entire system from failing when one component fails
reliability	the capability of the ISDS to maintain a specified level of performance when used under specified conditions
risk	the usual definition of risk revolves around the qualitative or quantitative likelihood of an accident or unplanned event occurring, considered in conjunction with the potential consequences of such a failure in quantitative terms, risk is the quantified probability of a defined failure mode times its quantified consequence [DNV-OSS-300] however it is not practical to use a quantitative frequency of software failures or attacks for these reasons this RP proposes a tailored approach for determination of risk

Term	*Definition*
risk analysis	systematic use of information to identify sources and estimate the risk
risk assessment	overall process of risk analysis and risk evaluation
risk matrix	matrix portraying risk as the product of probability and consequence, used as the basis for risk assessment
software	computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system [IEEE 610.12:1990]
software/network topology	diagram depicting the virtual connections and the distribution of various software/firmware packages (see Figure K-1 for an example)
two-factor authentication	method of confirming a user's identity by the use of two different components, such as knowledge (password) and possession (token) or biometrics (e.g. fingerprint)
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled [ISO 9000:2005]
whitelisting	the process used to identify: (i) software programs that are authorized to execute on an information system; or (ii) authorized universal resource locators (URL)/websites [NIST SP-800-61]

1.5 Abbreviations

Table 1-2 Abbreviations

Abbreviation	*Description*
AIS	automatic identification system
OAuth	open standard for authorization, commonly used as a way for internet users to log in to third party websites using their Google, Facebook, Microsoft, Twitter, One Network, etc.
BNWAS	bridge navigation watch alarm system
BIMCO	Baltic and International Maritime Council
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	bring your own device
CCTV	closed circuit television
CD	compact disc
CS	cyber security
CIAA	confidentiality, integrity, availability & authenticity
CIO	chief information officer
CSET	cyber security evaluation tool
DCS	distributed control system
DDoS	distributed denial of service (attack)
DNS	domain name system

Abbreviation	*Description*
DoS	denial of service (attack)
DP	dynamic positioning
DVD	digital versatile disc
GA	general alarm
GS	Grundschutz (German): basic protection
GMDSS	global maritime distress and safety system
GMOD	generic product model defined by DNV GL containing a hierarchy of ship functions and library of ship components. GMOD was originally used to support class activities, but is also suitable for any application requiring identification and referencing to shipboard systems. For more information, see http://data.dnvgl.com/dnvgl-vis/.
GPS	global positioning system
HMI	human machine interface
IACS	industrial automation and control system
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
ISDS	integrated software dependent systems
IP	internet protocol
IPS	intrusion prevention system
IrDA	infrared data association
ISM Code	International Safety Management Code (i.e. SOLAS Chapter IX)
ISMS	information security management system
ISO	International Organisation for Standardization
ISPS Code	International Ship and Port facility Security Code
IT	information technology
IUT	implementation under test
IV&V	independent verification & validation
KPI	key performance indicator
LAN	local area network
MSC	(IMO) Maritime Safety Committee
N/A	not applicable
OT	operational technology
PA	public address
PC	personal computer

Abbreviation	*Description*
PBX	private branch exchange
PDA	personal digital assistant
PDCA	plan-do-check-act
PLC	programmable logic controller
PMS	planned maintenance system
PSA	Petroleum Safety Authority
PSWD	password
QR	quick response (code)
RACF	resource access control facility
RAMS	reliability, availability, maintainability and safety
RP	recommended practice
SAP	systems, applications & products in data processing (software maker)
SCADA	supervisory control and data acquisition
SFI	The SFI Group System was first released in 1972 as the result of a research project undertaken by the Ship Research Institute of Norway (SFI: Skipsteknisk Forskningsinstitutt).
SL	security level
SR	security requirement
URL	uniform resource locator
USB	universal serial bus
VDR	voyage data recorder
VLAN	virtual local area network
VoIP	voice over IP
VPN	virtual private network
WLAN	wireless local area network

SECTION 2 ASSESSMENT

Assessing the intersection between a company's assets, their vulnerabilities and the threats they are exposed to forms the basis for any targeted cyber security enhancement. A gap analysis between target security levels and existing countermeasures needs to point towards key areas for improvement programs. This RP recommends three different approaches. These assessments can either be used sequentially or in a standalone fashion that suits the organisation's priorities and skill sets as illustrated in Figure 2-1.

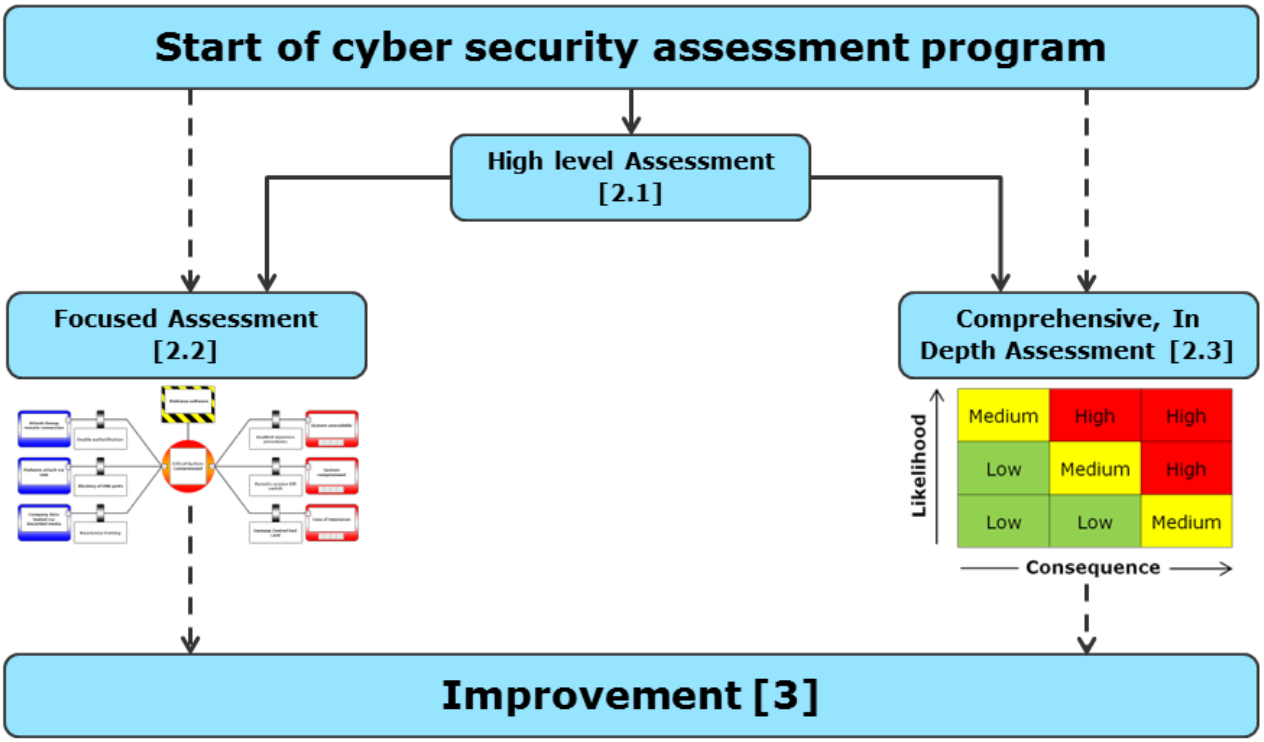

Figure 2-1 Assessment sequence

2.1 High level assessment

A high level assessment is recommended as an initial step in a company's cyber security enhancement program, when senior management quickly needs an overview of its cyber security risk picture and wants to gain a structured indication of where more focused assessments are required. This approach should be based on best judgement, reducing the effort required.

This RP proposes to:

1) Identify key systems of the company. On board systems and datasets will typically be captured based on key vessel functions while onshore systems and datasets will in turn be captured through the analysis of key business processes.
2) Consider the consequence (high, medium, low) of a successful attack regarding confidentiality, integrity, availability and authenticity for these systems and datasets.
3) Assess the likelihood (high, medium, low) of a successful attack on the identified vessel systems and key business processes by judging the likely effectiveness of the countermeasures in place, including technical countermeasures, organisational awareness, management systems and procedures.
4) Display the results of steps 2 and 3 in a risk matrix.

Conducting the high level assessment in a group rather than purely individually will yield additional benefits. It can help identify blind spots where a substantial share of the participants in the assessment answered unknown (or similar) to questions of the high-level assessment questionnaire. These should warrant further investigation or second party reviews. The same holds true for areas where substantially different views exist about consequence or likelihood of a successful attack. High level assessments as described above can be supported by the use of offline or online questionnaires (see Sec.6, ref. /1/, /2/, /3/ for more).

This RP then recommends conducting a more focused assessment ([2.2]) for those systems and datasets in use in the areas of concern (business processes or vessel functions) that are placed in the unacceptable part of the risk matrix. A comprehensive, in depth assessment ([2.3]) can also be conducted, in order to address a broader set of systems with more detailed requirements (mitigating a more substantial risk picture).

2.2 Focused assessment

This RP proposes a systematic and focused approach to assess the robustness of barriers against threats when the need is to focus on selected systems (possibly derived from a high level assessment described in [2.1]).

This RP proposes to:

1) Identify the threats to systems supporting specific vessel functions and business processes.
2) Identify the barriers that prevent incidents related to these threats.
3) Identify barriers that reduce the consequence should these incidents occur.
4) Assess the robustness of these preventive and consequence reduction barriers.

Figure 2-2 illustrates the sequence of activities involved in the focused assessment approach:

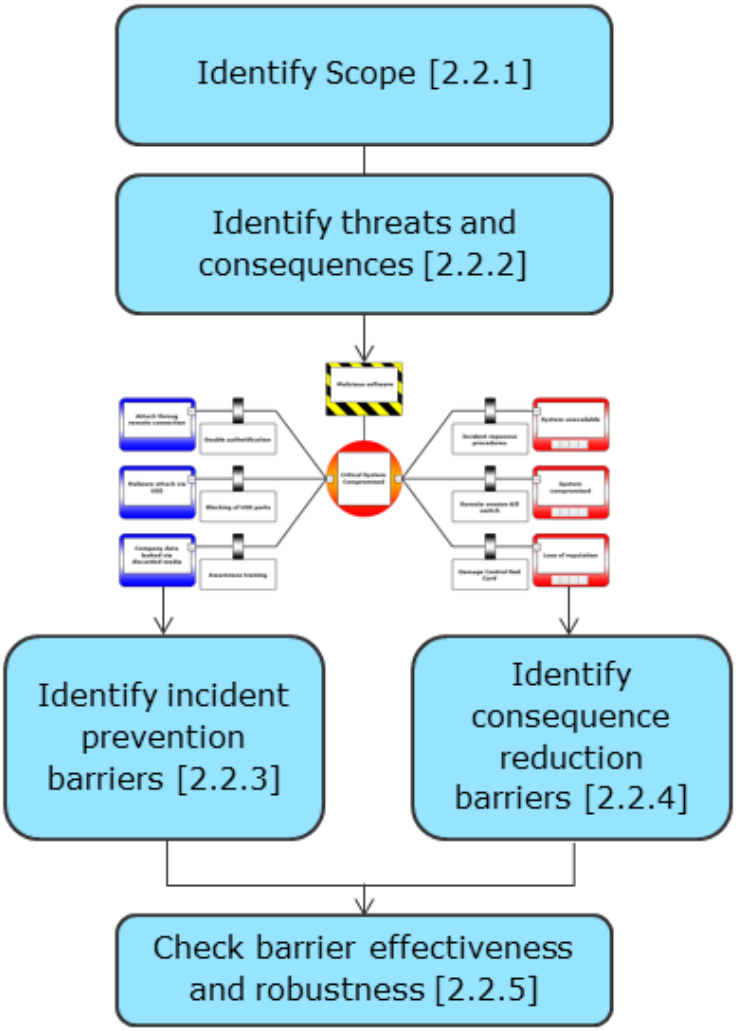

Figure 2-2 Focused assessment process flow

In cyber security a barrier (or countermeasure) is an action, device, procedure, or technique that reduces a threat, vulnerability or an attack by:

— eliminating it
— or preventing it,
— by minimizing the harm it can cause
— or by discovering and reporting it so that corrective action can be taken
— [IETF RFC 2828 ref. /24/].

The focused assessment approach proposed in this section is based on the Bow-Tie method. The approach assesses the cyber-attack related risks and on controls and barriers against such an attack, without focusing on its probability or frequency. This helps to quickly visualise if more measures need to be implemented. Figure 2-3 illustrates the Bow-Tie method, where the left part of the Bow-Tie shows barriers (grey bars) that help prevent the threats (blue boxes) becoming a cyber-incident (central red circle). Barriers on the right side of the Bow-Tie show mitigation barriers that help prevent the undesired consequences (red boxes).

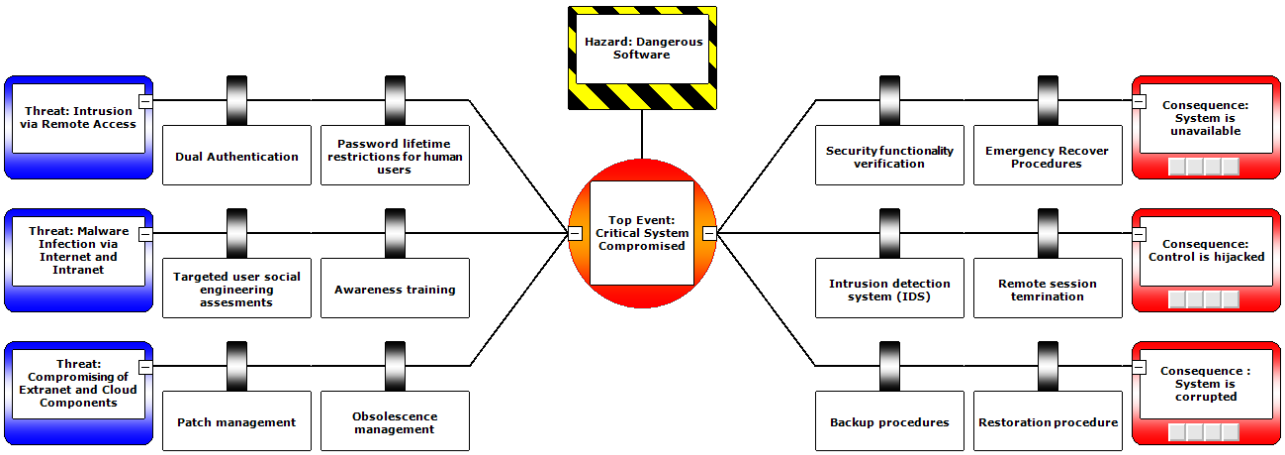

Figure 2-3 Example visualisation of cyber security Bow-Tie components

Bow–Tie diagrams can also be used for simple capturing of observations and are recommended as an effective tool to communicate and build awareness about CS (cyber security) efforts. They can also be used to help cover the general concepts of the NIST five framework core functions (ref. /34/) also referenced in the BIMCO guideline on CS. More examples of cyber security Bow-Tie barriers against remote connection related threats, malware related incidents and denial of service attacks can be found in App.A.

The Bow-Tie method articulates CS risks around hazards, top events, threats, vulnerabilities, CS incidents, consequences and mitigations. Table 2-1 describes the main components of the CS Bow-Tie method (see ref. /36/):

Table 2-1 Cyber security Bow-Tie element descriptions

CS Bow-Tie element	*Description and examples*
Hazard	An entity with the potential to cause harm, but also being necessary for performing the business. Samples used in this RP refer to software which is business critical, but notorious for being infected with viruses, malware and Trojan traps.
Top event	As long as a hazard is controlled, the top event does not occur. It is the event that shall be avoided, for example: The event when the critical system is compromised. Ex. infections, intrusions, successful password hacking, security breach.
Threats	Threats are categorised as unintentional and intentional attacks from internal or external attackers exploiting vulnerabilities such as the top 10 threats listed by the BSI ref. /29/: — malware infection via internet and intranet — introduction of malware on removable media and external hardware — social engineering — human error and sabotage — intrusion via remote access — control components connected to the internet — technical malfunctions and force majeure — compromising of smartphones in the production environment — compromising of extranet and cloud components — (D)DoS attacks.

CS Bow-Tie element	*Description and examples*
Consequences	The outcome of an unwanted event (occurrence of the top event). Examples: system is down, control is hijacked, damage to infrastructure due to resulting malfunctions.
Barrier	Any measure taken that acts against some undesirable force or intention, in order to maintain a desired state. There are two types of barriers: — Proactive or preventive barriers (left side of the top event) that prevent the top event from happening. For example: PSWD lifetime restrictions for human users, dual authentication, targeted user social engineering assessments, awareness training, patch management, obsolescence management, USB management policies. — Reactive or mitigating barriers (right side of the top event) that prevent the top event resulting into unwanted consequences. For example: security functionality verification, remote session termination, intrusion detection systems (IDS), emergency recovery procedures, backups, restoration procedures, spare parts.

In addition of the above elements of the Bow-Tie used in this RP are vulnerabilities which can be known and unknown built-in weaknesses in the system which are not addressed, such as the top 5 vulnerabilities stated by the INFOSEC Institute ref. /32/.

— SQL injections
— buffer overflows
— sensitive data exposure (weak or lack of encryption when sending/receiving sensitive data that hackers can intercept)
— broken authentication and session management (due to faulty custom implementations of session management procedures)
— security misconfiguration (running outdated software, running in debug, use of factory settings, default account, keys and passwords).

2.2.1 Identify scope

In order to define systems for which to conduct a focused assessment, the user of this RP can either start with the high risk systems and processes identified in the high level assessment ([2.1]) and/or by conducting interviews with the various users of the OT/IT systems of interest. For systems on vessels we recommend to identify high risk systems by asking the users basic questions such as listed in Table 2-2.

Table 2-2 System focused assessment questions

Typical questions to help determine systems to spot check
Is the operating system up to date?
How are software updates handled? Are suitable procedures in place?
What about software security patches, how are these handled? Is there a patch management policy?
Are antivirus and malware protections up to date? — Is there a procedure to update the OT systems? — Is there a procedure in place for OT systems to react on known vulnerabilities?
Are passwords used and changed at the expected intervals?
Are the default passwords changed?
Are there means to detect and identify cybersecurity incidents and intrusions?

Typical questions to help determine systems to spot check
Are there any security logs available (e.g. virus and malware detections)? Are they used? Reported?
Do we have a security breach response plan in place? Is it known?
Are admin rights limited?
Is Email and web browser protection implemented?
Are there access controls for the wireless network (see [3.2])
Is encryption used? Where?
Are personal USB and data storage devices allowed on the company network? Are USB sticks scanned? Cleaned? Blocked?
How is data stored on company phones/PDAs disposed of? Are disposal policies applied?
Where are the backups stored? Are storage devices tracked? Are the backups tested?
Are employees trained on cyber security policies?
Are contractors screened for adequate security clearance?
Is external access allowed for sub-suppliers? How is it controlled?
Is the remote maintenance performed adequately logged?
Are satellite and radio communications secured?
If the system is intended to be kept behind locked doors, is the physical security and boundary defence implemented?
Is the system secured against theft, fire, and accidental damage?

2.2.2 Identify threats and consequences

Depending on the responses to the above questions, the assessors acquire a first impression of what systems at risk they should focus on when assessing or building CS barriers. For each system at risk, the first step is to describe the different threat scenarios that cause unwanted consequences:

— Identify top event: When we know what is potentially hazardous, we need to know how we could lose control over it. For cyber security, the hazard is software itself, being pernicious in nature or potentially infested with viruses and malware. The top event is then the successful attack that compromises the system.
— Identify the threat scenarios which could directly cause the occurrence of the top event: Various information sources can help assess the existing threat picture such as latest CS audit reports, penetration test reports, security logs (attempted and successful hacks, security incidents), inventory of antivirus programs, lists of people having received awareness training, and left to train.
— Evaluate consequences in the event that the top event occurs. The estimated severity of each of the consequences will warrant the existence and the effectiveness of the prevention and consequence reduction barriers described below.

2.2.3 Identify incident prevention barriers

The next step is to identify barriers which prevent threats from causing the top event. These are prevention barriers. Safeguards (CS barriers at the left side of the Bow-Tie) should be identified for the different categories of IT/OT/networks that typically fall under one or more of the following:

— security management

— compliance management
— personnel training (including information security awareness and training) and hiring
— data protection against information theft
— protection against malware
— cryptology
— network segregation
— hardware and software diversity (mitigating against common mode failures in redundant systems)
— whitelisting
— remote access management or denial
— adequately managed outsourcing of IT/OT responsibilities or services
— procurement of certified components
— patch and change management (see App.G and App.I).

2.2.4 Identify consequence reduction barriers

Barriers on the right side of the CS Bow-Tie prevent or reduce the consequences and/or the resulting losses and damage caused by a CS incident. Typical consequence reduction barriers include:

— incident handling routines (NIST Special Publication 800.61 ref. /33/ can be used for detailed guidance)
— system architecture and isolation mechanisms preventing spreading of viruses, malware, etc.
— business continuity management (a simple business continuity plan should prepare a summary action plan on how to deal with a cyber event; defined routines with IT support/PR should be in place and linked with HR/senior management, see S1.3 Business continuity management in App.G for more guidance)
— backup procedures and regular testing of backups
— disaster recovery procedures (manual modes, backup restorations, etc.)
— redundancy
— software fault tolerance
— network traffic information collection (to help track down cyber criminals following an attack which increases the chances of recovering extortion money or limiting damage to the business' reputation). In addition to being a consequence reduction barrier, the gathering of forensics information can help capture lessons learned and understand how barriers have failed and how vulnerabilities can be mitigated (see App.J).

2.2.5 Check barrier robustness and effectiveness

There are several approaches to assess barriers using the Bow-Tie barrier management approach. In this RP we discuss two:

Assessing the robustness of existing barriers requires preparing building cyber security Bow-Tie diagrams for OT and IT systems under consideration. Once the diagrams have been created, barrier robustness checks can be performed by identifying the specific situations or conditions under which the barriers are performing as expected and see what barrier degrading factors should be managed. Discrepancies between the expected robustness and actual state of each barrier are to be tracked and compiled as an improvement action plan.

Assessing the effectiveness of existing barriers is performed in the same manner as the approach above with the added outlook towards complementary protection means that could apply to a given threat scenario. See Sec.3 for cost benefit analysis and work planning.

2.3 Comprehensive, in depth assessment

A comprehensive, in depth assessment is used when senior management needs a more detailed risk assessment, especially when substantial consequences of CS incidents are plausible and if substantial system interdependencies exist. Due to the more technical nature of the in depth assessment, this approach will often require the involvement of external specialists. This assessment should be carried out for critical business processes and typically involves:

1) identifying critical IT/OT systems that are vulnerable to CS threats through the mapping of key business processes and respective vessel functions
2) identifying the consequences of a successful attack for each of the systems
3) determining the ease of access to each of the systems as a practical metric for the likelihood of an attack
4) rating of the systems with regards to their CS risk (determined by the likelihood of an attack X consequence of successful attack)
5) comparing the current safeguards with target protection levels.

Figure 2-4 illustrates the steps and activities involved in the proposed comprehensive, in depth assessment approach.

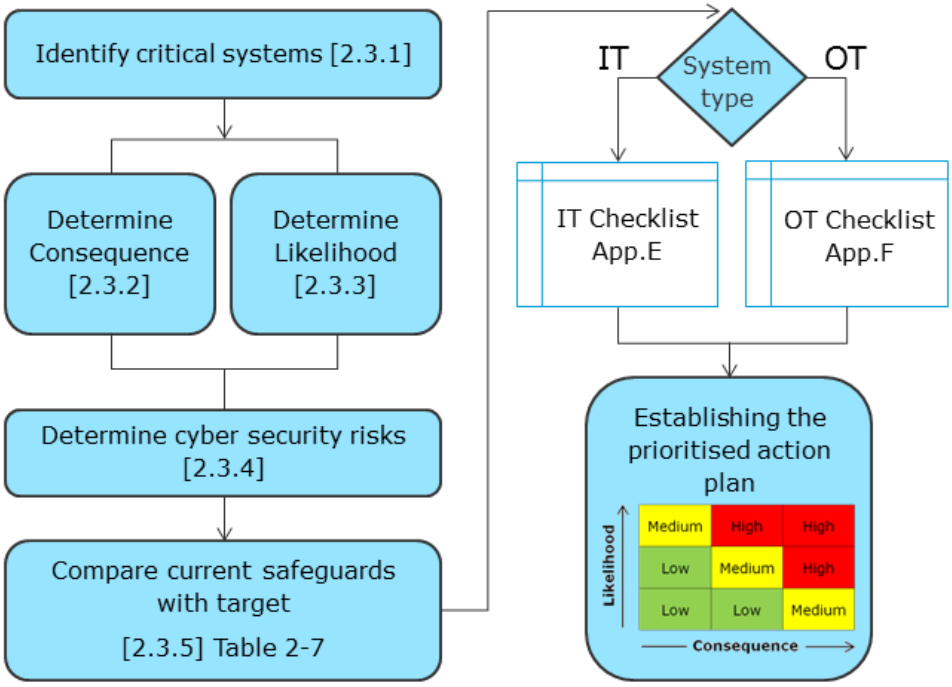

Figure 2-4 Comprehensive, in depth assessment steps

2.3.1 Identify critical systems

Companies engaging in a comprehensive, in depth assessment need to start by listing all critical systems vulnerable to cyber threats. A comprehensive identification of these critical IT/OT systems will depend on:

— the range of business activities carried-out (processes and vessel functions)
— the information transmitted and handled through these processes
— the users of the information and the systems involved in processing it.

These critical systems are best determined by mapping IT/OT systems onto the business processes the organisation performs. By first highlighting the key business processes, systems critical to these processes and therefore the company's operations can be identified. The process maps provide high level overviews of the steps, the users, the information and the systems that are involved in circulating information through the IT and OT systems on shore, on board vessel(s) and between them.

Process maps are usually created using workshops that involve key users of the different business processes and IT/OT systems, including:

— crew/officers
— shore staff (incl. IT staff, representatives of key functions)
— owner representative and other actors relevant for the business.

In these workshops, the following questions (not limited to) can help identify specific processes and identify the IT/OT systems involved in them, in order to capture the systems, interactions and critical dependencies for the business.

For the identification of key IT systems, the following questions should be addressed for each organisational unit:

— objectives of the unit
— processes required to achieve these objectives

— sequence of events in a given process (how does the process start; what are the different steps in the process; who is dependent on a given process and where does the process stop)
— information needed to execute a given process
— systems involved (application software including networks they are running on)
— any other IT systems with relation to the business, e.g. crew facing networks and entertainment.

Key OT systems are identified by addressing typical vessel functions as below:

— water tight integrity and water tightness
— power generation
— propulsion
— steering
— drainage and bilge pumping
— ballasting
— anchoring
— cargo
— drilling
— oil and gas production
— dynamic Positioning
— fire and gas detection
— ignition Source Control
— accommodation and passenger
— navigation
— communication
— other.

See App.B and App.C for more details.

For each of the IT & OT systems identified, the following questions (not limited to) can help identify interfacing systems, user interactions and critical dependencies for the business:

— who has access to the systems and how (administrator and user rights)
— databases used to store, process /compute the information
— who uses databases and how (administrator and user rights)
— different entry points (remote access, automatic updates)
— location of IT/OT components (physical and virtual according to the software topology)
— software operating systems (Windows, Linux, Unix, Simantec, etc.)
— changes that can be made on the systems (unlocked configuration or software code)
— requirements of CS for different users (e.g. policy and objectives).

IT & OT inventory lists (bills of materials, computer inventory lists, vendor software lists, etc.) and diagrams (software topologies, electrical and communication drawings) should be available as input to the mapping exercise. Sources of topology information typically are electrical drawings, communication and system block diagrams normally produced during the engineering phase and updated during construction and commissioning. Topology information should include (see Figure K-1 for an example of a software topology drawing):

— IT/OT systems, i.e. client and server computers, active network components (such as switches, routers, and WLAN access points), network printers, etc.
— network connections between these systems, i.e. LAN connections such as Ethernet, WLANs, backbone technologies, etc.
— connections between the vessel and the outside world, i.e. satellite or shore connections, etc.

This inventory and topology information enables the workshop participants to ensure that no important aspects have been overlooked in the mapping exercise. In addition, it helps discuss connections between systems and the outside world (including remote access from vendors) and check if network segregation principles have been applied.

2.3.2 Determine consequences of successful attacks

As a next step, the protection needs for the company's critical system need to be determined to guide efforts where they are most relevant. This is done by assessing the consequences of a successful attack using the CIAA (ref. /39/) model described in Figure 2-5:

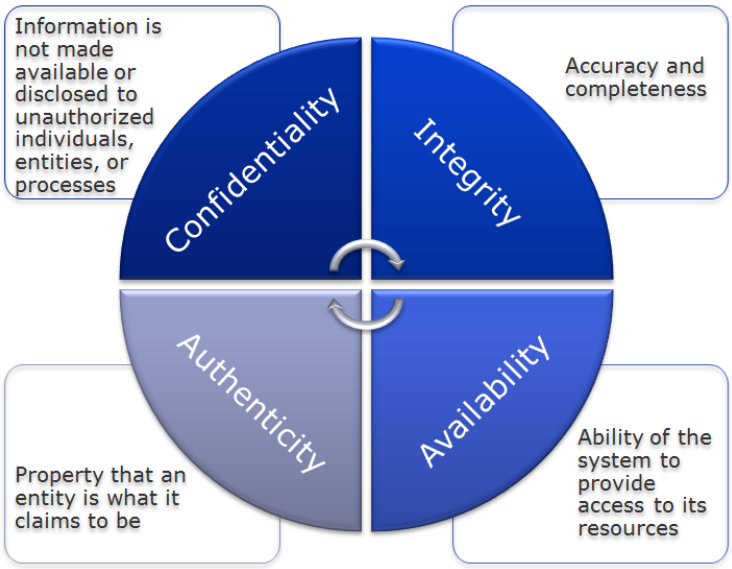

Figure 2-5 CIAA model (applied in 2014 version of the ISO/IEC 27000)

The four security properties can be of higher or lower importance. For example, for an electronic chart system confidentiality is immaterial as the charts are published information, but availability and integrity are of high importance.

For any system perceived as critical, the importance for each of the four CIAA properties should be rated by evaluating the consequence that a breach of the properties would entail, typically as high, medium or low. This can be done based on the additional information gathered in the workshop with relevant stakeholders as described in [2.3.1]. Using questions as proposed in Table 2-3 can help determine the required level of protection.

Table 2-3 Typical questions for assessing consequences

Security Property (CIAA)	*Typical questions to help rate the importance of a CIAA property*
Confidentiality	How important is the confidentiality of this information? What would happen if this information would be disclosed?
Integrity	How important is it for this information to be exact and complete? What would happen if the information would be wrong or altered?
Availability	If the system/information is unavailable for (5min/30min/1hr/1day), what would happen?
Authenticity	How important is it to know that the source of the information is who it claims to be?

This rating also serves as a reasonable estimate of the attractiveness to an attacker. While not all potential attackers are motivated by the same kind of consequence, it should be assumed that any attack resulting in significant consequence is likely to be attractive to some kind of attacker (financial gain, competitive advantage, curiosity, recognition, or sabotage/terrorism could all be motivators for some potential attackers). See App.D for more details on the implications of the CIAA.

2.3.3 Determine likelihood of attacks

After determining and rating the consequences of a successful attack, the likelihood of an attack is then determined for each system under consideration. Several factors can drive the likelihood of an attack such as the attacker's capabilities, motivation and opportunity towards the attack.

In the context of this RP (vessels in operation), it is considered impractical to consider all aspects that drive likelihood mentioned in literature. Applying such aspects would include addressing information that is either extremely difficult to calculate or not available, and would require a deep knowledge of the software code, its architecture and the availability of automation tools at the disposal of attackers which can change rapidly over time.

In this RP the assessment of the 'ease of access' is used as a practical approximation of the likelihood of an attack (ref. /40/, /41/, /42/, /43/). For example, a system that can be updated and controlled via a remote internet connection is easier to access than a stand-alone system, disconnected from the internet and kept secured behind locked doors. In this RP the following example properties are used to determine the ease of access:

— Remote connection, i.e. system access from a location not on the vessel. Examples include remote connections to an onshore operation centre or to an equipment vendor's onshore monitoring system.
— Physically accessible, i.e. access to the equipment on-board the vessel. Examples include unlocked cabinet doors and easy tampering possibilities at equipment location.
— Connected and/or integrated, i.e. a system connected with other systems via a network. Typically information sharing and centralised administration could be reason to integrate systems or create interfaces.
— Requiring software updates plays a role since this will require either a portable storage or vendor support workstation (laptop) to be connected in order to perform a software update.

The combination of the answers to these questions can help rate the ease of access as illustrated in Table 2-4:

Table 2-4 Example rating of 'ease of access'

Remote connection	*Physically accessible*	*Connected and/ or integrated*	*Requiring software updates*	*Ease of Access*
X	-	-	-	Medium
X	-	-	X	High
X	-	X	No effect on Ease of access	High
X	X			High
-	-	X		Medium
-	X	-		Medium
-	X	X		Medium
X	X	X		High
-	-	-	X	Medium
-	-	-	-	Low

2.3.4 Determine cyber security risks

Combining the likelihood (ease of access) with the consequence of successful attack will determine the CS risk of the specific critical system. As illustrated in Figure 2-6, a high likelihood of an attack combined with a high consequence of successful attack results in a high CS risk for the system under consideration.

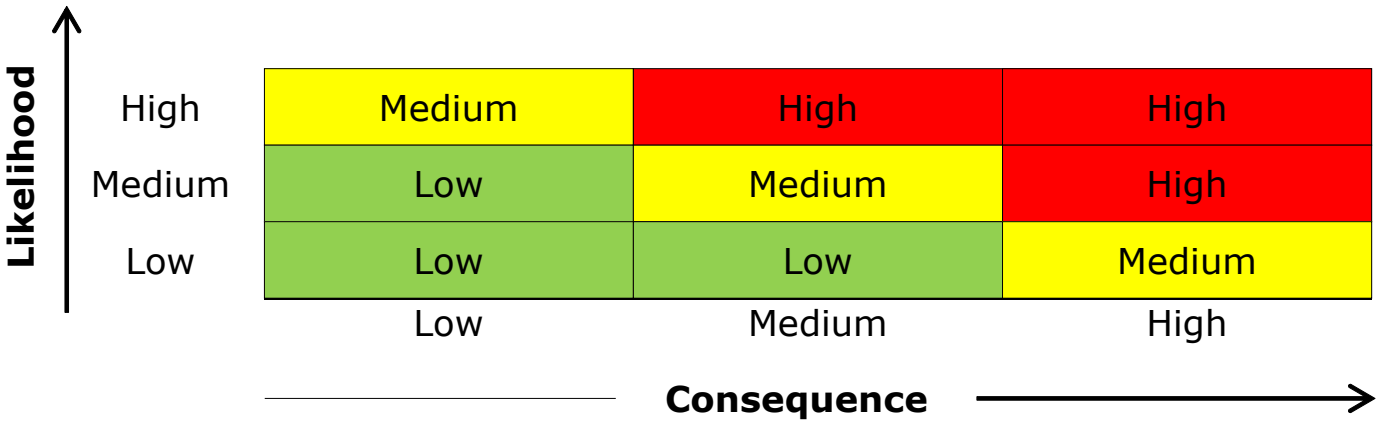

Figure 2-6 CS Risk matrix

Table 2-5 provides an example of a critical OT system (the AIS system) a critical IT system such as the PMS (planned maintenance system) and the level of risk associated to them by considering the dimensions of likelihood of an attack and consequence of successful attack.

Table 2-5 Example of cyber security risk rating for critical systems

Function/system under consideration			*Consequence*			*Likelihood*	*System CS risk*
Function	*System*	*Component*	*Security property (CIAA)*	*Importance of security property (L,M,H or N/A)*	*Reason for security property ranking*	*(L, M, H) (see Table 2-4)*	*Calculated risk (L, M, H) (See Figure 2-6)*
Navigation	AIS (OT)	N/A	Confidentiality	N/A	…	High	High
			Integrity	High	*Incorrect data can lead to collisions and grounding*		
			Availability	Low	…		
			Authenticity	Medium	…		
	GPS (OT)	…	Confidentiality	…	…	…	…
			Integrity	…	…		
			Availability	…	…		
			Authenticity	…	…		
Preventive maintenance	PMS (IT)	N/A	Confidentiality	Low	…	Medium	Medium
			Integrity	Medium	Missed mainte-nance can be harmful or costly		
			Availability	Medium	Missed mainte-nance can be harmful or costly		
			Authenticity	Low	…		

For OT systems, the CIAA ratings combined with likelihood of an attack gives an individual risk rating (one for of C, I, A and A). For IT systems, the highest of the four aspects (C, I, A, A) combined with likelihood of attack is used as the risk rating.

Depending on the size of the system and detail level of the discussion, the function/system under consideration can either be rated at the component or at the system level. The level of detail required should be determined on a case by case basis.

Acceptable alternatives can be taken into account as mitigation for the risk ranking. For example, in the event the navigation system goes offline, experienced navigators could resort to the use of paper charts and manual means of navigation to mitigate the consequences. An organisation could therefore choose to accept the system CS risk ranking if acceptable mitigation means are available. In this case the acceptable

alternative would be recorded along the ranking exercise and followed-up to confirm its effectiveness, ensure it is known, communicated and made available to the users.

2.3.5 Compare current safeguards with target

Once a critical system's specific CS risk has been determined as discussed in [2.3.4], the existing safeguards should be compared to the target safeguards depending on the IT/OT nature of the system under consideration:

— *IT*: In this RP we aim to provide practical guidance towards building more detailed checklists referencing the technical and prioritised verifiable control points (L, M, H). The BSI Grundschutz (GS) information security requirements contain a practical and technical approach to CS and is aligned with ISO/IEC 27001. Thus the BSI GS catalogue is used in this RP. For each component identified in [2.3.1]. (databases, ERP, email and operating systems, general and web servers, desk- and laptops, internet PCs, etc.), the relevant applicable IT requirements can be found in App.E. The appendix contains further information on how to construct the respective checklists.
— *OT*: IEC-62443-3-3 foundational requirements (FR) applicable to control systems on board (see App.F). The OT system risk level rating is used for prioritising what systems should receive improvement efforts. For each CIAA security property rated for the OT system under consideration the relevant applicable requirements can be found in App.F. The appendix contains further information on how to construct the respective checklists. Depending on the components that make-up the OT system under consideration, the user of this RP may also find useful component related requirements in App.E.

Comparing these requirements to the current state of CS safeguards requires preparing of customised checklists and interviewing the relevant experts, OT and IT responsible staff and users. Once the checklists have been created, detailed checks can be performed for each of the systems under consideration. Requirements that are found to not be implemented should be prioritised for action. These actions are then detailed and tracked through an improvement program.

SECTION 3 IMPROVEMENT

The assessments recommended in this RP will help to identify areas for improvement. This is particularly true for the focused assessment and the comprehensive, in depth assessment (with the high level assessment more targeted at identifying areas for further and more thorough investigation). Depending on the available resources and risk rating, management will naturally decide to initially focus its CS improvement plan on systems with high CS risks. For the risks to be addressed, different mitigation options exist as described in Table 3-1.

Table 3-1 Risk mitigating options

Risk mitigating option	*Implication*
Avoid	Circumvent the risk by changing the course of action (opposite of risk acceptance)
Reduce	Implement corrective actions to reduce the likelihood and/or the severity
Accept	Accept the risk and take the chance of the negative impact (opposite of risk avoidance)
Transfer	Risk outsourcing and sharing via third parties (e.g. cyber insurance)

A cost benefit analysis is required to determine the most efficient risk mitigation strategy. This analysis requires insights on the CS risk picture which consists of the threats, the vulnerabilities and the criticality of the systems.

Where risk reduction is the preferred choice, this RP recommends using the gaps identified in [2.2] or [2.2.5] and the respective checklists to build a work plan that needs to be agreed and implemented by the management team in charge. As the risk picture differs by segment and company, a generic improvement plan that fits all needs is not practical. In addition, as the CS risk picture continuously changes, continuous improvement cycles are needed to confirm that checklists and policies/procedures and barriers are still effective, maintained and kept up to date. The PDCA approach used for these continuous improvement cycles is required for any management system as illustrated in Figure 3-1 and discussed in [3.3]. Through these continuous improvement cycles, the organisation's CS maturity and resiliency will increase over time by moving from a reactive to a more predictive and proactive maturity level.

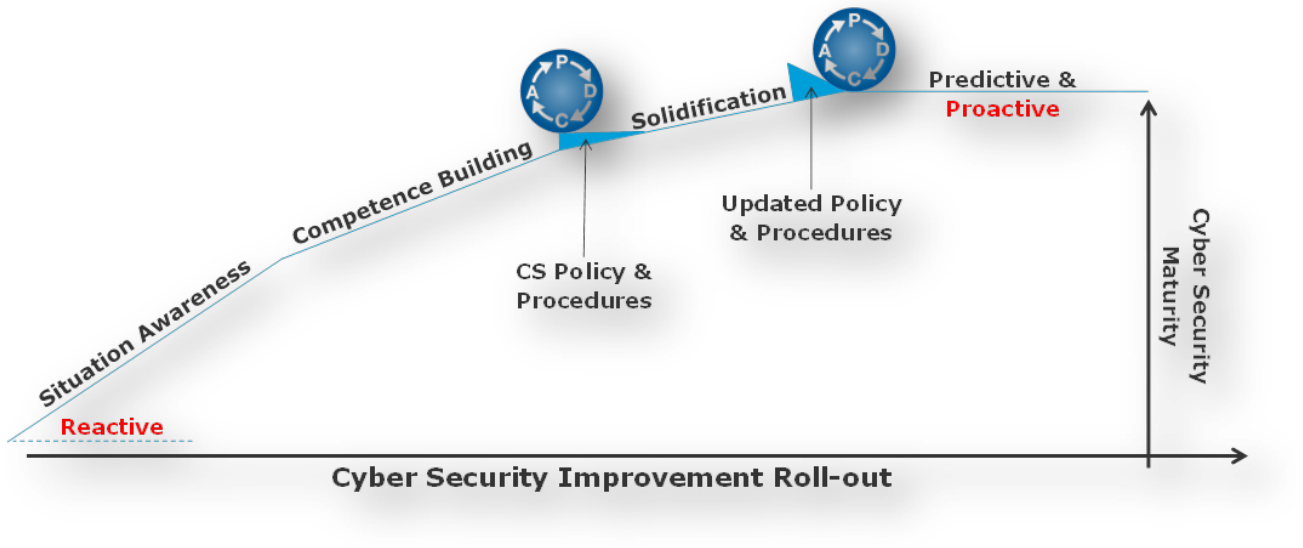

Figure 3-1 Increasing levels of an organisation's cyber security maturity

Approving investments needed for the improvement actions will most likely require a solid cost benefit analysis. An up to date risk picture with an evaluation of the current protection needs and ease of access/ robustness of the barriers in place can be helpful to build the financial models. This picture will help investment decision making as well as visualising the current CS risks. Depending on the assessment chosen, different visualisation approaches are proposed by this RP (for example the Bow-Tie method described in [2.2] or the cyber risk matrix proposed in [2.3.4]).

The improvement actions to be carried-out will depend on the organisation's maturity and changing risk picture. Actions will typically fall within the areas of competence and awareness, technical improvements and the implementation of an IT security management system.

3.1 Competence and awareness

Phishing and social engineering and unintentional downloads of malware are common issues. Symantec Security Response said: […] *"You don't need as many technical skills to find one person who might be willing, in a moment of weakness, to open up an attachment that contains malicious content. Only about 3% of the malware they run into tries to exploit a technical flaw. The other 97% is trying to trick a user through some type of social engineering scheme"* (ref. /44/). Staff in many organisations is insufficiently prepared and not competent to react correctly if CS incidents occur, possibly resulting in behaviour that does not sufficiently contribute to reducing the risks and containing the situation. The assessments proposed in this RP should highlight parts of the organisation where awareness is lacking or competencies are an issue. It is recommended to focus awareness and competence building campaigns towards these parts of the organisation. E-Learnings combined with classroom trainings can contribute to improve the situation.

Various research studies shed light on the human information retention rates. The desired behaviour and awareness in terms of CS therefore needs to be evaluated just like any other objective. This means that the organisation should have periodic refreshers based on the changing risk picture, retention rate and changing requirements. See ref. /4/ for more information on E-Learning.

Insider threat has been historically linked to physical security compromises and breaches, latest industry reports have found that over 60 percent of stolen information (electronically) or CS breaches are linked directly to insider threats. While ISO/IEC 27001 briefly includes the insider threat within the organisations CS policy, this RP proposes to address the insider threat into the overall basis of CS awareness and culture. Companies, especially small to medium business, have to balance giving employees access to information while monitoring for abnormal network use and traffic. This can be done with a written, annually reviewed information security and governance plan signed by each employee to establish policies to safeguard proprietary and sensitive information from both cyber and physical loss. Special attention should be given to former, disgruntled, or temporary employees that possess credentials to access sensitive or proprietary data. It is recommended to grant employee information access as an "implicit deny, unless required" approach. Additionally, periodic review and follow-on revocation of access credentials is a necessary part of protecting company data, and should be included expounded upon further in the organisation's CS policy (see [3.3.2] Monitoring of KPIs).

3.2 Technical improvements

A wide range of options to enhance the technical aspects of CS exists and will often be employed by or in close cooperation with the providers of the respective critical system. In this RP we propose to highlight typical improvement opportunities that are commonly found in the maritime and offshore industries:

Network segregation is a common best practice on board vessels depending on the criticality of networked devices. The minimum requirement is to have separate networks for both safety systems and critical systems for the operation of the ship. Recommended practice is to have separate networks for administrative, entertainment and internet access, with networks physically or virtually separated. Physical access to cabling and wiring closets shall be limited as should administrative access to VLAN switches. See App.A and ISO/ IEC 27002:2013 ref. /7/, section 13.1.3. If data traffic is allowed between segments, such traffic should be controlled by a firewall or a networking device with firewalling functionality. More precise guidelines on firewall settings are available in ref. /25/. When network segregation is employed as a means to address safety, reliability or cyber security requirements, it shall be maintained; any changes to the segmentation,

e.g. by introducing WLAN, changes to cabling or VLAN configuration require a thorough and documented management of change process including risk assessment.

Factory default accounts and passwords should not be allowed on any device. Many systems and network switching elements (routers, voice data multiplexers etc.) are delivered with default manufacturer passwords which should be changed during installation of new hardware and software. Resetting of default passwords should be verified and confirmed as no longer valid for accessing the system after the reset.

Access control is a basic control to mitigate risks. For instance, limiting administrative permissions to a few IT professionals can prevent the introduction of malignant files, ensure firewall integrity, etc. This can for example help avoid inadvertent file corruptions to bridge or engineering consoles from access during ordinary operations by users with unnecessary admin credentials.

Hardening secure remote connections – remote connections to both IT and OT systems shall be tightly controlled. Passwords alone are a weak protection method. Two-factor authentication systems, such as tokens, one-time passwords, or digital certificates may be hard to maintain securely in a marine environment for the lifetime of a vessel. Modern approaches of two-factor authentication frameworks should be investigated, such as OAuth (smartphone-based) or USB-pluggable hardware devices that appear to the computer like a regular keyboard.

See App.L for more information on securing remote connections.

Software configuration management is a major component of cyber risk reductions. Tracking of software changes should be included in a management of change process. See App.I for more guidance on software configuration management. Further guidance can also be found in ref. /26/ and /27/.

Software patch management helps address one of the most common vulnerabilities, namely unpatched software. Implementing this practice helps limit the effectiveness of attackers who enjoy the ease of exploiting known vulnerabilities that are in the public domain. Software patch management is part of the overarching software configuration management practice. See App.I for more guidance.

Creating software topology information helps during forensics and general fault trouble shooting but will also help trigger discussions relating to the connections between systems and the outside world (including remote access from vendors) and check if any network segregation principles have been applied (see [4.1]). This can easily be done by using the network topology as a starting point and linking and/or displaying the software system names that run on these systems by cross checking the software register. Software topology information should be maintained within the software configuration management process. A software register example can be found in Table I-2 and a software topology example is provided in Figure K-1.

The above enhancement options are given as examples of common improvement areas. A more systematic approach is described in [2.2] and more so in [2.3].

3.3 Information security management system

Many organisations find it worthwhile to establish an information security management system (ISMS) according to the international standard ISO/IEC 27001 ref. /7/. The standard is fully aligned with recent editions of the other commonly used ISO management system standards, such as ISO 9001:2015 (for quality management) and ISO 14001:2015 (for environmental management), allowing for easy integration of the ISMS into the wider scope of a company's integrated management system if so desired.

At time of writing, ISO/IEC 27001:2013 together with two corrigenda (Cor1 and Cor2) is the current edition of the standard. The relevant terms and definitions are given in ISO/IEC 27000:2016 ref. /37/, key terminology can be found in [1.1] of this RP.

ISO/IEC 27001 requires continuous CS management, through implementing an information security management system (ISMS). The ISMS shall be established, implemented, maintained and continually improved in accordance with the requirements of ISO/IEC 27001, covering the organisation, responsibilities and management of IT & OT-systems. The typical PDCA management system cycle also applies to the ISMS.

This RP deals with the operational aspects of CS Management, focusing on the ship in operation. The ISO/IEC 27001 approach complements the RP's approach with an organisation-centric approach, putting much emphasis on planning, resources, and continuous improvement.

In order to be compliant with ISO/IEC 27001 standard, all requirements of ISO/IEC 27001 shall be covered by the ISMS.

3.3.1 ISO/IEC 27001 formal requirements

ISO/IEC 27001 is divided into ten clauses and an annex. Clauses 1 to 3 contain the scope of the standard, normative references, and a reference to ISO 27000 for terms and definitions. Clauses 4 to 10 contain the requirements and are summarised below:

Clause 4: Context of the organisation

4.1-4.4 The organisation shall consider its context: its purpose, interested parties and their requirements, the scope of the ISMS, and the commitment to establish an ISMS.

Clause 5: Leadership

5.1 Top management shall show leadership and commitment, establish a cyber-security policy with respect to objectives, supply relevant resources, communicate the importance of CS, and promote continuous improvement.

5.2 The CS policy shall be appropriate and shall contain CS objectives, a commitment to applicable requirements and continuous improvement. It shall be documented, communicated within the organisation, and be made available to interested parties.

5.3 Top management shall assign responsibility for the ISMS and for the reporting of the ISMS performance.

Clause 6: Planning

6.1 The organisation shall plan the ISMS with the goals of managing and controlling cyber security risks and ensuring continuous improvement. CS risk assessment and treatment are required. The planned controls shall be compared with the list in Annex A to ensure that no necessary controls are overlooked.

6.2 Planned information security objectives shall be in line with the CS policy, measurable, communicated, and updated as appropriate. Plans shall include what will be done, with what resources, who will be responsible, when it will be completed, and how the results will be evaluated.

Clause 7: Support

7.1 The organisation shall determine and provide the necessary resources.

7.2 The organisation shall determine the necessary competences and ensure that resources are competent and/or develop the competences, and keep records.

7.3 The workforce[1] shall be aware of the CS policy, how they contribute to CS, and the implications of not conforming to CS requirements.

7.4 The organisation shall ensure that relevant internal and external communications are effective.

7.5 The ISMS system shall include documented information required by either ISO/IEC 27001 or necessary for the effectiveness of the information security management system. Documented information shall be maintained in a current and useful state, and properly controlled. It may be paper-based or electronic. This includes externally generated information such as user manuals, commissioning records, configuration settings and certificates.

[1] This includes non-employees such as contractors, riding gangs, service engineers and suppliers

Clause 8: Operation

8.1 The organisation shall plan, implement and control the processes needed to meet CS requirements, and implement the actions planned following clause 6. The organisation shall keep documented information as necessary to have confidence that the processes have been carried out as planned. Both planned and unplanned changes must be controlled. The organisation shall ensure that outsourced processes are determined and controlled.

8.2 The organisation shall perform CS risk assessments at planned intervals or before implementing significant changes, and keep records.

8.3 The organisation shall implement the CS risk treatment plan, and keep records.

Clause 9: Performance evaluation

9.1 The organisation shall select and monitor suitable KPIs.

9.2 The organisation shall perform internal audits to determine the effectiveness of the ISMS.

9.3 Top management shall review the organisation's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

Clause 10: Improvement

10.1 When a nonconformity occurs, the organisation shall react to it, take appropriate corrective action, retain adequate documentation and make changes to the ISMS as appropriate.

10.2 The organisation shall continuously improve the suitability, adequacy and effectiveness of the information security management system.

Annex A (normative) Reference control objectives and controls lists in detail controls to be used for the main clauses of the standard. The organisation's controls must be checked against this list to ensure no necessary controls are overlooked.

3.3.2 Practical implications for implementation

An organisation implementing this RP will cover most of the requirements of ISO/IEC 27001 clauses 7 and 8, and a significant part of the other clauses' requirements. Most additional work to achieve full ISO/IEC 27001 compliance will be driven by the organisation-centric clauses 4, 5, the more global aspects of clauses 6 and 9, and clause 10. Many organisations already perform a significant part of the actions required by these clauses informally, so often only formalising and documenting those activities is necessary.

The following non-exhaustive list should provide practical guidance to organisations implementing an ISMS. Relevant clauses of ISO/IEC 27001 are noted for easy reference.

Current ISO management system standards have reduced the *documentation requirements* compared to older editions and now use the term documented information to cover both documents and records. While documented information can be paper based or electronic, it shall include clear identification and description (such as title, date, author, and reference number), trace of reviews and approvals, and be in a usable format. This information can be contained in the documented information itself or kept separately, such as in a document describing the location, format and contents of a system-generated log file.

The *scope of the ISMS* has to be defined and documented (clause 4). Scope definition techniques are explained in [2.3.1] of this RP. It is possible to exclude certain business areas, processes, assets, or activities from the ISMS altogether or from some ISMS processes. For example, it would be possible to differentiate between owned and chartered vessels. The scope definition shall include *statutory, regulatory and contractual requirements*, including the requirements of customers, other stakeholders like employees and shareholders, and the society at large.

To prepare an organisation for potential CS threats, a *cyber security policy has to be developed* (clauses 5.1 and 5.2). Such a policy requires that the topics described in this section are documented according to ISO/IEC 27001 - either separately or integrated into a general company policy document like a HSSEQ

(health, safety, security, environment and quality) policy. The CS policy needs to be communicated within the company and available for all involved parties (incl. stakeholders like customers) and updated as appropriate. A detailed checklist of the required documents can be found in App.H.

Leadership commitment and responsibility for the integration of the ISMS in the company's processes and resources are essential for the success of the ISMS. Management shall communicate the importance of CS and promote continuous improvements, etc. (clause 5.1 and 5.3), and ensure the commitment and responsibilities of the different management levels.

Based on the CS policy, the organisation shall set up *cyber security objectives* (clause 6.2) that take into account applicable information security *requirements* and results from a cyber risk assessment. Objectives should be measurable (where practicable). The relation between the CS objectives and the business objectives should be clearly defined, as there can be conflicting goals that need to be carefully balanced.

ISO/IEC 27001 *Annex A* provides a detailed list of controls that the organisation shall review to ensure that no necessary controls are overlooked.

The following *security roles and responsibilities* shall be defined (clause A7.1.2 and A13.2.4):

— *Employees*: Agreement covering their liabilities and responsibilities with respect to CS, e.g. in employment contracts.
— *Suppliers*: If cyber services or products are obtained from suppliers, including contractors and cloud service providers, a supplier or vendor security policy should be available, communicated, and enforced through contractual agreements covering their liabilities and responsibilities with respect to CS. This policy shall be used in selection and management of supply contracts. A clear definition and documentation of interfaces between activities performed by the organisation and suppliers is essential. This can, for example, take the form of service level agreements (SLA), underpinning contracts, or service descriptions. Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information need to be put in place.

A comprehensive list of *inventory of assets* is required (clause A.8). This inventory should cover hardware, interconnections, and software installation, configuration/commissioning, and patch levels. [2.3.1] of this RP and App.I provides guidance to assist in preparing and maintaining the inventory.

The risk assessment and risk treatment methodology used has to be documented (clauses 6.1.2 and 6.1.3) and should include risk acceptance criteria. [2.2.5] of this RP can be used as basis. A risk assessment should be carried out, documented and regularly repeated (clauses 8.2 and 8.3).

The organisation shall develop an *access control policy* (clause A.9.1.1). The policy should cover all relevant business processes.

An *operating procedure* for the management of IT and OT systems should be developed for the topics covered by this RP (clause A.12.1.1).

The *systems engineering principle* covering IT and OT should be documented (clause A.14.2).

An *incident management procedure* shall be developed (clause A.16, see also [2.2.4] of this RP), and include:

— management responsibilities
— incident reporting
— security weakness reporting
— incident response
— drills and training.

It is recommended to set a limited number of internal key performance indicators to track the development with respect to CS (clauses 9 and 5.3). The indicators to be monitored should be defined considering CS processes and control options. It should be stated who should monitor, when and who has to evaluate the results. Typical indicators include:

— number and date of CS audits (including internal)
— number and date of CS tests
— number of security incidents and near misses and development over time (see App.J for more on logging of security incidents)

— % of software patches applied within 4 weeks of release
— drills and other educational measures performed
— number of cyber assets that cannot be patched or kept current (e.g. due to software incompatibility with current operating systems).

Internal audits are used to check if a CS management system is effectively implemented and maintained, including compliance with the company's own procedures, policies and international standards (clause 9.2). An audit plan shall be developed, stating the frequency of audits, person(s) responsible, audit methods and reporting. For each audit, criteria and scope have to be defined and auditors shall be selected based on their qualifications and objectivity, and shall not be auditing their own work. The execution of the audit plan has to be monitored, results of the audits documented and provided to the relevant management.

Management reviews shall be carried out at least annually in order to follow-up the implementation and development of the CS management system (clause 9.3). This covers review of actions status, changes, feedback incl. corrective actions, audit results and monitoring of KPIs. During a management review, results of risk assessments and implementation of risk reducing measures should be reviewed as well as opportunities for continuous improvement. The management review shall be documented.

Improvements need to be carried-out systematically on a *continuous* basis (clause 10). Possible measures to reduce existing and new CS risks should be evaluated. Non-conformities identified during audits are to be addressed without undue delays, actions taken to control and correct them. *The effectiveness of the corrective actions* should be measured and documented (clause 10.1). An example for a checklist of managing CS incidents and improvements is provided in clause A.16.1.

Within any improvement program, specific responsibilities need to be assigned (clause A.6.1.1), including those for (technical) testing of barriers, maintaining the management systems and adapting it to changes of the risk picture, as well as securing that awareness and competence are maintained at sufficient levels (clauses 7.2 and 7.3). The responsibilities will have to cover verification and validation activities as described in Sec.4.

SECTION 4 VERIFICATION AND VALIDATION

Once the CS of an organisation has been assessed and improvement actions initiated, the achieved improvements should be verified and validated. This RP proposes different approaches for verification and validation, suited for the specific needs of ships and mobile offshore units.

4.1 Monitoring and testing of technical barriers

Third-party testing can bring added value to the independent verification and validation (IV&V) activities. Expert knowledge of the personnel conducting the test can provide improved transparency and objectiveness as well as better test quality.

Generally, third-party testing methods can be applied in at least two phases. First as part of a vulnerability assessment, secondly as technical verification of the mitigating actions put in place. Both approaches are recommended. A physical test, i.e. testing by connecting to the on-board IT & OT networks can be considered part of fulfilling the requirements in regulation 8 of the ISPS Code (ship security assessment).

Typically, CS testing should cover the technical and the procedural barriers in place. At the same time, appropriate methods of testing should be able to uncover vulnerabilities in the current deployment of systems, i.e. vulnerabilities caused by software or hardware, as well as by policies and procedures. Thorough testing can uncover vulnerabilities in individual components and systems, as well as weaknesses in specific configurations used. It is recommended that component and system level testing is included in a verification and validation program.

This RP recommends to repeat testing on a recurring basis to verify if barriers are still effective and robust, given the ever changing risk picture of IT/OT systems.

However, due to the nature of software, demonstrating that there are no CS issues would require an infinite number of tests. For practical reasons the testing scope and regime should therefore be carefully planned and clearly targeted towards the highest risk within the attack surface.

4.1.1 Testing of components

Component level testing can increase confidence in new or upgraded building blocks of the systems under consideration. One particular example is a type approval program targeting the safety and security of on-board networked equipment. Figure 4-1 illustrates a component test setup where the implementation under test (IUT), e.g. an operator station, is being tested by the tester via a local network in a lab.

Employing third-party tested devices constituting various nodes in a network can increase overall CS. Test cases should be tailored to the specific environment the component will operate in; alternatively, predefined ones can be used. Both the IEC 62443-4-2 standard, applied in Embedded Device Security Assurance certification, and the IEC 61162-460 standard give guidance on testing CS of components deployed in automation and maritime systems.

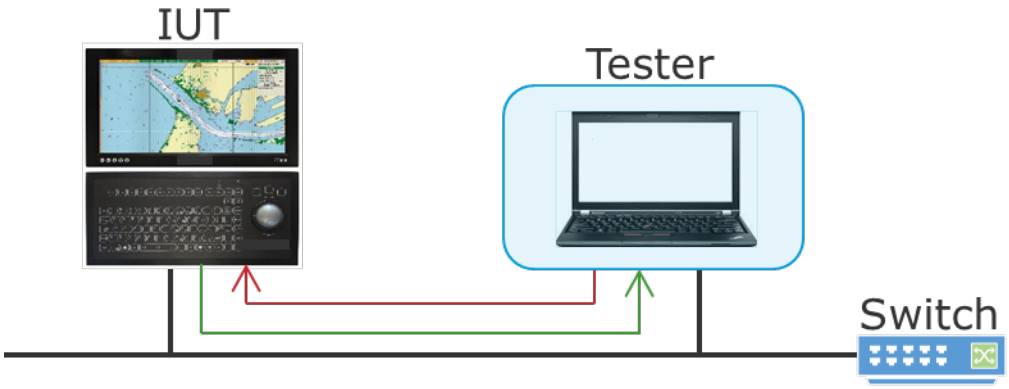

Figure 4-1 Component testing example setup

The general robustness of the communication channel can be evaluated by load testing and network storm simulation. During a network storm simulation, components are flooded with telegrams to test their capability of handling the overload. Testing individual components can also uncover weaknesses in authentication methods and other protection mechanisms. Besides probing for known vulnerabilities within the implementation, unknown vulnerabilities should be targeted by fuzz testing the input handling capabilities of components. This can be achieved through device level functionality testing to the breaking point: negative robustness test and testing against all testable requirements of security standards.

4.1.2 Testing of systems

Once component level robustness tests have been performed, system level or end-to-end tests can be performed via two types of approaches, namely actively provoking failures, e.g. by generating traffic and passive measurements that can be repeated periodically, i.e. snapshotting. The aim is to assess the network architecture against the design and to gather snapshots of the current status of the network. These snapshots can then be used as reference points when measurements are repeated at a later point in time, to be able to identify unexpected or malicious changes – a technique often employed in anomaly detection. Probing (on-board) networks for possible vulnerabilities and for robustness under high loads are important in order to verify that the implementation of the design is safe, secure and according to the documentation.

Penetration testing is a systematic employment of methods that an attacker would use to gain access. All the tools at the disposal of an attacker can be used, including social engineering attacks, depending on the scope of the study. Special care shall be taken when performing penetration tests on live (in-production) systems; it is preferable to run penetration testing against test systems (that shall be close duplicates of the targeted in-production systems to provide meaningful results) or against systems not yet in production, such as commissioning or factory acceptance tests. Penetration testing should be considered especially when employing new technology or processes as well as when the risk picture has changed.

The overall scope of verifying CS and resilience through testing should cover stress testing, robustness testing, testing for network segregation failures, screening for running undesired or unnecessary services, missing patches and outdated firmware, authentication weaknesses, known and unknown vulnerabilities, traffic anomalies and others, to answer questions such as:

— What can a malicious attacker from inside or outside the network defences do?
— Are there any known or unknown cyber vulnerabilities on the asset?
— Is there proper network segregation in place?
— Is the remote support solution secure?
— What if redundancy or communication connections are lost in the networks?
— Can operations be maintained under network stress and DoS attacks?

— Are appropriate and sufficient warnings and alarms issued?
— Are alarms and events handled properly?

Execution of CS tests shall be based on the information collected from documentation and the topology of the asset. Information can be gathered during risk assessments and security audits conducted prior to testing, likely leading to more thorough testing.

Appropriate network segregation is key when aiming to properly sealing off the control network from less critical networks, such as an office network as proposed in [3.2]. Segregation of networks should be tested as well and is deemed insufficient if a probe within the critical part of the network can be reached from the other side of a segregation point. Analysis of topology drawings can serve as a starting point for testing network segregation inside an asset.

Vendors often use remote login to provide support. During a penetration test, the security of remote login solutions shall be evaluated. If remote maintenance is allowed, the different security mechanisms shall be tested including authentication, authorisation, firewall, encryption and jump server. Remote maintenance access to critical components from the jump-server should only be allowed according to time limited work orders. Monitoring solutions for alarms and event-logs from networking devices shall be tested as well.

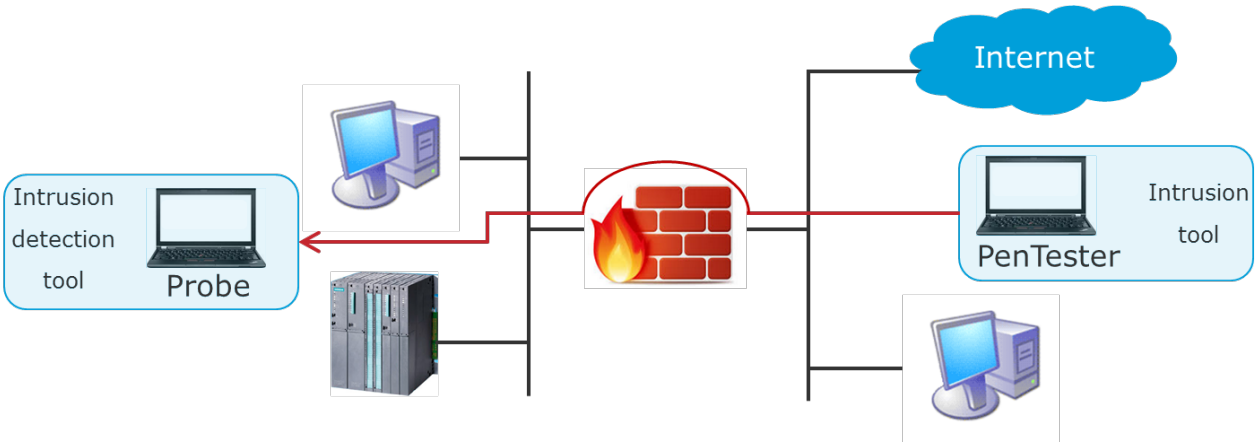

Figure 4-2 Penetration testing example setup

Many of the different tests proposed are commonly referred to as penetration testing, normally performed by qualified testers. They use techniques including simulating known attack scenarios, social engineering and testing of the physical perimeters protecting computing and networking devices.

4.2 Verification of information security management system

Verification by an accredited third party can add value by having an internationally recognized certificate to document compliance towards customers and other stakeholders. Even more importantly, making a company subject to certification (recertification) of its information security management systems helps keep the momentum of improving CS in a continuous improvement cycle. Annual external audits ensure that the organisation does not slip back into convenient but less secure behavioural patterns.

The activities relating to IT and OT systems given in this RP are significant steps to fulfil the operational requirements of ISO/IEC 27001. For the full scope of requirements, refer to ISO/IEC 27001 and especially its Annex A (normative) for a list of recommended controls. App.H indicates which of the ISO/IEC 27001 requirements are addressed by the different sections of this RP.

SECTION 5 CONCLUSION

5.1 Closing remarks

Users of the recommended practice will find that dealing with CS related challenges has many commonalities with other tasks they manage. Assessing, improving and verifying is required for any task at hand, as is the continuous improvement of these activities to secure progress over time and adaptation to a constantly changing environment.

With CS being a reasonably new challenge to the maritime and offshore industry, this recommended practice puts emphasis on a thorough assessment of the risk picture. It proposes to obtain a solid understanding of threats, vulnerabilities, possible consequences and barriers against them as foundation for any improvement and verification activity.

Following a systematic approach to increasing CS resilience makes this a manageable task. What is required is to put CS on the agenda of senior management in each company and to maintain attention over time.

SECTION 6 REFERENCES

6.1 Bibliography

/1/ DNV GL Cyber Security Self-assessment App.

/2/ BSI Self-assessment questionnaire

/3/ ISO 27001:2013 Self-Check List - Info-Tech Research Group

/4/ DNV GL Maritime Academy E-Learning on Cyber Security Awareness for staff and crew

/5/ BIMCO, The guidelines on cyber security on-boards ships, Version 1.1, February 2016

/6/ CSET tool developed by the US Department of Homeland Security (DHS 2014)

/7/ ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems -Requirements (with corrigenda Cor1 and Cor2)

/8/ ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security management

/9/ ISO/IEC 27005 Information technology - Security techniques - Information security risk management

/10/ BSI-Standard 100-1 Information Security Management (ISMS), Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.5, 2008

/11/ BSI-Standard 100-2 IT GS Methodology, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, 2008

/12/ BSI-Standard 100-3 Risk analysis based on IT-GS, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.5, 2008

/13/ BSI-Standard IT 100-4 Business Continuity Management, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, 2008

/14/ BSI IT-Grundschutz catalogue-15th edition (German), own translation into English

/15/ BSI IT-Grundschutz catalogue-13th edition (English international version)

/16/ NEK IEC 62443-2-4 Security for industrial automation and control systems Part 2-4: Security program requirements for IACS service providers

/17/ NEK IEC 62443-3-1 Security technologies for industrial automation and control systems (draft for review purposes only)

/18/ IEC 61162-460 Ed.1: Maritime Navigation And Radio Communication Equipment And Systems – Digital Interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security

/19/ International Ship and Port Facilities Security Code (ISPS)

/20/ International Safety Management (ISM) Code

/21/ Interim Guidelines On Maritime Cyber Risk Management: IMO-MSC 1/CIRC 1526 June 1st 2016

/22/ NEK IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

/23/ ISA 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components (working draft 2, edit 4, July 2, 2015)

/24/ IETF RFC 2828

/25/ CPNI Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks

/26/ IEEE Std 828-2005

/27/ DNV-OS-D203 - Integrated Software Dependent Systems (ISDS) -> Configuration Management

/28/ ENISA – Electronic evidence - A basic guide for First Responders - ISBN 978-92-9204-111-3

/29/ BSI-Industrial Control System Security - Top 10 Threats and Countermeasures 2014

/30/ BSI-ICS Security Compendium Version 1.23

/31/ Digitale Sårbarheter Maritim Sektor - Lysneutvalget

/32/ INFOSEC Institute - The Top Five Cyber Security Vulnerabilities

/33/ NIST SP-800-61, Computer Incident Handling Guide, Revision 2 (2012)

/34/ NST - Preliminary Cybersecurity Framework Core Functions: (Identify, Protect, Detect, Respond, Recover)

/35/ DNV-OS-D203 - Integrated Software Dependent Systems (ISDS)

/36/ Bowtie Methodology Manual Revision 13 - CGE Risk Management Solutions

/37/ ISO/IEC 27000:2016 Information technology - Security techniques - Information security management systems - Overview and vocabulary

/38/ Booz | Allen | Hamilton Industrial Cybersecurity Threat Briefing, June 2016 report

/39/ ISO/IEC 27000:2014 (also proposes Authenticity as a security criteria which is needed for the Comprehensive, In Depth Assessment approach in [2.3.2])

/40/ Anals of Information Systems - Christopher C.Yang, Michael Chiu-Lung Chau, Jau-Hwang Wang, Hsinchun Chen

/41/ UMI Microform 3315434 - Hybrid FMECA/CARVER model parameters and interpretation – McGill, William L

/42/ An Asset Based Approach For Industrial Cyber Security Vulnerability Analysis - by Paul Baybutt

/43/ Screening Facilities For Cyber Security Risk Analysis - by Paul Baybutt

/44/ www.pcworld.com/article/197737

APPENDIX A CYBER SECURITY BARRIER MANAGEMENT

The following are examples of Bow-Tie barrier management diagrams applied to cyber security.

BARRIERS AGAINST MALWARE

For the first example, the barrier management model and the Bow-Tie method for malware and denial of service (DoS) attacks are explained below. Some cyber security countermeasures in these samples, such as testing and training, are not usually defined as barriers, but for simplicity they are handled as such in the following examples.

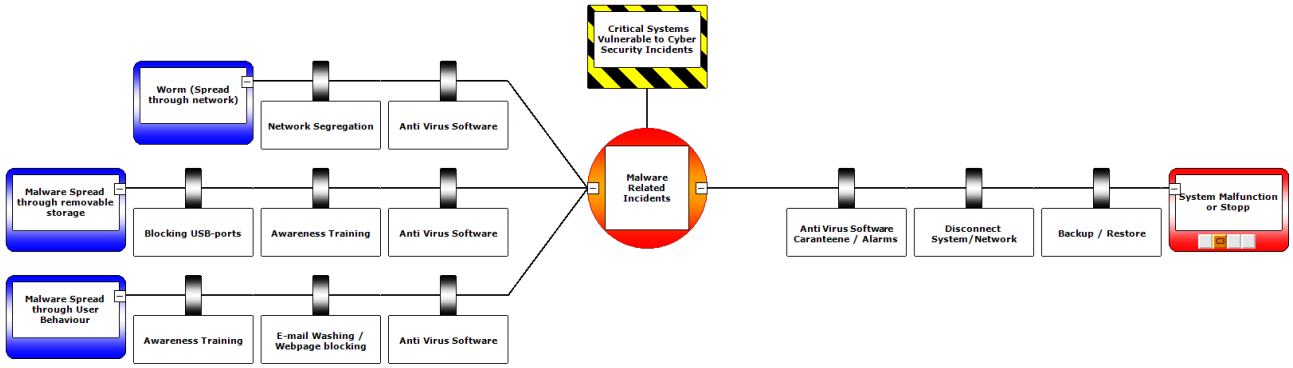

Figure A-1 Barriers against malware

This figure shows the threats categorised by how the malware can get into the system. Normally, this happens through the network (worms), through removable storage media or based on user behaviour. Social engineering is increasingly used to exploit weaknesses in user behaviour.

In this example, the barriers to prevent a worm are network segregation and limiting the traffic allowed to flow between network segments. Thus, only defined traffic (protocols) and nodes (addresses) are allowed. Special intrusion prevention systems (IPS) that recognise and block known malicious patterns are available, but these are mainly targeted at larger information systems and they may not be suitable for industrial control systems. However, anti-virus and anti-spyware software are mandatory for all malware threats as well, including the regime to keep the signatures updated. Updating anti-virus and spyware software for ships may require manual procedures since data traffic to ships may be limited due to segmentation and limited bandwidth. System hardening and patch management are needed barriers for malware given that changes are tested, particularly for critical systems. Lastly, a software patch inventory system is essential to know what patches have been installed in all components.

Figure A-1 indicates the left side of Bow-Tie enabling to lower the probability of successful attacks by addressing threats with the 4 Ds:

— *Deter*: Logs of security events need to be continuously monitored to deter malicious insider attacks and to detect attack, to be conserved for forensics after security compromise [IEC 62443-3 §7.3.4, §8.6.3]
— *Detect*: Successful additional protection on the attack path from the outside to the inside of the network does not rely on border defence alone but also on detection and reaction [IEC 62443-3 §5.6.2]
— *Delay*: Standards action may be defined as, for example, unlimited retry, unlimited retries with progressive delay, or lock-out after a limited number of retries, and possible generation and escalation of alarms [IEC 62443-3 §8.3.4.2]
— *Deny*: partitioning of resources, delimited physical or logical zone to allow or deny access to certain resources, subject to access rules and control mechanisms. Partitions can be hierarchical [IEC 62443-3 §3.1.42, §5.6.2].

BARRIERS AGAINST DENIAL OF SERVICE ATTACKS

A denial of service attack makes a system or network resource unavailable to its intended users (deny the service). A coordinated DoS attack from multiple sources is called a distributed denial of service attack (DDoS). Either of these may also be executed to camouflage other attacks, such as espionage or hacking. The figure below shows a simplified Bow-Tie for a DoS attack against an industrial control system.

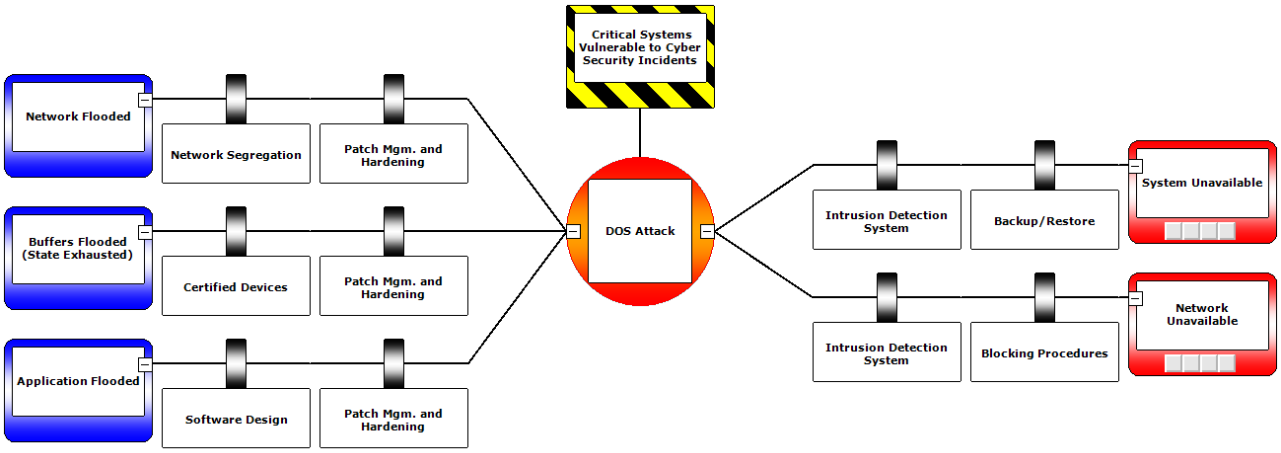

Figure A-2 Barriers against DoS attack

In the scenario depicted in the above figure, the attacker floods the network, floods buffers in devices (e.g. state buffers in the firewall) or floods the application (e.g. by doing frequent resource intensive operations).

Barriers to prevent a network flooding threat shall segregate the network and limit the traffic allowed to flow between the segments. Only a minimum of defined traffic (protocols) and nodes (addresses) should be allowed. Special devices to block DoS attacks (cleaning centres or scrubbing centres) are available, but they are mainly targeted at larger information systems and may not be suitable for industrial control systems on-board a ship, offshore rig or terminal. As with malware barriers, software updates and patch management are important barriers as well as hardening of systems for all types of attacks.

Typical barriers to prevent buffer flooding are the use of security certified devices and to configure the devices according to certificate requirements.

Application flooding is primarily addressed by building resistance into the application design so that it is resistant against "legal input with evil intent". Then, coupled with strong user authentication and authorisation, an effective barrier to application flooding can be established.

In order to reduce the consequences of a DoS attack, the unwanted traffic shall be identified and there are special intrusion detection systems (IDS) or DoS detection systems available, but these may not be suitable for the smaller shipboard and offshore industrial control systems. So, another approach for a DoS barrier is to use simpler devices to monitor the network traffic and establish procedures to monitor these logs. Then, if abnormalities are detected, the source network should be blocked and systems may be restored.

BARRIERS FOR THE HANDLING OF REMOTE CONNECTIONS

New satellite based connections makes it possible to conduct remote maintenance of components even when the ship is in operation. Public and private networks (telephony, wireless, mobile phone and internet) are used as transmission media. If these access points are planned inadequately, configured incorrectly or are not monitored, threat agents may access individual ICS components and the ICS infrastructure in an unauthorised manner and bypass the security mechanisms at the perimeter.

By allowing such connections, a large attack surface for malicious attackers is enabled, and proper barriers are mandatory.

A sample bow tie for such barriers is shown in Figure A-3:

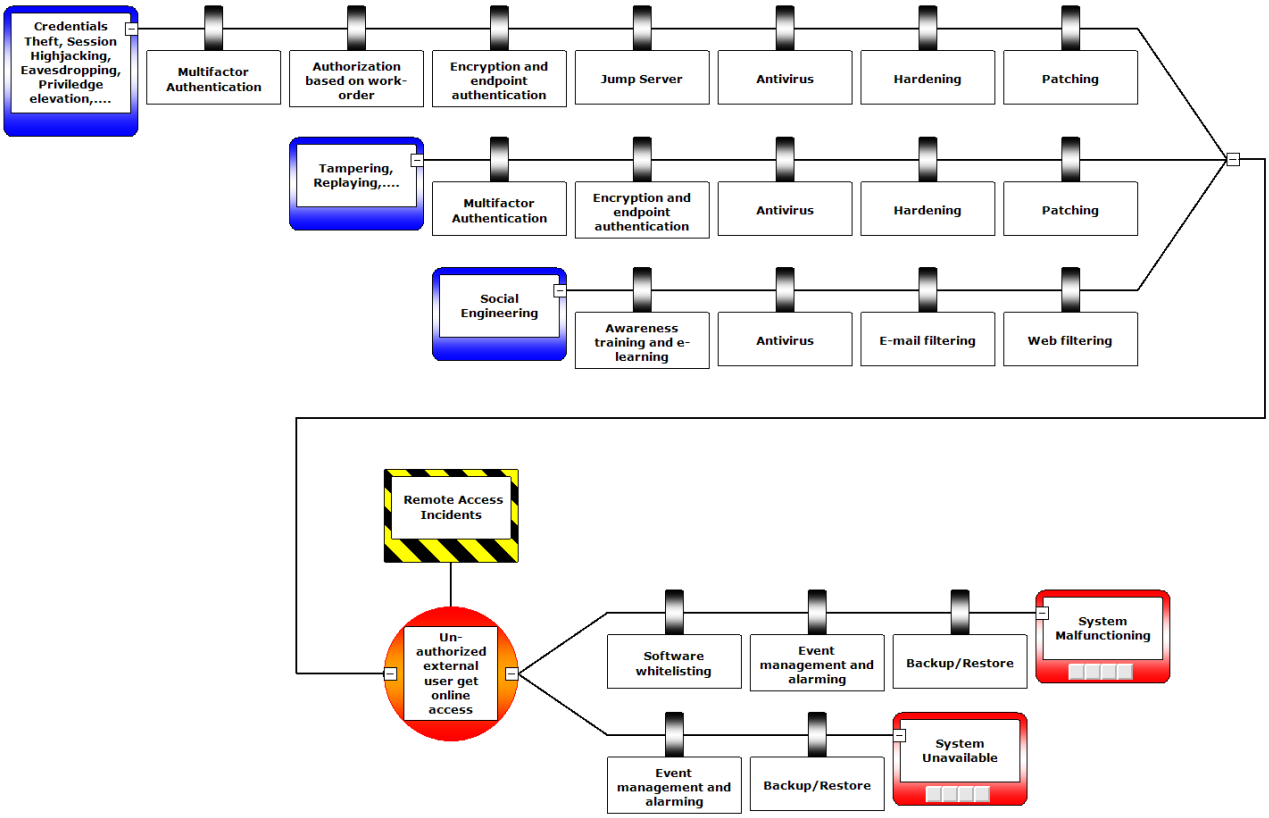

Figure A-3 Barriers to secure remote connections

In the scenario depicted in the above figure, a malicious attacker may use traditional hacking techniques to gain online access to a critical system on board. Without gaining access, the attacker may also modify or replay control sequences.

The typical barriers to prevent such incidents are firstly to make sure the operator is identified. This is done by implementing multifactor authentication. Then access shall be given only in a limited time period based on the work order. The network connection should be encrypted and the communication endpoints should be authenticated by digital certificates. Then the session from the user client should be terminated in a jump-server. This server is normally placed in a separate network segment. A new session from the jump-server to the target system is then established. Antivirus, hardening and patching of all components including remote operator clients should be assured.

Without compromising technical barriers, a malicious attacker may also use social engineering to gain credentials etc. from unsuspecting authorised users. Awareness training for personnel is therefore vital. To limit exposure for social engineering, e-mail and web filtering should be implemented. Multifactor authentication will reduce the risk for compromised passwords. Remote access solutions normally involve file transfer capabilities which require additional barriers.

APPENDIX B MAPPING OF IT SYSTEMS

Example tables supporting the mapping of IT systems to IT supported processes are provided below.

Table B-1 Example of IT supported processes

Identifier	*Description of IT supported process*	*Responsible person*	*Users*
P1	Processing of ship administrative information	Master	Officers
P2	IT-System management (admin system, intrusion prevention, etc.)		
P3	Surveillance (physical access control, closed circuit television (CCTV) and personnel on board system)		
P4	Ship communication (e.g. Email, fax, intercom, sat-telephones, mobile phones)		
P5	Information provision via data storage devices (e.g. USB,DVD/CD, portable HDD)		
P6	Maintenance		
P7	Crew entertainment (crew facing networks (entertainment, communication, internet)		
P8	Passenger entertainment (passenger facing networks (entertainment, communication, internet).		
P9	Passenger servicing and management system		
P10	Remote support and access/connectivity (secure connections to onshore) for performing IT support from land based IT department		
P11	…		
…			

Table B-2 Example of inventory of IT systems

Identifier	*Description*	*Platform*	*No. of components*	*Installation site*	*Users*	*Admin rights*	*Remote access*	*USB/DVD access*	*Restricted physical access*
S1	Group of clients for vessel administration	Windows 7	6	Bridge, cargo control room, etc.	Officers only	Master	Yes or No	Yes or No	Yes or No
S2	Group of servers								

Identifier	*Description*	*Platform*	*No. of components*	*Installation site*	*Users*	*Admin rights*	*Remote access*	*USB/DVD access*	*Restricted physical access*
S3	Group of printers								
S4	Group of external HDD								
S5	Group of wireless access points								
S6	Group of firewalls								
S7	Group of IP telephones								
…									

Table B-3 Example of mapping

Identifier	*Description of IT process*	*IT system*			
		S1	*S2*	*S3*	*S…*
P1	Processing of ship administrative information	x	x	x	
P2	IT-System management (admin system, intrusion prevention, etc.)	x	x	x	
P3	Security control (physical access control, surveillance system, closed circuit television (CCTV) and personnel on board system)	x	x		
P4	Ship communication (e.g. Email, fax, intercom, sat-telephones, mobile phones)	x	x	x	
P5	Information provision via data storage devices (e.g. USB,DVD/CD, portable HDD)	x	x		x
P6	Maintenance	x	x	x	
P7	Crew entertainment (crew facing networks (entertainment, communication, internet)	x	x		
P8	Passenger entertainment (passenger facing networks (entertainment, communication, internet).	x	x	x	
P9	Passenger servicing and management system	x	x		
…					

APPENDIX C MAPPING OF OT SYSTEMS

The table below intends to guide the reader in mapping OT systems with vessel functions/services as described in section [2.2.5]. The list of systems is not to be considered complete and the relevance of the listed OT systems depends on technical arrangement and vessel type. Other systems might be applicable and have to be assessed case-by-case.

Table C-1 Example of vessel functions and related OT systems

Vessel function/service	*OT system*

Water tight integrity	— Local and remote control, monitoring and alarm systems for:
	  — water tight doors
	  — shell doors
	  — hatches

Power generation and distribution	— Local and remote control, monitoring and alarm systems for:
	  — engine, turbine, generator, battery and other power sources
	  — auxiliary machinery
	— Power management system
	— Power source safety system
	— Electrical circuit protection system

Propulsion	— Local and remote control, monitoring and alarm system for:
	  — propulsion system (driver, shaft, gear, propeller, etc)
	  — propulsion auxiliary machinery
	— Propulsion safety system

Steering	— Local and remote control, monitoring and alarm systems for:
	  — steering (rudder, thruster, waterjet, etc.)
	  — steering auxiliaries

Navigation	— Radar — Electronic chart display and information system (ECDIS) — Heading/gyro system — Autopilot — Automatic identification system (AIS) — Position reference system (GPS, etc.) — Voyage data recorder (VDR) — Bridge navigation watch alarm system (BNWAS) — CCTV — Navigation light system — Weather routing assistance system
Communication	— External communication system (GMDSS, satellite, radio etc.) — Internal communication system (PA, GA, telephone, radio etc.)
Drainage and bilge pumping	— Local and remote control, monitoring and alarm systems for bilge pumps, valve, sensors — Water ingress monitoring and alarm system

Vessel function/service	*OT system*
Ballasting	— Local and remote control, monitoring and alarm systems for ballast pumps, valve, sensors — Load calculation system
Anchoring	— Anchor and winch control and monitoring system — Position mooring control system
Cargo operation	— Local and remote control, monitoring and alarm systems for cargo pumps, valve — Cargo level, pressure and temperature monitoring and alarm system — Cargo tank and other cargo-related safety systems — Inert gas control and monitoring system — Loading and offloading control and monitoring system — Crane control and monitoring system — Cargo conditioning, temperature, ventilation system
Fire and gas	— Fire detection system — Gas detection system (gas fuel) — Fire door control and monitoring system — Fire pump control and monitoring — Fire extinguishing systems
Ignition source control	— Gas detection system — Emergency shutdown system
Accommodation and passenger	— Ventilation and climate control system — Emergency safety/response system — Flooding detection system

Dynamic positioning	— Local and remote control, monitoring and alarm system for:
	  — DP-thrusters and other driven units for positioning
	  — auxiliary machinery
	— DP control system
	— Independent joystick system
	— DP sensors and reference systems

Drilling	— Hoisting control and monitoring system — Rotation control and monitoring system — Vertical pipe handling control and monitoring system — Horizontal pipe handling control and monitoring system — Well control and monitoring system — Mud and shaker control and monitoring system — Well intervention control and monitoring system — Manage pressure drilling control and monitoring system — Heave compensation control and monitoring system

Vessel function/service	*OT system*
Oil and gas production	— Process control and monitoring system — Production safety system — Production skid local control and monitoring system — Production skid safety system — Subsea control and monitoring system — High integrity pressure protection system (HIPPS)
Other	— Auxiliary boiler control and monitoring system — Auxiliary safety system — Incinerator control and monitoring system — Main alarm system — Integrated control, monitoring, alarm and safety system — CCTV — Jacking control and monitoring system — Pollution prevention system

APPENDIX D DNV GL PROFILING OF BSI STANDARD 100-2 IMPLICATIONS OF CONSEQUENCE BY CIAA CATEGORY

The following consequence category descriptions are given in order to help the reader determine if the consequence is low, medium or high, and should be read as an extension of Table 2-3. This table has been profiled based on the generic "Protection requirements categories" of the BSI Standard 100-2 IT-Grundschutz Methodology, Ref. /11/.

Table D-1

	Consequence		
	Low	*Medium*	*High*
Violations of laws, regulations, or contracts	Violations of regulations and laws with minor consequences. Minor breaches of contract which result in at most minor contractual penalties.	Violations of regulations and laws with substantial consequences. Major breaches of contract with high contractual penalties.	Fundamental violations of regulations and laws. Breaches of contract with ruinous damage liabilities.
Impairment of the right to informational self-determination	Processing of personal data that could adversely affect the social standing or financial wellbeing of those concerned.	Processing of personal data that could have a seriously adverse effect on the social standing or financial well-being of those concerned.	Processing of personal data that could result in the injury or death of the persons concerned or that could endanger the personal freedom of the persons concerned.
Physical injury	Does not appear possible.	Physical injury to an individual cannot be absolutely ruled out.	Serious injury to an individual is possible. There is a danger to life and limb.
Impaired ability to perform tasks	Impairment was assessed to be tolerable for vessel. No risk of external impact (e.g. collision, grounding).	Impairment of the ability to perform some tasks at hand was assessed as intolerable for vessel.	Impairment of the ability to perform tasks was assessed as intolerable for vessel.
Negative internal or external effects	Only minimal impairment or only internal impairment of the reputation/trustworthiness of the organisation is expected.	Considerable impairment of the reputation/ trustworthiness can be expected.	A nation-wide or world-wide loss of reputation/ trustworthiness is conceivable, possibly even endangering the existence of the organisation.
Financial consequences	The financial loss is acceptable to the organisation.	The financial loss is considerable, but does not threaten the existence of the organisation.	The financial loss threatens the existence of the organisation.

APPENDIX E DNV GL PROFILING OF BSI GS REQUIREMENTS FOR GENERAL IT SYSTEMS

BSI is the German Federal Office for Information Security. The IT-GS catalogues address developments in the field of IT, for which government agencies and companies shall find solutions, taking into account user comfort, costs, and security in equal measures. These catalogues are recognised by the European Union Agency for Network and Information Security and are IT baseline protection manuals with adaptations to the latest state of the art, proposed by the *Bundesamt für Sicherheit in der Informationstechnik* (BSI).

These following tables guide the reader in determining which of the BSI GS cyber security requirements apply for general IT systems, networks and applications. Next to the listed IT systems, safeguard references the BSI GS requirements catalogue are listed, and the last columns identify which of the security requirements apply based on the risk level resulting from the assessment in [2.3.5] (L = low, M = medium or H = high). At time of writing, only the 13th international edition has been officially published in English, therefore in this RP Table E-4 has been added as an indication of the additional requirements of the 15th edition that complement the 13th edition of the BSI-GS catalogue.

Table E-1 Requirements for IT system; Module 3 – IT-systems

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.101 General server	S 2.22	Escrow of passwords			×
S 3.101 General server	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 3.101 General server	S 4.24	Ensuring consistent system management	×	×	×
S 3.101 General server	S 4.93	Regular integrity checking			×
S 3.101 General server	S 4.238	Use of local packet filters	×	×	×
S 3.101 General server	S 4.239	Secure operation of a server	×	×	×
S 3.101 General server	S 4.240	Setting up a testing environment for servers			×
S 3.101 General server	S 5.8	Regular security checks of the network		×	×
S 3.101 General server	S 5.9	Logging on the server		×	×
S 3.102 Servers under Unix	S 4.25	Use of logging in Unix systems	×	×	×
S 3.102 Servers under Unix	S 4.26	Regular security checks of Unix systems			×
S 3.107 S/390 and zSeries mainframes	S 2.291	Security reporting and security audits under z/OS			×
S 3.107 S/390 and zSeries mainframes	S 2.292	Monitoring of z/OS systems		×	×
S 3.107 S/390 and zSeries mainframes	S 2.293	Maintenance of zSeries systems			×
S 3.107 S/390 and zSeries mainframes	S 2.294	Synchronisation of z/OS passwords and RACF commands			×
S 3.107 S/390 and zSeries mainframes	S 4.210	Secure operation of the z/OS operating system		×	×
S 3.107 S/390 and zSeries mainframes	S 4.214	Administration of data media under z/OS systems		×	×

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.107 S/390 and zSeries mainframes	S 4.215	Protection of z/OS utilities that are critical to security		×	×
S 3.107 S/390 and zSeries mainframes	S 4.218	Information on character set conversion in z/OS systems			×
S 3.108 Windows Server 2003	S 2.368	Handling of administrative templates under Windows Server 2003 and higher			×
S 3.108 Windows Server 2003	S 2.369	Regular security-relevant maintenance of a Windows Server 2003	×	×	×
S 3.108 Windows Server 2003	S 2.370	Administration of access rights under Windows Server 2003 and higher	×	×	×
S 3.108 Windows Server 2003	S 4.56	Secure deletion under Windows operating systems			×
S 3.109 Windows Server 2008	S 2.368	Handling of administrative templates under Windows Server 2003 and higher			×
S 3.109 Windows Server 2008	S 2.369	Regular security-relevant maintenance of a Windows Server 2003	×	×	×
S 3.109 Windows Server 2008	S 2.370	Administration of access rights under Windows Server 2003 and higher	×	×	×
S 3.109 Windows Server 2008	S 4.56	Secure deletion under Windows operating systems			×
S 3.109 Windows Server 2008	S 4.343	Reactivation of Windows systems from a volume licence contract in Vista or Server 2008 and higher versions			×
S 3.109 Windows Server 2008	S 4.344	Monitoring of Windows Vista, Windows 7 and Windows Server 2008 systems		×	×
S 3.109 Windows Server 2008	S 4.411	Secure use of DirectAccess under Windows			×
S 3.109 Windows Server 2008	S 4.415	Secure operation of biometric authentication under Windows			×
S 3.109 Windows Server 2008	S 4.416	Use of Windows Server Core			×
S 3.109 Windows Server 2008	S 4.417	Patch Management with WSUS under Windows Server 2008 and higher		×	×
S 3.201 General client	S 3.18	Log-out obligation for PC users	×	×	×
S 3.201 General client	S 4.2	Screen lock	×	×	×
S 3.201 General client	S 4.3	Use of virus protection programs	×	×	×
S 3.201 General client	S 4.4	Correct handling of drives for removable media and external data storage			×
S 3.201 General client	S 4.200	Handling of USB storage media			×
S 3.201 General client	S 4.238	Use of local packet filters	×	×	×
S 3.201 General client	S 4.241	Secure operation of clients	×	×	×
S 3.201 General client	S 4.242	Setting up a reference installation for clients			×

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.201 General client	S 5.45	Secure use of browsers		×	×
S 3.202 General stand-alone IT systems	S 2.22	Escrow of passwords			×
S 3.202 General stand-alone IT systems	S 3.18	Log-out obligation for PC users	×	×	×
S 3.202 General stand-alone IT systems	S 4.2	Screen lock	×	×	×
S 3.202 General stand-alone IT systems	S 4.4	Correct handling of drives for removable media and external data storage			×
S 3.202 General stand-alone IT systems	S 4.30	Utilisation of the security functions offered in application programs	×	×	×
S 3.203 Laptop	S 1.33	Safe keeping of laptop PCs during mobile use	×	×	×
S 3.203 Laptop	S 1.34	Safe keeping of laptop PCs during stationary use	×	×	×
S 3.203 Laptop	S 1.35	Pooled storage of portable IT systems			×
S 3.203 Laptop	S 1.46	Use of anti-theft devices			×
S 3.203 Laptop	S 4.3	Use of virus protection programs	×	×	×
S 3.203 Laptop	S 4.27	Laptop access protection	×	×	×
S 3.203 Laptop	S 4.28	Software reinstallation in the case of change of laptop users			×
S 3.203 Laptop	S 4.31	Ensuring power supply during mobile use	×	×	×
S 3.203 Laptop	S 4.235	Comparison of stored data on laptops		×	×
S 3.203 Laptop	S 4.236	Central administration of laptops			×
S 3.203 Laptop	S 4.255	Use of the IrDA interfaces	×	×	×
S 3.204 Unix client	S 4.25	Use of logging in Unix systems	×	×	×
S 3.204 Unix client	S 4.26	Regular security checks of Unix systems			×
S 3.208 Internet PCs	S 2.313	Secure registration with Internet services	×	×	×
S 3.208 Internet PCs	S 4.3	Use of virus protection programs	×	×	×
S 3.208 Internet PCs	S 4.152	Secure operation of Internet PCs		×	×
S 3.208 Internet PCs	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 3.208 Internet PCs	S 5.93	Security issues relating to the use of web browsers by Internet PCs	×	×	×
S 3.208 Internet PCs	S 5.94	Security issues relating to the use of e-mail clients by Internet PCs	×	×	×
S 3.208 Internet PCs	S 5.95	Secure e-commerce using Internet PCs		×	×
S 3.208 Internet PCs	S 5.96	The secure use of webmail	×	×	×

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.209 Windows XP client	S 2.329	Introduction of Windows XP SP2	×	×	×
S 3.209 Windows XP client	S 2.330	Regular checks of the Windows XP, Windows Vista and Windows 7 security policies and their implementation		×	×
S 3.209 Windows XP client	S 4.56	Secure deletion under Windows operating systems			×
S 3.209 Windows XP client	S 4.146	Secure operation of Windows client operating systems	×	×	×
S 3.209 Windows XP client	S 4.148	Monitoring a Windows 2000/XP system		×	×
S 3.209 Windows XP client	S 4.249	Keeping Windows client systems up to date	×	×	×
S 3.210 Windows Vista client	S 2.330	Regular checks of the Windows XP, Windows Vista and Windows 7 security policies and their implementation		×	×
S 3.210 Windows Vista client	S 2.443	Implementation of Windows Vista SP1	×	×	×
S 3.210 Windows Vista client	S 4.56	Secure deletion under Windows operating systems			×
S 3.210 Windows Vista client	S 4.146	Secure operation of Windows client operating systems	×	×	×
S 3.210 Windows Vista client	S 4.249	Keeping Windows client systems up to date	×	×	×
S 3.210 Windows Vista client	S 4.343	Reactivation of Windows systems from a volume licence contract in Vista or Server 2008 and higher versions			×
S 3.210 Windows Vista client	S 4.344	Monitoring of Windows Vista, Windows 7 and Windows Server 2008 systems		×	×
S 3.211 Client under Mac OS X	S 2.359	Monitoring and administration of storage systems		×	×
S 3.211 Client under Mac OS X	S 2.360	Security audits and reporting for storage systems		×	×
S 3.211 Client under Mac OS X	S 4.275	Secure operation of storage systems	×	×	×
S 3.212 Clients under Windows 7 or higher	S 2.330	Regular checks of the Windows XP, Windows Vista and Windows 7 security policies and their implementation		×	×
S 3.212 Clients under Windows 7 or higher	S 4.56	Secure deletion under Windows operating systems			×
S 3.212 Clients under Windows 7 or higher	S 4.146	Secure operation of Windows client operating systems	×	×	×
S 3.212 Clients under Windows 7 or higher	S 4.249	Keeping Windows client systems up to date	×	×	×
S 3.212 Clients under Windows 7 or higher	S 4.343	Reactivation of Windows systems from a volume licence contract in Vista or Server			×
S 3.212 Clients under Windows 7 or higher	S 4.344	Monitoring of Windows Vista, Windows 7 and Windows Server 2008 systems		×	×
S 3.212 Clients under Windows 7 or higher	S 4.420	Secure use of the Maintenance Center under Windows 7	×	×	×
S 3.212 Clients under Windows 7 or higher	S 4.422	Use of BitLocker To Go in Windows 7 and higher			×

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.301 Security gateway (firewall)	S 2.78	Secure operation of a firewall	×	×	×
S 3.301 Security gateway (firewall)	S 2.302	Security gateways and high availability			×
S 3.301 Security gateway (firewall)	S 4.47	Logging of security gateway activities	×	×	×
S 3.301 Security gateway (firewall)	S 4.100	Security gateways and active content			×
S 3.301 Security gateway (firewall)	S 4.101	Firewalls and encryption			×
S 3.301 Security gateway (firewall)	S 4.222	Correct configuration of security proxies		×	×
S 3.301 Security gateway (firewall)	S 4.223	Integration of proxy servers into the security gateway		×	×
S 3.301 Security gateway (firewall)	S 4.225	Use of a logging server on a security gateway			×
S 3.301 Security gateway (firewall)	S 4.226	Integration of virus scanners into a security gateway			×
S 3.301 Security gateway (firewall)	S 4.227	Use of a local NTP server for time synchronisation			×
S 3.301 Security gateway (firewall)	S 5.39	Secure use of protocols and services	×	×	×
S 3.301 Security gateway (firewall)	S 5.46	Installing stand-alone-systems for Internet use	×	×	×
S 3.301 Security gateway (firewall)	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 3.301 Security gateway (firewall)	S 5.70	Network address translation (NAT)	×	×	×
S 3.301 Security gateway (firewall)	S 5.71	Intrusion detection and intrusion response system			×
S 3.301 Security gateway (firewall)	S 5.115	Integration of a web server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.116	Integration of an email server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.117	Integration of a database server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.118	Integration of a DNS server into a security gateway			×
S 3.301 Security gateway (firewall)	S 5.119	Integration of a web application with web, application, and database servers into a security gateway			×

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.301 Security gateway (firewall)	S 5.120	Handling of ICMP on the security gateway	×	×	×
S 3.303 Storage systems and storage networks	S 2.359	Monitoring and administration of storage systems		×	×
S 3.303 Storage systems and storage networks	S 2.360	Security audits and reporting for storage systems		×	×
S 3.303 Storage systems and storage networks	S 4.275	Secure operation of storage systems	×	×	×
S 3.304 Virtualisation	S 2.448	Monitoring the function and configuration of virtual infrastructures		×	×
S 3.304 Virtualisation	S 2.449	Minimum use of console accesses to virtual IT systems			×
S 3.304 Virtualisation	S 4.348	Time synchronisation in virtual IT systems			×
S 3.304 Virtualisation	S 4.349	Secure operation of virtual infrastructures	×	×	×
S 3.305 Terminal servers	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 3.305 Terminal servers	S 4.3	Use of virus protection programs	×	×	×
S 3.305 Terminal servers	S 4.367	Secure use of client applications for terminal servers		×	×
S 3.305 Terminal servers	S 4.368	Regular audits of the terminal server environment		×	×
S 3.305 Terminal servers	S 5.164	Secure use of a terminal server from a remote network		×	×
S 3.401 Telecommunications system	S 3.82	Training on the secure use of PBX systems		×	×
S 3.401 Telecommunications system	S 4.5	Logging for PBX systems		×	×
S 3.401 Telecommunications system	S 4.6	Audit of the PBX configuration			×
S 3.402 Fax machine	S 2.48	Designating authorised fax operators			×
S 3.402 Fax machine	S 2.51	Producing copies of incoming fax messages			×
S 3.402 Fax machine	S 2.52	Supply and monitoring of consumables			×
S 3.402 Fax machine	S 2.53	Deactivation of fax machines after office hours			×
S 3.402 Fax machine	S 4.43	Fax machine with automatic envelopment sealing system			×
S 3.402 Fax machine	S 5.24	Use of a suitable fax cover sheet			×
S 3.402 Fax machine	S 5.25	Using transmission and reception logs	×	×	×
S 3.402 Fax machine	S 5.26	Announcing fax messages via telephone			×
S 3.402 Fax machine	S 5.27	Acknowledging successful fax reception via telephone			×
S 3.402 Fax machine	S 5.28	Acknowledging correct fax origin via telephone			×

Module 3 – IT Systems	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.402 Fax machine	S 5.29	Periodic checks of destination addresses and logs			×
S 3.404 Mobile telephones	S 2.189	Blocking of the mobile phone in the event of its loss	×	×	×
S 3.404 Mobile telephones	S 4.115	Safeguarding the power supply of mobile phones		×	×
S 3.404 Mobile telephones	S 4.255	Use of the IrDA interfaces	×	×	×
S 3.404 Mobile telephones	S 5.78	Protection against mobile phone usage data being used to create movement profiles			×
S 3.404 Mobile telephones	S 5.79	Protection against call number identification during use of mobile phones			×
S 3.404 Mobile telephones	S 5.80	Protection against bugging of indoor conversations using mobile phones			×
S 3.404 Mobile telephones	S 5.81	Secure transmission of data over mobile phones		×	×
S 3.405 PDA	S 1.33	Safe keeping of laptop PCs during mobile use	×	×	×
S 3.405 PDA	S 4.3	Use of virus protection programs	×	×	×
S 3.405 PDA	S 4.31	Ensuring power supply during mobile use	×	×	×
S 3.405 PDA	S 4.228	Using the built-in security mechanisms on PDAs	×	×	×
S 3.405 PDA	S 4.229	Secure operation of PDAs			×
S 3.405 PDA	S 4.230	Central administration of PDAs			×
S 3.405 PDA	S 4.232	Secure use of extended memory cards			×
S 3.405 PDA	S 4.255	Use of the IrDA interfaces	×	×	×
S 3.406 Printers, copiers, and all-in-one devices	S 2.52	Supply and monitoring of consumables			×
S 3.406 Printers, copiers, and all-in-one devices	S 4.302	Logging on printers, copiers, and all-in-one devices			×
S 3.406 Printers, copiers, and all-in-one devices	S 4.303	Use of network-enabled document scanners			×
S 3.406 Printers, copiers, and all-in-one devices	S 4.304	Administration of printers			×
S 3.406 Printers, copiers, and all-in-one devices	S 5.146	Network separation when using all-in-one devices			×

Table E-2 Requirements for IT system; Module 4 – Networks

Module 4 - Networks	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 4.1 Heterogeneous networks	S 4.81	Auditing and logging of activities in a network		×	×
S 4.1 Heterogeneous networks	S 4.83	Updating/upgrading of software and hardware in network components			×
S 4.2 Network- and System management	S 2.146	Secure operation of a network management system	×	×	×

Module 4 - Networks	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 4.2 Network- and System management	S 4.92	Secure operation of a system management system	×	×	×
S 4.3 Modem	S 2.60	Secure administration of a modem	×	×	×
S 4.3 Modem	S 3.17	Briefing personnel on modem usage	×	×	×
S 4.3 Modem	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 4.3 Modem	S 5.44	One-way connection setup			×
S 4.4 VPN	S 4.321	Secure operation of a VPN	×	×	×
S 4.5 LAN connection of an IT system via ISDN	S 5.29	Periodic checks of destination addresses and logs			×
S 4.6 WLAN	S 2.388	Appropriate key management for WLAN		×	×
S 4.6 WLAN	S 2.389	Secure use of hotspots			×
S 4.6 WLAN	S 4.293	Secure operation of hotspots			×
S 4.6 WLAN	S 4.296	Use of a suitable management solution for WLAN			×
S 4.6 WLAN	S 4.297	Secure operation of WLAN components	×	×	×
S 4.6 WLAN	S 4.298	Regular audits of WLAN components		×	×
S 4.6 WLAN	S 5.141	Regular security checks of WLANs		×	×
S 4.7 VoIP	S 3.12	Informing all staff members about possible PBX warning notices, warning symbols, and acoustic alarm signals		×	×
S 4.7 VoIP	S 3.13	Increasing staff awareness of potential threats to the PBX		×	×
S 4.7 VoIP	S 4.5	Logging for PBX systems		×	×
S 4.7 VoIP	S 4.6	Audit of the PBX configuration			×
S 4.7 VoIP	S 4.291	Secure configuration of VoIP middleware	×	×	×
S 4.7 VoIP	S 4.292	Logging of VoIP events	×	×	×
S 4.8 Bluetooth	S 2.463	Use of a central pool of Bluetooth peripheral devices			×
S 4.8 Bluetooth	S 4.363	Secure operation of Bluetooth devices	×	×	×

Table E-3 Requirements for IT system; Module 5 – Applications

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.2 Exchange of data media	S 1.36	Safekeeping of data media before and after dispatch	×	×	×
S 5.2 Exchange of data media	S 2.43	Adequate labelling of data media for dispatch	×	×	×
S 5.2 Exchange of data media	S 2.44	Secure packaging of data media	×	×	×

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.2 Exchange of data media	S 3.14	Briefing personnel on correct procedures of exchanging data media		×	×
S 5.2 Exchange of data media	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 5.2 Exchange of data media	S 4.35	Pre-dispatch verification of the data to be transferred			×
S 5.3 Groupware	S 3.76	Basic user training on how to use groupware and e-mail			×
S 5.3 Groupware	S 4.199	Avoiding problematic file formats		×	×
S 5.3 Groupware	S 4.357	Secure operation of groupware systems	×	×	×
S 5.3 Groupware	S 4.358	Logging groupware systems		×	×
S 5.3 Groupware	S 5.54	Dealing with unwanted e-mails		×	×
S 5.3 Groupware	S 5.56	Secure operation of a mail server	×	×	×
S 5.3 Groupware	S 5.108	Cryptographic protection of groupware and/or e-mail			×
S 5.3 Groupware	S 5.109	Use of an e-mail scanner on the mail server			×
S 5.4 Web servers	S 2.174	Secure operation of a web server	×	×	×
S 5.4 Web servers	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 5.4 Web servers	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 5.4 Web servers	S 4.78	Careful modifications of configurations	×	×	×
S 5.4 Web servers	S 4.177	Assuring the integrity and authenticity of software packages		×	×
S 5.4 Web servers	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 5.5 Lotus Notes/Domino	S 4.128	Secure operation of the Lotus Notes/Domino environment	×	×	×
S 5.5 Lotus Notes/Domino	S 4.132	Monitoring the Lotus Notes/Domino environment			×
S 5.5 Lotus Notes/Domino	S 4.426	Archiving for the Lotus Notes/Domino environment			×
S 5.5 Lotus Notes/Domino	S 4.427	Security-relevant logging and evaluating for Lotus Notes/Domino			×
S 5.5 Lotus Notes/Domino	S 4.428	Audit of the Lotus Notes/Domino environment			×
S 5.6 Fax servers	S 5.24	Use of a suitable fax cover sheet			×
S 5.6 Fax servers	S 5.25	Using transmission and reception logs	×	×	×
S 5.6 Fax servers	S 5.26	Announcing fax messages via telephone			×
S 5.6 Fax servers	S 5.27	Acknowledging successful fax reception via telephone			×

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.6 Fax servers	S 5.28	Acknowledging correct fax origin via telephone			×
S 5.6 Fax servers	S 5.73	Secure operation of a fax server	×	×	×
S 5.6 Fax servers	S 5.74	Maintenance of fax server address books and distribution lists	×	×	×
S 5.6 Fax servers	S 5.75	Protecting against overloading the fax server			×
S 5.7 Databases	S 2.31	Documentation of authorised users and rights profiles	×	×	×
S 5.7 Databases	S 2.34	Documentation on changes made to an existing IT system	×	×	×
S 5.7 Databases	S 2.65	Checking the efficiency of user separation on an IT system			×
S 5.7 Databases	S 2.127	Inference prevention		×	×
S 5.7 Databases	S 2.128	Controlling access to a database system	×	×	×
S 5.7 Databases	S 2.129	Controlling access to database information	×	×	×
S 5.7 Databases	S 2.130	Ensuring the integrity of a database	×	×	×
S 5.7 Databases	S 2.131	Separation of administrative tasks for database systems			×
S 5.7 Databases	S 2.133	Checking the log files of a database system	×	×	×
S 5.7 Databases	S 3.18	Log-out obligation for PC users	×	×	×
S 5.7 Databases	S 4.67	Locking and deleting database accounts which are no longer required		×	×
S 5.7 Databases	S 4.68	Ensuring consistent database management	×	×	×
S 5.7 Databases	S 4.69	Regular checks of database security		×	×
S 5.7 Databases	S 4.70	Monitoring a database			×
S 5.7 Databases	S 4.72	Database encryption			×
S 5.7 Databases	S 5.117	Integration of a database server into a security gateway			×
S 5.8 Telecommuting	S 3.21	Training of telecommuters as regards security-related issues	×	×	×
S 5.9 Novell eDirectory	S 4.159	Secure operation of Novell eDirectory	×	×	×
S 5.9 Novell eDirectory	S 4.160	Monitoring of Novell eDirectory		×	×
S 5.9 Novell eDirectory	S 5.97	Protection of communications with Novell eDirectory		×	×
S 5.12 Microsoft Exchange/ Outlook	S 2.482	Regular security checks of Exchange systems		×	×
S 5.12 Microsoft Exchange/ Outlook	S 4.166	Secure operation of Exchange systems	×	×	×

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.13 SAP System	S 2.347	Regular security checks of SAP systems		×	×
S 5.13 SAP System	S 2.348	Security aspects relating to the customisation of SAP systems			×
S 5.13 SAP System	S 2.349	Secure software development for SAP systems			×
S 5.13 SAP System	S 4.270	Logging of SAP events	×	×	×
S 5.13 SAP System	S 4.271	Computer virus protection for SAP systems			×
S 5.13 SAP System	S 4.272	Secure use of the SAP transport system	×	×	×
S 5.13 SAP System	S 4.273	Secure use of the SAP Java Stack software deployment	×	×	×
S 5.14 Mobile data media	S 3.60	Sensitising staff to secure handling of mobile data media and devices			×
S 5.14 Mobile data media	S 4.4	Correct handling of drives for removable media and external data storage			×
S 5.14 Mobile data media	S 4.200	Handling of USB storage media			×
S 5.14 Mobile data media	S 4.232	Secure use of extended memory cards			×
S 5.15 General directory service	S 4.78	Careful modifications of configurations	×	×	×
S 5.15 General directory service	S 4.311	Secure operation of directory services	×	×	×
S 5.15 General directory service	S 4.312	Monitoring directory services		×	×
S 5.15 General directory service	S 5.147	Protection of communications with directory services			×
S 5.16 Active Directory	S 4.138	Configuration of Windows Server as a domain controller	×	×	×
S 5.16 Active Directory	S 4.315	Maintenance of the operational reliability of an Active Directory	×	×	×
S 5.16 Active Directory	S 4.316	Monitoring the Active Directory infrastructure		×	×
S 5.17 Samba	S 4.335	Secure operation of a Samba server		×	×
S 5.18 DNS-Server	S 2.8	Assignment of access rights	×	×	×
S 5.18 DNS-Server	S 2.35	Obtaining information on security weaknesses of the system		×	×
S 5.18 DNS-Server	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 5.18 DNS-Server	S 4.78	Careful modifications of configurations	×	×	×
S 5.18 DNS-Server	S 4.354	Monitoring of a DNS server		×	×
S 5.18 DNS-Server	S 5.118	Integration of a DNS server into a security gateway			×
S 5.19 Internet use	S 2.313	Secure registration with Internet services	×	×	×
S 5.19 Internet use	S 5.45	Secure use of browsers		×	×

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.19 Internet use	S 5.155	Data protection aspects when using the Internet			×
S 5.19 Internet use	S 5.156	Secure use of Twitter			×
S 5.19 Internet use	S 5.157	Secure use of social networks			×
S 5.19 Internet use	S 5.158	Use of web disk space			×
S 5.19 Internet use	S 5.173	Use of short URLs and QR codes			×
S 5.20 OpenLDAP	S 4.390	Secure updating of OpenLDAP			×
S 5.20 OpenLDAP	S 4.391	Secure operation of OpenLDAP		×	×
S 5.20 OpenLDAP	S 4.407	Logging when using OpenLDAP		×	×
S 5.20 OpenLDAP	S 5.170	Secure communication connections when using OpenLDAP			×
S 5.21 Web applications	S 2.8	Assignment of access rights	×	×	×
S 5.21 Web applications	S 2.31	Documentation of authorised users and rights profiles	×	×	×
S 5.21 Web applications	S 2.34	Documentation on changes made to an existing IT system	×	×	×
S 5.21 Web applications	S 2.35	Obtaining information on security weaknesses of the system		×	×
S 5.21 Web applications	S 2.64	Checking the log files	×	×	×
S 5.21 Web applications	S 2.110	Data protection guidelines for logging procedures	×	×	×
S 5.21 Web applications	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 5.21 Web applications	S 3.5	Training on security safeguards	×	×	×
S 5.21 Web applications	S 4.78	Careful modifications of configurations	×	×	×
S 5.21 Web applications	S 4.397	Logging security-relevant events of web applications			×
S 5.21 Web applications	S 5.150	Performing penetration tests			×
S 5.22 Logging	S 2.8	Assignment of access rights	×	×	×
S 5.22 Logging	S 2.64	Checking the log files	×	×	×
S 5.22 Logging	S 2.110	Data protection guidelines for logging procedures	×	×	×
S 5.22 Logging	S 4.225	Use of a logging server on a security gateway			×
S 5.22 Logging	S 4.227	Use of a local NTP server for time synchronisation			×
S 5.22 Logging	S 4.430	Analysing the logged data	×	×	×
S 5.22 Logging	S 4.431	Selecting and processing relevant information for logging	×	×	×
S 5.22 Logging	S 5.9	Logging on the server		×	×

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.22 Logging	S 5.171	Secure communication with a centralised logging server	×	×	×
S 5.22 Logging	S 5.172	Secure time synchronisation for centralised logging	×	×	×

Table E-4 Additional requirements from the 15th revision of the BSI-GS catalogue

Module 3, 4 & 5 – IT Systems (new in 15th rev)	*Safeguard*	*Requirement*	*L*	*M*	*H*
S3.302 Routers and switches	S 2.281	Documentation of the system configuration of routers and switches	×	×	×
S 3.302 Routers and switches	S 2.282	Regular checking of routers and switches	×	×	×
S 3.302 Routers and switches	S 2.283	Software maintenance on routers and switches		×	×
S 3.302 Routers and switches	S 4.204	Secure administration of routers and switches			×
S 3.302 Routers and switches	S 4.205	Logging on routers and switches			×
S 3.302 Routers and switches	S 4.206	Protection of switch ports			×
S 3.302 Routers and switches	S 5.112	Security aspects of routing protocols			×
S 3.303 Storage systems and storage networks	S 2.527	Secure deletion in SAN environments		×	×
S 3.303 Storage systems and storage networks	S 4.447	Ensuring the integrity of the SAN fabric			×
S 3.404 Virtualisation	S 2.558	Staff awareness on information security concerning mobile phones, smartphones, tablets and PDAs	×	×	×
S 3.405 PDA	S 2.558	Staff awareness on information security concerning mobile phones, smartphones, tablets and PDAs	×	×	×
S 3.405 PDA	S 4.466	Use of anti-virus programs for smartphones, tablets and PADs			×
S 3.405 PDA	S 4.469	Defense against infiltrated GSM codes on end devices with phone function	×	×	×
S 3.405 PDA	S 5.173	Use of URL shortening services and QR codes			×
S 3.405 PDA	S 5.176	Secure connection of smartphones, tablets and PDAs to the corporate network		×	×
S 3.407 Embedded systems	S 1.81	Physical protection of embedded systems	×	×	×
S 3.407 Embedded systems	S 2.34	Documentation of changes to an existing system	×	×	×
S 3.407 Embedded systems	S 2.565	Logging security events in embedded systems	×	×	×
S 3.407 Embedded systems	S 4.78	Careful implementation of configuration changes	×	×	×
S 3.407 Embedded systems	S 4.177	Ensuring integrity and authenticity of software packages		×	×
S 3.407 Embedded systems	S 4.490	Built-in self test (BIST) of embedded system modules	×	×	×

Module 3, 4 & 5 – IT Systems (new in 15th rev)	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 3.407 Embedded systems	S 4.491	Preventing debugging capabilities in embedded systems	×	×	×
S 3.407 Embedded systems	S 4.492	Secure configuration and use of embedded web servers		×	×
S 4.1 Heterogeneous networks	S 2.578	Installation, configuration and support of local networks by third parties			×
S 4.1 Heterogeneous networks	S 2.579	Regular audits of local networks		×	×
S 4.2 Network- and System management	S 3.11	Training of maintenance and administrative staff	×	×	×
S 4.2 Network- and System management	S 4.81	Audit and logging of activities in the network		×	×
S 5.19 Internet use	S 3.78	Correct behaviour on the Internet and social networks			×
S 5.22 Logging	S 5.172	Secure time synchronisation for centralised logging	×	×	×
S 5.23 Cloud Management	S 2.518	Use of a highly-available firewall-solution			×
S 5.23 Cloud Management	S 2.519	Controlled administration of users and permissions in cloud computing	×	×	×
S 5.23 Cloud Management	S 2.520	Safe and complete deletion of user data in the cloud			×
S 5.23 Cloud Management	S 2.521	Controlled provisioning and de-provisioning of cloud services	×	×	×
S 5.23 Cloud Management	S 2.522	Reporting system and communication to cloud users		×	×
S 5.23 Cloud Management	S 2.523	Safe automation in cloud administrative processes			×
S 5.23 Cloud Management	S 4.430	Analysis of log data	×	×	×
S 5.23 Cloud Management	S 4.442	Central protection of malware in the cloud infrastructure			×
S 5.23 Cloud Management	S 4.443	Logging and monitoring of events in the cloud infrastructure		×	×
S 5.23 Cloud Management	S 4.444	Patch management for cloud components	×	×	×
S 5.23 Cloud Management	S 4.445	Comprehensive segregation of cloud service users	×	×	×
S 5.23 Cloud Management	S 5.71	Intrusion Detection and Intrusion Response systems			×
S 5.24 Web services	S 2.8	Allocation of access rights	×	×	×
S 5.24 Web services	S 2.31	Documentation of registered users and access profiles	×	×	×
S 5.24 Web services	S 2.34	Documentation of changes on existing systems	×	×	×

Module 3, 4 & 5 – IT Systems (new in 15th rev)	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.24 Web services	S 2.35	Obtaining information on security gaps in the system		×	×
S 5.24 Web services	S 2.64	Checking of log information	×	×	×
S 5.24 Web services	S 2.110	Data privacy protection during log writing	×	×	×
S 5.24 Web services	S 2.273	Timely application of security related patches and updates	×	×	×
S 5.24 Web services	S 3.5	Education on security measures	×	×	×
S 5.24 Web services	S 4.78	Careful implementation of configuration changes	×	×	×
S 5.24 Web services	S 4.397	Logging of security related events of web applications and services			×
S 5.24 Web services	S 4.452	Monitoring of web services	×	×	×
S 5.24 Web services	S 5.150	Execution of penetration tests			×
S 5.25 General applications	S 3.4	Training before using a system	×	×	×
S 5.25 General applications	S 4.464	Maintaining security during operation		×	×
S 5.26 Service oriented architecture	S 3.5	Education on security measures	×	×	×
S 5.26 Service oriented architecture	S 4.476	Protection of a WS-Notification-Subscription in Broker		×	×
S 5.26 Service oriented architecture	S 4.477	Protection of a WS-Notification		×	×
S 5.26 Service oriented architecture	S 4.478	Key management for SOA			×
S 5.26 Service oriented architecture	S 4.479	Protection of regulations in a SOA		×	×
S 5.26 Service oriented architecture	S 4.480	Protection of WS-resources in a SOA-environment			×
S 5.26 Service oriented architecture	S 4.481	Safe usage of connectionless SOAP-communication			×
S 5.26 Service oriented architecture	S 5.147	Protection of communication with the directory service			×
S 5.26 Service oriented architecture	S 5.150	Execution of penetration tests			×
S 5.27 Software development	S 2.273	Timely application of security-related patches and updates	×	×	×
S 5.27 Software development	S 2.575	Regular security audits of the software development environment			×
S 5.27 Software development	S 4.33	Usage of anti-viros software during media exchange and transmission	×	×	×

Module 3, 4 & 5 – IT Systems (new in 15th rev)	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.27 Software development	S 4.78	Careful implementation of configuration changes			×
S 5.27 Software development	S 4.93	Regular integrity check			×
S 5.27 Software development	S 4.496	Safe installation of the developed software			×

APPENDIX F DNV GL PROFILING OF IEC 62443-3-3 FOUNDATIONAL REQUIREMENTS FOR OT SYSTEMS

The IEC-62443 standard on Industrial communication networks – Network and system security provides a good foundation for cyber security towards industrial control systems. Requirements address components, systems, policies & procedures and more generic requirements addressing concepts, models metrics, and life-cycles. This RP references the security requirements (SR, #requirement reference) proposed in IEC 62443-3-3 helping the reader in determining which of the security requirements apply based on the risk level resulting from the assessment in [2.3.4] (L = low, M = medium or H = high).

Table F-1 shall be used for all cases and Table F-2 to Table F-5 shall be used for the respective CIAA rating of each system's CIAA criteria.

Table F-1 Recommendations for timely responses to events

CIAA	*Timely response to events*	*L*	*M*	*H*
SR 6.1	Audit log accessibility	×	×	×
SR 6.1 RE 1	Programmatic access to audit logs			×
SR 6.2	Continuous monitoring		×	×

Table F-2 Requirements for Confidentiality in OT system

Confidentiality	*Data confidentiality*	*L*	*M*	*H*
SR 4.1	Information confidentiality	×	×	×
SR 4.1 RE 1	Protection of confidentiality at rest or in transit via untrusted networks		×	×
SR 4.2	Information persistence		×	×
SR 4.2 RE 1	Purging of shared memory resources			×
SR 4.3	Use of cryptography	×	×	×

Table F-3 Requirements for Integrity in OT system

Integrity	*System integrity*	*L*	*M*	*H*
SR 3.1	Communication integrity	×	×	×
SR 3.2	Malicious code protection	×	×	×
SR 3.2 RE 1	Malicious code protection on entry and exit points		×	×
SR 3.2 RE 2	Central management and reporting for malicious code protection			×
SR 3.3	Security functionality verification	×	×	×
SR 3.4	Software and information integrity	×	×	×
SR 3.5	Input validation	×	×	×
SR 3.6	Deterministic output	×	×	×
SR 3.7	Error handling		×	×
SR 3.8	Session integrity		×	×
SR 3.9	Protection of audit information		×	×

Table F-4 Requirements for Availability in OT system

Availability	*Restricted data flow and timely response to events and resource availability*	*L*	*M*	*H*
SR 5.1	Network segmentation	×	×	×
SR 5.1 RE 1	Physical network segmentation	×	×	×
SR 5.1 RE 2	Independence from non-control system networks	×	×	×
SR 5.1 RE 3	Logical and physical isolation of critical networks	×	×	×
SR 5.2	Zone boundary protection	×	×	×
SR 5.2 RE 1	Deny by default, allow by exception		×	×
SR 5.2 RE 2	Island mode			×
SR 5.3	General purpose person-to-person communication restrictions	×	×	×
SR 5.3 RE 1	Prohibit all general purpose person-to-person communications	×	×	×
SR 5.4	Application partitioning	×	×	×
SR 7.1	Denial of service protection	×	×	×
SR 7.1 RE 1	Manage communication loads		×	×
SR 7.1 RE 2	Limit DoS effects to other systems or networks			×
SR 7.2	Resource management	×	×	×
SR 7.3	Control system back-up	×	×	×
SR 7.3 RE 1	Backup verification		×	×
SR 7.3 RE 2	Backup automation			×
SR 7.4	Control system recovery and reconstitution	×	×	×
SR 7.5	Emergency power		×	×
SR 7.6	Network and security configuration	×	×	×
SR 7.6 RE 1	Machine-readable reporting of current security settings			×
SR 7.7	Least functionality	×	×	×
SR 7.8	Control system component inventory		×	×

Table F-5 Requirements for Authenticity in OT system

Authenticity	*Identification and authentication control and use control*	*L*	*M*	*H*
SR 1.1	Human user identification and authentication	×	×	×
SR 1.1 RE 1	Unique identification and authentication			×
SR 1.2	Software process and device identification and authentication		×	×
SR 1.3	Account management	×	×	×
SR 1.4	Identifier management	×	×	×

Authenticity	*Identification and authentication control and use control*	*L*	*M*	*H*
SR 1.5	Authenticator management	×	×	×
SR 1.6	Wireless access management	×	×	×
SR 1.6 RE 1	Unique identification and authentication		×	×
SR 1.7	Strength of password-based authentication	×	×	×
SR 1.7 RE 1	Password generation and lifetime restrictions for human users			×
SR 1.8	Public key infrastructure certificates		×	×
SR 1.9	Strength of public key authentication		×	×
SR 1.10	Authenticator feedback	×	×	×
SR 1.13	Access via untrusted networks	×	×	×
SR 1.13 RE 1	Explicit access request approval		×	×
SR 2.1	Authorization enforcement	×	×	×
SR 2.1 RE 1	Authorization enforcement for all users		×	×
SR 2.1 RE 2	Permission mapping to roles		×	×
SR 2.1 RE 3	Supervisor override			×
SR 2.2	Wireless use control	×	×	×
SR 2.2 RE 1	Identity and report unauthorized wireless devices			×
SR 2.3	Use control for portable and mobile devices	×	×	×
SR 2.3 RE 1	Enforcement of security status of portable and mobile devices			×
SR 2.4	Mobile code	×	×	×
SR 2.4 RE 1	Mobile code integrity check			×
SR 2.6	Remote session termination		×	×
SR 2.7	Concurrent session control			×
SR 2.8	Auditable events	×	×	×
SR 2.8 RE 1	Centrally managed, system-wide audit trail			×
SR 2.9	Audit storage capacity	×	×	×
SR 2.9 RE 1	Warn when audit record storage capacity threshold reached			×
SR 2.10	Response to audit processing failures	×	×	×
SR 2.11	Timestamp	×	×	×
SR 2.11 RE 1	Internal time synchronization	×	×	×

APPENDIX G BSI GS REQUIREMENTS FOR COMMON ASPECTS AND INFRASTRUCTURE

These tables demonstrate requirements aligned with the BSI GS cyber security requirements which apply for common aspects and infrastructure. A case-by-case assessment needs to be performed for each individual vessel in order to determine which requirements are applicable.

Table G-1 Requirements for IT system; Module 1 – Common aspects

Module 1 – Common aspects	*Safeguard*	*Requirement*
S 1.0 Security management	S 2.199	Maintaining information security
S 1.0 Security management	S 2.200	Management reports on information security
S 1.0 Security management	S 2.201	Documentation of the security process
S 1.1 Organisation	S 2.6	Granting of site access authorisations
S 1.1 Organisation	S 2.7	Granting of (system/network) access authorisations
S 1.1 Organisation	S 2.8	Assignment of access rights
S 1.1 Organisation	S 2.16	Supervising or escorting outside staff/visitors
S 1.1 Organisation	S 2.18	Inspection rounds
S 1.1 Organisation	S 2.37	Clean desk policy
S 1.1 Organisation	S 2.39	Response to violations of security policies
S 1.1 Organisation	S 2.177	Security during relocation
S 1.1 Organisation	S 5.33	Secure remote maintenance
S 1.2 Personnel	S 3.3	Arrangements for substitution
S 1.2 Personnel	S 3.4	Training before actual use of a program
S 1.2 Personnel	S 3.5	Training on security safeguards
S 1.2 Personnel	S 3.7	Point of contact in case of personal problems
S 1.2 Personnel	S 3.8	Avoidance of factors impairing the organisation climate
S 1.2 Personnel	S 3.11	Training of maintenance and administration staff
S 1.3 Business continuity management	S 6.117	Tests and emergency drills
S 1.3 Business continuity management	S 6.118	Checking and maintaining the emergency measures
S 1.3 Business continuity management	S 6.119	Documentation in the business continuity management process
S 1.3 Business continuity management	S 6.120	Checking and controlling the business continuity management process
S 1.4 Data backup policy	S 6.20	Appropriate storage of backup data media
S 1.4 Data backup policy	S 6.22	Sporadic checks of the restorability of backups
S 1.5 Data protection	S 2.110	Data protection guidelines for logging procedures

Module 1 – Common aspects	*Safeguard*	*Requirement*
S 1.5 Data protection	S 2.513	Documentation of admissibility regarding data protection
S 1.5 Data protection	S 2.514	Maintenance of data protection during operation
S 1.5 Data protection	S 2.515	Deletion/destruction in compliance with data protection
S 1.6 Protection against malware	S 2.34	Documentation on changes made to an existing IT system
S 1.6 Protection against malware	S 2.158	Reporting infections of malware,
S 1.6 Protection against malware	S 2.159	Updating the virus protection programs and signatures
S 1.6 Protection against malware	S 2.224	Prevention against malware
S 1.6 Protection against malware	S 4.3	Use of virus protection programs
S 1.8 Handling security incidents	S 6.64	Remedial action in connection with security incidents
S 1.8 Handling security incidents	S 6.65	Notification of parties affected by security incidents
S 1.8 Handling security incidents	S 6.66	Evaluation of security incidents
S 1.8 Handling security incidents	S 6.68	Testing the effectiveness of the management system for the handling of security incidents
S 1.8 Handling security incidents	S 6.130	Detection and documentation of security incidents
S 1.8 Handling security incidents	S 6.131	Classifying and assessing security incidents
S 1.8 Handling security incidents	S 6.132	Limiting the effects of security incidents
S 1.8 Handling security incidents	S 6.133	Recovering the operating environment after security incidents
S 1.8 Handling security incidents	S 6.134	Documentation of security incidents
S 1.9 Hardware and software management	S 1.46	Use of anti-theft devices
S 1.9 Hardware and software management	S 2.10	Audit of the hardware and software inventory
S 1.9 Hardware and software management	S 2.22	Escrow of passwords
S 1.9 Hardware and software management	S 2.31	Documentation of authorised users and rights profiles

Module 1 – Common aspects	*Safeguard*	*Requirement*
S 1.9 Hardware and software management	S 2.34	Documentation on changes made to an existing IT system
S 1.9 Hardware and software management	S 2.35	Obtaining information on security weaknesses of the system
S 1.9 Hardware and software management	S 2.64	Checking the log files
S 1.9 Hardware and software management	S 2.65	Checking the efficiency of user separation on an IT system
S 1.9 Hardware and software management	S 2.110	Data protection guidelines for logging procedures
S 1.9 Hardware and software management	S 2.215	Error handling
S 1.9 Hardware and software management	S 2.219	Continuous documentation of information processing
S 1.9 Hardware and software management	S 2.273	Prompt installation of security-relevant patches and updates
S 1.9 Hardware and software management	S 2.402	Resetting passwords
S 1.9 Hardware and software management	S 4.78	Careful modifications of configurations
S 1.9 Hardware and software management	S 4.107	Use of the vendor resources
S 1.9 Hardware and software management	S 4.109	Software reinstallation on workstations
S 1.9 Hardware and software management	S 4.254	Secure usage of wireless keyboards and mice
S 1.9 Hardware and software management	S 4.306	Handling of password storage tools
S 1.9 Hardware and software management	S 4.345	Protection against undesired outflows of information
S 1.9 Hardware and software management	S 5.150	Performing penetration tests
S 1.10 Standard software	S 2.88	Licence management and version control for standard software
S 1.11 Outsourcing	S 2.256	Planning and maintenance of IT security during ongoing outsourcing operations
S 1.12 Archiving	S 1.60	Appropriate storage of archiving media
S 1.12 Archiving	S 2.257	Monitoring of the memory resources of archiving media
S 1.12 Archiving	S 2.258	Consistent indexing of documents during archiving
S 1.12 Archiving	S 2.260	Regular auditing of the archiving procedure
S 1.12 Archiving	S 2.261	Regular market surveys of archive systems

Module 1 – Common aspects	*Safeguard*	*Requirement*
S 1.12 Archiving	S 2.263	Regular regeneration of archived data resources
S 1.12 Archiving	S 2.264	Regular regeneration of encrypted data in archiving
S 1.12 Archiving	S 4.171	Protection of the integrity of the archive system index database
S 1.12 Archiving	S 4.172	Logging of the archival accesses
S 1.12 Archiving	S 4.173	Regular function and recovery tests for archiving
S 1.13 Information security awareness and training	S 2.198	Making staff aware of information security issues
S 1.13 Information security awareness and training	S 3.4	Training before actual use of a program
S 1.13 Information security awareness and training	S 3.5	Training on security safeguards
S 1.13 Information security awareness and training	S 3.11	Training of maintenance and administration staff
S 1.13 Information security awareness and training	S 3.26	Instructing staff members in the secure handling of IT
S 1.13 Information security awareness and training	S 3.47	Performing simulations on information security
S 1.14 Patch and change management	S 2.219	Continuous documentation of information processing
S 1.14 Patch and change management	S 2.426	Integration of patch and change management into the business processes
S 1.14 Patch and change management	S 2.427	Co-ordination of change requests
S 1.14 Patch and change management	S 2.428	Scalability in patch and change management
S 1.14 Patch and change management	S 2.429	Measuring the success of change requests
S 1.14 Patch and change management	S 4.78	Careful modifications of configurations
S 1.14 Patch and change management	S 4.177	Assuring the integrity and authenticity of software packages
S 1.14 Patch and change management	S 4.323	Synchronisation within patch and change management
S 1.14 Patch and change management	S 4.324	Configuration of auto-update mechanisms in patch and change management
S 1.15 Deleting and destroying data	S 2.217	Careful classification and handling of information, applications and systems
S 1.16 Compliance management	S 2.199	Maintaining information security

Module 1 – Common aspects	*Safeguard*	*Requirement*
S 1.16 Compliance management	S 2.217	Careful classification and handling of information, applications and systems
S 1.16 Compliance management	S 2.340	Consideration of legal framework conditions
S 1.16 Compliance management	S 2.380	Granting exceptions
S 1.16 Compliance management	S 3.26	Instructing staff members in the secure handling of IT

Table G-2 Requirements for IT system; Module 2 – Infrastructure

Module 2 - Infrastructure	*Safeguard*	*Requirement*
S 2.1 General vessel	S 1.15	Closed windows and doors
S 2.1 General vessel	S 1.23	Locked doors
S 2.1 General vessel	S 2.14	Key management
S 2.1 General vessel	S 2.15	Fire safety inspection
S 2.1 General vessel	S 2.391	Timely provision of information to the fire safety engineer
S 2.2 Electrical Cabling	S 2.391	Timely provision of information to the fire safety engineer
S 2.2 Electrical Cabling	S 2.394	Inspection of electrical equipment
S 2.3 Office/local workplace	S 1.15	Closed windows and doors
S 2.3 Office/local workplace	S 1.23	Locked doors
S 2.3 Office/local workplace	S 1.45	Suitable storage of official documents and data media
S 2.3 Office/local workplace	S 1.46	Use of anti-theft devices
S 2.3 Office/local workplace	S 2.37	Clean desk policy
S 2.4 Server room	S 1.15	Closed windows and doors
S 2.4 Server room	S 1.23	Locked doors
S 2.5 Data media archives	S 1.15	Closed windows and doors
S 2.5 Data media archives	S 1.23	Locked doors
S 2.6 Technical infrastructure room	S 1.15	Closed windows and doors
S 2.6 Technical infrastructure room	S 1.23	Locked doors
S 2.7 Protective cabinets	S 1.15	Closed windows and doors
S 2.7 Protective cabinets	S 2.96	Locking of protective cabinets
S 2.7 Protective cabinets	S 2.97	Correct procedure for code locks
S 2.8 Home workplace	S 1.15	Closed windows and doors
S 2.8 Home workplace	S 1.23	Locked doors

Module 2 - Infrastructure	*Safeguard*	*Requirement*
S 2.8 Home workplace	S 2.37	Clean desk policy
S 2.9 Computer centre	S 1.15	Closed windows and doors
S 2.9 Computer centre	S 1.23	Locked doors
S 2.9 Computer centre	S 1.71	Function tests of the technical infrastructure
S 2.9 Computer centre	S 1.72	Construction projects during ongoing operations
S 2.9 Computer centre	S 1.73	Protecting a computer centre from unauthorised entry
S 2.10 Mobile workplace	S 1.15	Closed windows and doors
S 2.10 Mobile workplace	S 1.23	Locked doors
S 2.10 Mobile workplace	S 1.46	Use of anti-theft devices
S 2.10 Mobile workplace	S 2.37	Clean desk policy
S 2.10 Mobile workplace	S 2.389	Secure use of hotspots
S 2.10 Mobile workplace	S 4.251	Working with external IT systems
S 2.11 Meeting, event, and training rooms	S 1.15	Closed windows and doors
S 2.11 Meeting, event, and training rooms	S 2.16	Supervising or escorting outside staff/visitors
S 2.11 Meeting, event, and training rooms	S 4.109	Software reinstallation on workstations
S 2.11 Meeting, event, and training rooms	S 4.293	Secure operation of hotspots
S 2.12 IT-Cabling	S 1.39	Prevention of transient currents on shielding
S 2.12 IT-Cabling	S 2.20	Monitoring of existing connections
S 2.12 IT-Cabling	S 5.143	Ongoing update and review of network documentation

APPENDIX H CYBER SECURITY MANAGEMENT VERIFICATION

Mandatory documents and records as well as non-mandatory documents referenced in [4.2] are listed and a reference to the corresponding part of ISO-27001 ref. /7/ is provided in the tables below.

Table H-1 Mandatory documents

Mandatory documents	*Check*
Scope of the ISMS (clause 4.3)	
Information security policy and objectives (clauses 5.2 and 6.2)	
Risk assessment and risk treatment methodology (clause 6.1.2)	
Statement of Applicability (clause 6.1.3 d)	
Risk treatment plan (clauses 6.1.3 e and 6.2)	
Risk assessment report (clause 8.2)	
Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)	
Inventory of assets (clause A.8.1.1)	
Acceptable use of assets (clause A.8.1.3)	
Access control policy (clause A.9.1.1)	
Operating procedures for IT/OT management (clause A.12.1.1)	
Secure system engineering principles (clause A.14.2.5)	
Supplier security policy (clause A.15.1.1)	
Incident management procedure (clause A.16.1.5)	
Business continuity procedures (clause A.17.1.2)	
Statutory, regulatory, and contractual requirements (clause A.18.1.1)	

Table H-2 Mandatory records

Mandatory records	*Check*
Records of training, skills, experience and qualifications (clause 7.2)	
Monitoring and measurement results (clause 9.1)	
Internal audit program (clause 9.2)	
Results of internal audits (clause 9.2)	
Results of the management review (clause 9.3)	
Results of corrective actions (clause 10.1)	
Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)	

Table H-3 Non-mandatory documents

Non-mandatory documents	*Check*
Procedure for document control (clause 7.5)	
Controls for managing records (clause 7.5)	
Procedure for internal audit (clause 9.2)	
Procedure for corrective action (clause 10.1)	
Bring your own device (BYOD) policy (clause A.6.2.1)	
Mobile device and teleworking policy (clause A.6.2.1)	
Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)	
Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)	
Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)	
Procedures for working in secure areas (clause A.11.1.5)	
Clear desk and clear screen policy (clause A.11.2.9)	
Change management policy (clauses A.12.1.2 and A.14.2.4)	
Backup policy (clause A.12.3.1)	
Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)	
Business impact analysis (clause A.17.1.1)	
Exercising and testing plan (clause A.17.1.3)	
Maintenance and review plan (clause A.17.1.3)	
Business continuity strategy (clause A.17.2.1)	

APPENDIX I SOFTWARE CONFIGURATION MANAGEMENT

Tracking of software changes should be included in a management of change process. Table I-1 contains the recommended fields to be used in the change tracking form. It is recommended to use such a tracking mechanism and reference the tracking information within the configuration management process. Further guidance can also be found ISDS-CM requirements ref. /27/.

Table I-1 Software change tracking template

Software change request #	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*…*
Major/Minor								
Vendor tracking number								
Date change made								
System SFI* or GMOD** code								
System name								
System tag number								
Description of change								
Previous software version								
New software version								
Vessel name								
Sister vessel name								
More sister vessel names […]								
Date software change was tested								
Date software change was closed								
Impacts of other systems/Tests needing to be performed								
Reference to any other issue tracking system #								

(*) The SFI Group is classification system for the maritime and offshore industry worldwide. It is an international standard, which provides a functional subdivision of technical and financial ship or rig information covering all aspects of ship/rig specification. SFI code can be used for all systems in the shipping/offshore industry.

(**) GMOD is a generic product model defined by DNV GL. It contains a hierarchy of ship functions and library of ship components. GMOD was originally used to support class activities, but is also suitable for any application requiring identification and referencing to shipboard systems. For more information, see http://data.dnvgl.com/dnvgl-vis/.

Software patch management

One of the most common vulnerabilities is unpatched software and attackers are quick to get the upper hand when software patches are not kept up to date. Software patches for OT & IT support should therefore be managed by a defined process that includes:

— regular examination for new vulnerability alert messages from the OT and third-party software system suppliers and CERTs[2] such as the vulnerability analysis knowledge base on www.cert.org
— assessing the criticality of patches

[2] CERTs: Computer emergency response teams (expert groups that handle computer security incidents)

— obtaining the patches and updates
— backing-up the system for restoration in case something goes wrong. This is particularly important when the OT system is required for production
— testing the patches prior to installing them (if possible first on a redundant system) and checking if a restart is required. It is particularly important to have a plan for the restart of OT systems needed for production
— approval process (vessel owner and the product supplier contractual agreement for periods of time for the approval and provision of patches and updates or alternative workarounds for vulnerabilities)
— handling product supplier approvals of patches and
— handling the patching of additional software.

Ideally the patches can be scheduled during maintenance Windows. If however the OT systems have redundant systems then the patch updates can be done sooner [BSI-ICS Security Compendium Version 1.23, §5.6.4 Patch management].

Software register

Additionally to software change tracking, it is recommended to create and maintain a software register. This register should be linked and referenced in the software change management process and kept up to date following patches, updates and fixes. Table I-2 proposes useful fields that should be tracked for each software dependent system.

Table I-2 Software register template

Software register	*SW #1*	*SW #2*	*SW #3*	*SW #4*	*SW #5*	*SW …*
Vendor name						
CPU/RCU/SBC/device manufacturer						
The firmware						
Model no of CPU/RCU/SBC/device						
Hardware version of CPU/RCU/SBC/device						
System that software is backed up from						
TAG No of cabinet where software is installed						
Description of state of software (pre-FAT, FAT, pre-commissioning, commissioning, release)						
Software description (name of software application, could be the software developed by the vendor for the control of equipment such as PLC code, vessel management system application software, web client, HMIs, etc.)						
Patches applied to the software (could be contained within the version identifier)						
Configuration files*						
Software revision						
Date of software revision						
Type of software (source, executable, other)						
Final location of software backup						
I/O or signal lists, and its version						

Software register	*SW #1*	*SW #2*	*SW #3*	*SW #4*	*SW #5*	*SW …*
Cause and effects information and it's version						
Operating systems and their versions/patches						

*Configuration files: Security mechanism parameters are particularly important. The following should be considered:

— default configuration
— activation/deactivation of unsecure services
— replacing of passwords, certificates for all services
— required authorisations for configuration changes.

APPENDIX J FORENSICS

Incident logging

Logs of security events need to be continuously monitored to deter malicious attacks and to detect attacks, to be conserved for forensics after security compromise [IEC 62443-3 §7.3.4, §8.6.3]. Potentially critical actions such as configuration changes, failed logins, unusual connections, removal or replacement of CF cards or connection of an unknown device on the ship network are all potentially critical actions that should be recorded in log files.

Evidence collection preparations

It is recommended for first responders performing forensics analysis to have a ready prepared flow chart that would guide the seizure of the information in different possible cases.

The excerpt in Figure J-1 gives an idea of the types of a forensics activity from the flow chart by Lance Mueller[3], ref. /28/.

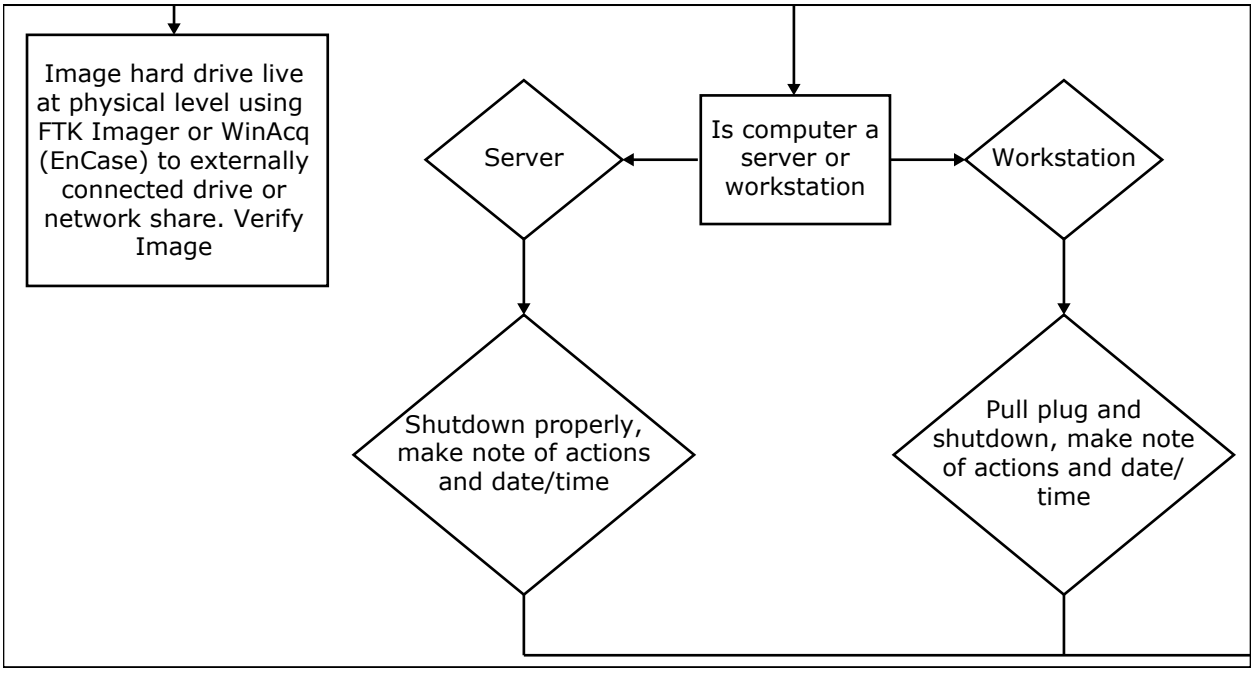

Figure J-1 Example steps of a flow chart on e-evidence gathering

[3] Mueller, L.,'Computer Forensic Hard Drive Imaging Process Tree with Volatile Data Collection', 11 December 2010. http://www.forensickb.com/2010/12/computer-forensic-hard-drive-imaging_11.html [last accessed 11 November 2014]

APPENDIX K IT/OT NETWORK TOPOLOGY

The diagram in Figure K-1 is an example of a network topology diagram for a LNG vessel, where segregation principles are applied using zoning.

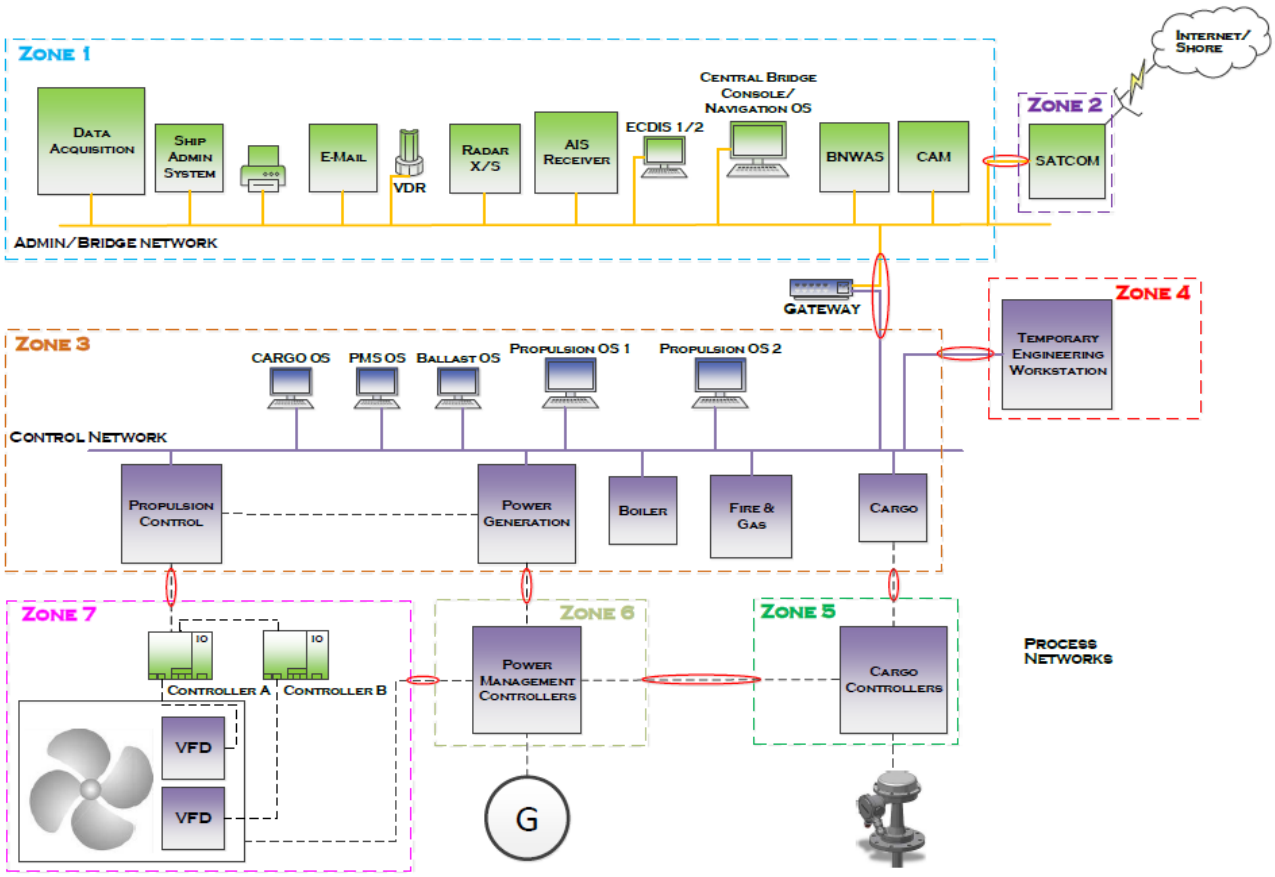

Figure K-1 Network topology example for an LNG carrier

APPENDIX L VESSEL REMOTE ACCESS/CONNECTIVITY

IT or OT support personnel will often need remote maintenance access to quickly provide assistance to users without having to physically go to the user location (i.e. on board). For security reasons, it makes sense to restrict using external personnel for remote maintenance. Additional safeguards shall provide the following security functions:

— A permit to work system like the one in use for hot work on board would add a good measure of security.
— The connection for remote maintenance should always be initiated by the local IT or OT system. This can be accomplished by having the target systems call the remote maintenance location or by using an automatic call-back function.
— The user of the system shall explicitly consent to the remote access, for example by entering a corresponding confirmation on the system. The user should monitor all activities during remote access.
— The external maintenance personnel shall authenticate when beginning the maintenance session. Passwords should never be transmitted in unencrypted form. If systems cannot provide encryption, tunnelling traffic through an encrypting virtual private network (VPN) should be mandatory.
— To the extent possible, remote access credentials shall be personal, not shared (e.g. by a vendor's technical support team). If this is not possible, one-time passwords should be used and reset after the session ended.
— Remote maintenance shall be logged. Logging information should at least contain the start and end time and persons involved during the remote maintenance. If the remote maintenance cannot be monitored by the use then all performing remote maintenance activities shall be logged on the target system.

Furthermore, additional functions can be implemented on the IT or OT system to be maintained:

— Activation of a lock-out period in the event of failed access attempts.
— Blocking of the remote maintenance feature during normal operation and express approval for a precisely defined period of time.
— Maintenance personnel should not be granted full administrator rights and should only have access to the data and directories requiring maintenance; graduated administration of rights shall be implemented.
— When possible, maintenance personnel should have a user ID for performing all maintenance work that is separate from their regular, non-privileged user ID.
— If the connection to the remote maintenance location is disrupted for some reason, access to the system shall be terminated by an automatic logout function.

Remote maintenance by 3rd parties

— When 3rd parities, such as manufacturer's support personnel, perform remote maintenance, additional safeguards are required.
— The remote maintenance personnel shall authenticate themselves and the data transmitted shall be encrypted. For example, the connection can be implemented via VPN or it is also possible to use dedicated connections (see VPN encryption methods) below.
— If technically feasible, all activities during third party administration should be monitored by in-house IT or OT experts. For example, a graphical user interface can be used to display and record all input and output regarding the system to be maintained while a client is remotely administered. The maintenance personnel should not be left unattended, even if third party remote maintenance is necessary because the know-how or capacity required are not available internally. If there is any uncertainty regarding the processes, the local IT expert should ask immediately. It shall be possible at all times to cancel remote maintenance locally.
— If data or programs are created on the local system while performing maintenance, this should only be performed in specifically indicated directories or using certain user IDs.
— Non-disclosure agreements (NDAs) relating to data secrecy shall be included in the contract concluded with the external maintenance personnel. It is especially important to specify that data stored externally in the context of maintenance shall be deleted carefully after completing the maintenance work. Likewise, the duties and qualifications of the external maintenance personnel shall be clearly defined.

VPN encryption methods

Sensitive information during transmission over insecure networks are exposed to many dangers, especially if an improper encryption method is used which can result in static cryptographic keys and pre-shared key (PSK) being made vulnerable to attacks by cryptanalysis. Furthermore, the choice of PSKs can have an impact on safety, for example when intercepted and used in brute force attacks. The use of static cryptographic keys poses security drawbacks. As the keys often remain unchanged for long periods of time, large amounts of data are encrypted with the same key thus facilitating the work of a cryptanalysis while significantly increasing the value of their results. Using a single PSK for the entire VPN infrastructure will result in a significant deterioration of the security.

CHANGES – HISTORIC

There are currently no historical changes for this document.

DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16 000 professionals are dedicated to helping our customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER