VHT
Verein Hanseatischer
Transportversicherer e.V.

IT-Grundschutz Profile for Shipping Companies

Minimum Protection for Ship Operations

Bremen, 24/01/2020

1. Change History

Version	Date	Name	Description
0.1		BSI	Preparation of Working Draft
0.2		BSI, VHT, afEfa Verwaltungsgesellschaft mbH	Summary of findings from the workshops
1.0	16/01/2020	VHT	Finalisation

2. Table of Contents

3. Preface

“Cyber security does not start at the end of the pier, nor does it suddenly stop there”. This is introductory sentence I use to greet the participants attending our IT-Grundschutz workshops. Right from the start, the focus is placed on ways to minimise cyber risks.

We started the series of "Ship Operations" workshops immediately after completing the "Land Operations" series in January 2019. As an innovation, aside from shipping companies and ship management companies, we invited OEMs (Original Equipment Manufacturer) who are responsible for the technical equipment onboard ships and their (cyber) security, along with other maritime service providers. The idea was to obtain the best possible intersection between ‘human’, ‘technology’ and ‘process’. The IT-Grundschutz profile "Ship Operation" represents a process.

It is the crew members who share the ship with other seafarers from other countries and cultures as a workplace and living space for several weeks or months. Each of them has a different view of cyber security. The prevention of cyber threats on board so that they can be transferred and experienced in day-to-day operations represents a process. It is not a one-off task and is certainly not an easy one. The Grundschutz profile is designed to act as an initial aid here, as a framework. Each shipping company can build individually on this Grundschutz profile in line with their respective needs and budgets.

We are extremely pleased that both maritime service providers and various research institutes have also contributed to the development of the IT-Grundschutz profile for "Ship Operations" in addition to shipping companies, and brought their valuable expertise to the table.

I have a particular memory of working out the ‘Nautical’, ‘Machine’, ’Cargo’ and ‘Communication’ business processes, which we developed with great enthusiasm and with the involvement of the participants in mid-June 2019 on the premises of the Federal Ministry of Economics in Bonn.

Processes need to be identified, described, installed, experienced and constantly developed. This sentence is easy to put down on paper. However, the sample processes were queried, changed and simplified several times during the workshops and in the expert groups. For the implementation of an ISMS (Information Security Management System), the workshops, under the direction of the BSI, undertook the preparatory work of mapping a sample shipping company. The further elaboration and finely detailed work are now in your hands.

In my opinion, cyber security only works if the ‘human-process-technology’ component is in a balanced equilibrium. Simply placing your blind trust in technology is not to be advised.

The IT-Grundschutz profile "Ship Operation" has created an opportunity to identify the operational processes and taking appropriate precautions. As an interested and competent party, it places a gratis tool in your hands than can be implemented and which you can put to work immediately. The tool grows with your organisation and technology and continues to offer you an excellent basis for protecting yourself against cyber threats onboard.

We, as VHT, will continue to address CYBER issues in the future.

Uwe Reder, VHT

4. Acknowledgements

I would like to extend my special thanks to the participants who took part in the IT-Grundschutz profile workshops and expert groups from the very start and who contributed in the form of discussions and cooperations and/or participated in the adoption and processing of the Grundschutz modules.

I would also like to thank the Institute for the Protection of Maritime Infrastructures (DLR) who provided us with rooms for the last event in November.

Uwe Reder, VHT

5. Introduction

Shipping companies are obliged to undertake technical and organisational measures in order to adequately protect their IT systems and business processes. These obligations arise, by way of example, from data protection requirements (e.g. EU General Data Protection Regulation (EU GDPR) and the German Federal Data Protection Act 2018 (BDSG)) and, in future, from the requirements of the International Maritime Organization (IMO). In addition, the substantial investments that shipping companies make in their IT equipment need to be protected using appropriate safeguards. With regard to the principles of economy, the profile described here includes the minimum requirements for preventing high material and non-material damage (e.g. damage to reputation or loss of trust) that can arise for a shipping company from a breach of confidentiality, manipulation of data or unavailability of the IT infrastructure.

As part of its involvement in the Alliance for Cyber Security, an initiative of the Federal Office for Information Security (BSI), VHT, in cooperation with the BSI, has initiated a process that makes it easier for shipping companies to adapt their security concept to their individual framework conditions based on IT-Grundschutz. The IT-Grundschutz from the BSI represents a tried and tested methodology for increasing the level of information security in institutions of all sizes.

This IT-Grundschutz profile has been compiled to make it easier for you to get started with the IT security process. An IT-Grundschutz profile represents a model security concept that serves as a template for institutions with comparable framework conditions. Steps to be taken for IT-Grundschutz are generalised in this example, in order to ultimately enable all interested shipping companies to use the template to increase information security in their own organisation. This saves a lot of work and time.

Based on four business processes that are considered to be relevant, this white paper on the "IT-Grundschutz profile for shipping companies - Minimum protection for ship operations" includes:

- A list of relevant target objects (applications, IT systems and premises) to be protected,
- An assignment of matching IT-Grundschutz modules with requirements and implementation advice and
- Recommendations for the implementation sequence.

The following provide central support for implementation in the organisation:

1. A "Map" for the management team as a basis for making decisions and an "Implementation Roadmap" for IT professionals,
2. Recommendations for the targeted use of the comprehensive requirements information and implementation instructions from the BSI IT-Grundschutz standard.

6. Formal Aspects

Aspects	Description
Title:	IT-Grundschutz profile for shipping companies - Minimum protection for ship operations
Authors:	See Sec. 9 "List of authors"
Publisher:	Verein Hanseatischer Transportversicherer e.V. (VHT)
Version status:	Published on 24/01/2020, Version 1.0 Finalised in January 2018
IT-Grundschutz Compendium	This IT-Grundschutz profile is based on the BSI IT-Grundschutz Compendium in the 2019 Edition
Revision cycle:	This white paper should be reviewed every three years.
Confidentiality:	This version of the white paper is openly accessible. A classified version will also exist, which will only be accessible to users who were or are involved in preparing the other version. It is envisaged that the TLP (Traffic Light Protocol) classification will be "Amber".

7. Disclaimer

This white paper has been prepared with the utmost care but makes no claim to be complete or correct. The authors have no influence over the use of this IT-Grundschutz profile by users and do not know the individual requirements of their security concepts, so that naturally the former cannot assume any liability for the impact on the legal position of the latter.

8. Copyright

All contents of this work are protected by copyright, in particular texts and graphics. If not explicitly referenced, copyright lies with the participants in the "IT-Grundschutz profile for shipping companies" workshop. Dissemination and disclosure to third parties is expressly desired.

9. List of authors

The participants in the workshop "IT-Grundschutz profile for shipping companies" series developed by the BSI were involved in the preparation of this white paper. The workshops were organised by VHT, while the moderation was taken over by the BSI. The participants are listed in alphabetical order in the following table.

Name	Organisation
Kersten Gevers	afEfa IT & Beratung GmbH
Leif Oelschläger	BOCS Bremen Overseas Charterinq and Shippinq GmbH
Jan Schirrmacher	bremenports GmbH & Co. KG
Jan Ruhnau	Bremer Bereederungsgesellschaft mbH & Co. KG
Klemens Kowalski	Federal Office for Agriculture and Food (BLE)
Martin Tolle	Federal Office for Agriculture and Food (BLE)
Heiko Zahn	Carl Büttner GmbH
Asmus Hammer	Consist Software Solutions GmbH
Henry Grow	Consist Software Solutions GmbH
Udo Wienstroer	Emder Schlepp-Betrieb GmbH
Silke Angermann	ERGO Versicherung AG
Christian Hemminghaus	Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE
Dr. Felix Greve	Hamburg Sudamerikanische Dampfschifffahrts-Gesellschaft A/S & Co KG
Frank Steffen	Hamburg Sudamerikanische Dampfschifffahrts-Gesellschaft A/S & Co KG
Michael lppich	Hartmann AG
Julius Vieregge	Howden Group
Christian Fölster	lnmarsat Global Limited
Carl Wrede	lnstitut fur den Schutz maritimer lnfrastrukturen, DLR e.V
Darian Sulies	lnstitut fur den Schutz maritimer lnfrastrukturen, DLR e.V
Malte Struck	lnstitut fur den Schutz maritimer lnfrastrukturen, DLR e.V
Dr. Nils Meyer-Larsen	ISL lnstitut fur Seeverkehrswirtschaft und Logistik
Andreas Held	ITE Solutions GmbH
Thomas Nintemann	Kanzlei Thomas Nintemann (law firm)
Louis Ravens	Lampe & Schwartze KG
Reinhard Kalkofen	Lampe & Schwartze KG
Steffen Thormann	Mund & Fester GmbH & Co. KG
Stefan Hentschel	NSB Niederelbe Schiffahrtsqesellschaft mbH & Co. KG
Andreas Fehrs	NSC Shipping GmbH & Cie. KG
Philip Timons	NSC Shipping GmbH & Co. KG
Martin Förster	NSSLGlobal GmbH
Anna Hanses	NSSLGlobal GmbH

Name	Organisation
Benjamin Weltz	PETER DOHLE Schiffahrts-KG
Wilko C. Bruhn	Raytheon Anschutz GmbH
Philipp Maas	Rhenus Schiffsmanaqement GmbH
Dirk Eggers	Sandomeer, Schulte & Partner
lngo Wenske	SLOMAN NEPTUN Schiffahrts-Aktiengesellschaft
Arne Maskus	Thomas Schulte Ship Management
Christoph Niendorf	Veinland GmbH
Uwe Reder	Verein Hanseatischer Transportversicherer e.V.
Jan Lausch	Wärtsilä SAM Electronics GmbH
Mattias Hamann	Waterway IT Solutions GmbH
Florian zum Felde	Waterway IT Solutions GmbH & Co. KG
Jurgen Berentzen	WESSELS Reederei GmbH & Co. KG

10. Management Summary

10.1. Target Audience

This IT-Grundschutz profile is aimed at shipping companies that want to ensure information security in ship operations.

It is specifically intended for managers, IT administrators and QA managers who are responsible for implementing and maintaining information security.

10.2. Purpose

This IT-Grundschutz profile focuses on four business processes in the operation of ships at a model shipping company and recommends security requirements that need to be met in accordance with the approach to standard protection according to IT-Grundschutz. The four business processes are:

- **Technical Operation**
- **Nautical Operation**
- **Loading Operation**
- **Communication**

The IT-Grundschutz profile helps organisations take the first steps in information security and get started with identifying the most serious vulnerabilities in the aforementioned processes, and also provides support in determining further protection needs and risk analysis.

In order to define the minimum protection requirement for the entire shipping company on the ship, all other business processes at the shipping company need to be included in accordance with the strategy for this IT-Grundschutz profile.

10.3. Tasks at management level

The authors recommend that the management level at shipping companies use this IT-Grundschutz profile as the basis for their information security concept for ship operations. That said, however, this IT-Grundschutz profile makes exclusive reference to the business processes ‘Technical Operation’, ‘Nautical Operation’, ‘Loading Operation’ and ‘Communication’ and not to the entire organisation at a shipping company. All other relevant business processes would need to be recorded and documented accordingly for them to be covered. This would then make it possible to determine the minimum requirements for action for ship operations and select appropriate security measures.

The authors recommend that shipping companies that, for instance, use third parties to operate parts of their technical infrastructure use this IT-Grundschutz profile as a basis for selecting the respective service providers. The requirements formulated here should be included in the terms of the contract.

11. Specification of the scope

11.1. Target Audience

This IT-Grundschutz profile is aimed at shipping companies that want to safeguard information security in ship operations.

11.2. Protection needs

The present IT-Grundschutz profile defines a level that corresponds to the Standard Protection in the IT-Grundschutz strategy and is appropriate for normal protection needs and sufficient to protect business-relevant information.

In addition, some target objects with increased protection needs have also been identified, such as the control network or the bridge. Additional safety measures may need to be determined and implemented for these target objects, on the basis of the risk analysis still to be carried out in detail.

11.3. IT-Grundschutz methodology

The requirements listed in this IT-Grundschutz profile are recommendations to shipping companies for implementing information security in ship operations. At a minimum, they cover the Standard Protection requirements of BSI Standard 200-2, and, in some cases, requirements relating to high or very high protection requirements that also need to be implemented.

11.4. Coverage Strategy

Use of the IT-Grundschutz profile for shipping companies achieves the standard level of protection and in some cases the protection level "High" and "Very High".

11.5. ISO 27001 compatibility

Implementation of the IT-Grundschutz strategy "Standard Protection" makes it compatible with ISO 27001.

11.6. Framework Conditions

The information security requirements described in this profile take into account the requirements of the EU General Data Protection Regulation (EU GDPR), the German Federal Data Protection Act (BDSG 2018) and the future requirements of the International Maritime Organization (IMO).

This IT-Grundschutz profile is based on the BSI IT-Grundschutz Compendium in the 2019 Edition.

11.7. Obligation to fulfil

It follows from the standards mentioned in Sec. 11.6 that shipping companies are obliged to safeguard information security. Information security can be safeguarded with the help of this IT-Grundschutz profile.

12. Specification of the information domain

12.1. Components in the information domain

The information domain for a shipping company's ship operations includes all processes, applications, IT systems and premises required for executing the entire process at a shipping company. This IT-Grundschutz profile is limited to the business processes ‘Technical Operation’, ‘Nautical Operation’, ‘Loading Operation’ and ‘Communication’ and takes into account the applications, IT systems and premises connected with them.

12.2. Objects not taken into account

This IT-Grundschutz profile does not take account of all the remaining processes required for executing the overall process in ship operations at a shipping company. The authors are convinced that the four business processes selected, "Technical Operation", "Nautical Operation", "Loading Operation" and "Communication" are sufficiently representative of all business processes not accounted for and that a shipping company can use this IT-Grundschutz profile very well as a basis for the development and continuation of a bespoke information security management system.

The information security on land (shore operation) at the shipping company continues not be to taken into account expressly. We make reference to the **IT-Grundschutz profile for shipping companies** - **Minimum protection for shore operations** for this purpose, which has already been prepared.

12.3. Link to other IT-Grundschutz profiles

We make reference to the **IT-Grundschutz profile for shipping companies - Minimum protection for shore operations** here for the purpose of securing shore operations at a shipping company.

13. Reference Architecture

The reference architecture (also referred to as the 'object under investigation') specifies the objects that the requirements of the IT-Grundschutz need to be applied to in terms of this IT-Grundschutz profile.

These include:

- Business Processes;
- Applications (software programs),
- Existing IT systems (including clients, servers, network coupling elements, mobile devices) as well as the networks, communication devices and external interfaces deployed;
- Spatial conditions/infrastructure (ships, rooms).

13.1. Object under investigation

13.1.1. Business Processes

The **business process 'Technical Operation'** comprises the sub-processes:

- Remote Management
- Remote Maintenance
- Maintenance
- Predictive Maintenance
- Monitoring (performance)
- Operation of the main machine
- Emergency power supply
- Machine Control
- Safety+Security
- Environmental Systems (Marpol)
- Ballasts (weight balancing)
- Bunkering

The **business process 'Nautical Operation'** comprises the sub-processes:

- Route Planning
- Voyage Execution
- Route Monitoring
- Collision Prevention
- Reporting
- Documentation
- Ballast water management
- Emergency Management
- Administration

The **business process 'Loading Operation'** comprises the sub-processes:

- Stowage Planning (stability)
- Loading
- Unloading
- Cargo Handling (monitoring)
- Communication (information exchange, reporting)

The **business process 'Communication'** comprises the sub-processes:

- Cross references technical/nautical/loading
- Private Communication

13.1.2. Applications

- Manufacturer Software
- Service provider software
- Standard Software
- Office
- Email
- Cloud
- M2M Software
- ECDIS
- Auto Pilot
- MS Office applications
- Bridge alert management
- Radar Software
- Nautical chart correction software
- GMDSS
- Weather Software
- Digital Publications
- Digital Log Book
- Planning Software (individual)
- Monitoring Software (sensors)
- File server/service (incl. automatic data transfer)
- Cloud (incl. web hosting)
- Reporting Software
- Remote Maintenance
- Web Browser (business, private)
- Email/Groupware (especially ship-land; crew; passengers etc.)
- DNS
- DHCP

- User Administration (AD, directory service)
- Interfaces (e.g. telex, fax to IT)
- File server/service (incl. automatic data transfer)
- Database
- Monitoring Software (sensors)

13.1.3. IT Systems

- Control Systems (e.g. main machine, WTS)
- Clients (Windows; terminal server)
- Server (Windows and Linux)
- Telephony (VoIP, satellite, SAT-C, radio, etc.)
- Network (router & switches/LAN/WIFI/VPN/firewall)
- Control Network (OT) Sensors
- Monitoring system sensors (e.g. fire alarm system)
- IOT
- Peripherals, multifunctional devices
- Mobile Devices (tablet, photo camera)
- GPS
- Voyage data recorder (VDR)
- AIS
- Control Network (OT) Sensors
- ECDIS PC (also multifunctional displays, radar, conning, etc.)
- Navigation Systems (e.g. INS)
- Navigation network sensors: echo sounder, gyrocompass, magnetic compass, speed log and, for example, NMEA-to-Ethernet converter
- Mobile data carrier
- Telephony (VoIP, satellite, SAT-C, radio, etc.)
- WAN (satellite system, LTE)
- Peripherals, multifunctional devices
- Laptop

13.1.4. Networks and Communications Links

- Firewall
- Router
- Switches
- LAN
- Wi-Fi
- VPN
- Telephone (VoIP, satellite, SAT-C, radio)
- Fax

- Telex
- Network

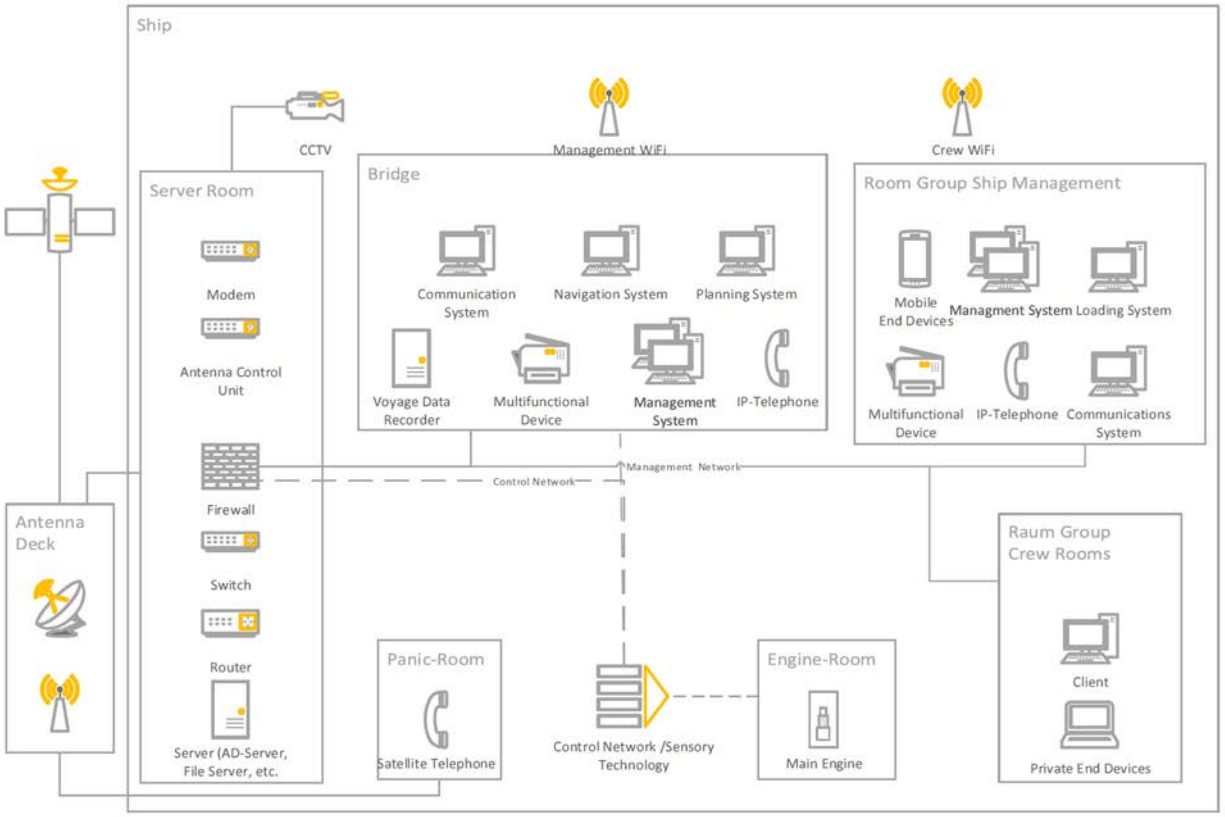
13.1.5. Spatial conditions/Infrastructure

- Bridge
- Engine Room
- Ship Management (captain’s cabin, engine control room)
- Crew Space
- Server Room
- Antenna Deck
- Panic Room (Citadel)
- Ship

13.2. Addressing differences

If the information domain to be protected deviates from the reference architecture, the additional or non-existent objects need to be documented. Suitable modules from the IT-Grundschutz Compendium are to be assigned to these. The requirements derived from the modules need to be adapted depending on the protection level wanted.

13.3. Network Plan



Room groups are to be understood as rooms that are equipped and used similarly.

14. Requirements to be fulfilled and measures to be implemented

Suitable IT-Grundschutz modules can be selected based on the reference architecture. These contain explanations on the risk exposure and security requirements, along with further information.

The modules from the IT-Grundschutz Compendium listed in this IT-Grundschutz profile generally suffice to achieve the security level wanted. Operational environments or components that deviate from the IT-Grundschutz profile require the use of other components in some circumstances. A review is therefore required within the context of using the IT-Grundschutz profile.

Tip for the management team:

Each IT-Grundschutz module contains information about the exposure to risk that describes the risks of failing to implement the recommended security requirements.

Additional implementation information with detailed descriptions of suitable security measures that can be used as a basis for security concepts exists for many modules.

14.1. Everything at a glance - Work aids: "Map"

A "Map" was created for each of the four business processes considered here. The map shows all essential findings from the structural analysis and modelling (selection of suitable IT-Grundschutz modules). The reference architecture (applications, IT systems and rooms) and the allocation of the IT-Grundschutz modules, including recommendations for the implementation sequence, are presented for each business process. In cases where it is not possible to allocate existing modules, it becomes clear that an in-house risk analysis and, eventually, organisation and/or industry-specific solutions are required.

The maps offer virtually "everything at a glance" in the form of graphics and thus open up access to the bespoke IT security process. They can serve both as a basis for decision-making for the company management and as an "implementation roadmap" for IT professionals.

The maps of the four business processes discussed here can be found in the Annex:

- **Technical Operation (17.1)**
- **Nautical Operation (17.2)**
- **Loading Operation (17.3)**
- **Communication (17.4)**

Information on use:

The **white shields** refer to appropriate IT-Grundschutz modules to be used on the respective target object. A module can play a role in several business processes. Implementation of the respective security requirements can result in synergies because the measures implemented for a prioritised business process immediately radiate out and have an effect on other business processes.

If the applications, IT systems, rooms and facilities are **marked with a white asterisk** (*), it shows that further steps are required to achieve the security level wanted. The individual meaning of the various markings is as follows:

- **No Marking:** The modules listed here from the IT-Grundschutz Compendium suffice alonefor achieving the safety level wanted.
- **One asterisk (*):** The modules listed here from the IT-Grundschutz Compendium do not suffice alone for achieving the safety level wanted. Further requirements and implementation instructions need to be developed individually.
- **Two asterisks (**):** Currently, the IT-Grundschutz Compendium does not contain a module for this. Further requirements and implementation instructions need to be developed individually. As a rule, this also requires a risk analysis in order to align the measures to be taken with the business risk identified. Information on this can be found in Section 16.2.

Marking with one or two **security shields** refers to a special need for protection. Since the protection requirement is not usually quantifiable, IT-Grundschutz is limited to a qualitative statement by dividing the protection requirement into three categories:

Protection Requirement categories	**Description**
"Normal" (not marked)	The effects of damage are limited and manageable.
"High" (one security shield)	The effects of damage can be considerable.
"Very High" (two security shields)	The effects of damage can reach a catastrophic extent that represents a threat to existence.

14.2. Overview I: General Modules

The modules listed in this section cannot be found on the maps since they relate more to the entire information domain and not to individual target objects. Examples of this are the modules ISMS.1 and CON.3, which are not applied to a single target object such as an IT system, but are used across the entire information domain. These modules are necessary for a comprehensive concept of an information security system and also need to be implemented.

Tip for the implementation sequence:

The following modules have notes added on the processing sequence:

- **R1:** These modules need to implemented as a priority since they form the basis for an effective security process
- **R2:** These modules should be implemented next, since they are needed as key components in the sustainable security information domain
- **R3:** These components are also needed to achieve the desired security level and have to be implemented, but we recommend considering them after the other components

14.2.1. ISMS.1 Security Management (R1)

14.2.2. ORP: Organisation and personnel

ORP.1 Organisation (R1)

ORP.2 Personnel (R1)

ORP.3 Awareness and Training (R1)

ORP.4 Identity and Access Management (R1)

ORP.5 Compliance Management (R3)

14.2.3. CON: Conception and strategies

CON.1 Crypto Concept (R3)

CON.2 Data Protection (R2)

CON.3 Backup Concept (R1)

CON.4 Selection and Use of Standard Software (R2)

CON.6 Deleting and Destroying Data and Devices (R1)

CON.7 Information Security on Trips Abroad (R3)

CON.8 Software Development (R3)

CON.9 Information Exchange (R3)

14.2.4. OPS: Operation

OPS.1.1.2 Proper IT Administration (R1)

OPS.1.1.3 Patch and Change Management (R1)

OPS.1.1.4 Protection against Malware (R1)

OPS.1.1.5 Logging (R1)

OPS.1.1.6 Software Tests and Approvals (R1)

OPS.1.2.2 Archiving (R3)

OPS.1.2.4 Teleworking (R3)

OPS.1.2.5 Remote Maintenance (R3)

OPS.2.1 Outsourcing for Customers (R2)

OPS.2.2 Cloud Usage (R2)

OPS.3.1 Outsourcing for Service Providers (R3)

14.2.5. DER: Detection of security incidents and incident response

DER.1 Detection of Security-Relevant Events (R2)

DER.2.1 Security Incident Handling (R2)

DER.2.2 Provisioning for IT Forensics (R3)

DER.2.3 Clean-Up of Extensive Security Incidents (R2)

DER.3.1 Audits and Revisions (R3)

DER.3.2 Audits based on the BSI “Guideline für IS-Audits” (R3)

DER.4 Business Continuity Management (R3)

14.2.6. SYS: IT Systems

SYS.3.2.2 Mobile Device Management (MDM) (R2)

14.2.7. IND: Industrial IT

IND.1 Operating and Control Technology (R2)

14.2.8. INF: Infrastructure

INF.9 Mobile Workplace (R2)

14.3. Overview II: Modules from the map

The modules listed in this section can also be found in the maps and are assigned there to individual target objects.

14.3.1. OPS: Operation

OPS 1.2.5 Remote Maintenance

OPS.2.2 Cloud Usage

14.3.2. APP: Applications

APP.1.1 Office Products (R2)

APP.1.2 Web Browsers

APP.1.4 Mobile Applications (Apps) APP.2.1 General Directory Dervice

APP.2.2 Active Directory

APP.2.3 OpenLDAP

APP.3.1 Web Applications APP.3.2 Web Servers APP.3.3 File Servers

APP.3.4 Samba APP.3.6 DNS Servers

APP.4.3 Relational Database Systems

APP.5.1 General Groupware

APP.5.2 Microsoft Exchange und Outlook

14.3.3. SYS: IT Systems

SYS.1.1 General Server

SYS.1.2.2 Windows Server 2012

SYS.1.3 Unix Servers

SYS.1.5 Virtualisation

SYS.1.7 IBM Z System

SYS.1.8 Storage Solutions

SYS.2.1 General Clients

SYS.2.2.2 Windows 8.1 Clients

SYS.2.2.3 Windows 10 Clients

SYS.2.3 Unix Clients

SYS.2.4 macOS Clients

SYS.3.1 Laptop

SYS.3.2.1 General Smartphones and Tablets (R2)

SYS.3.2.2 Mobile Device Management (MDM) (R2)

SYS.3.2.3 iOS (for Enterprise)

SYS.3.2.4 Android

SYS.3.3 Mobile Telephones

SYS.3.4 Mobile Storage Media

SYS.4.1 Printers, copiers and All-in-One Devices (R2)

SYS.4.4 General IoT Devices

14.3.4. NET: Networks and Communication

NET.1.1 Network Architecture and Design (R2)

NET.1.2 Network Management

NET.2.1 Wi-Fi Operation

NET.2.2 Wi-Fi Usage

NET.3.1 Routers and Switches

NET.3.2 Firewall

NET.3.3 VPN

NET.4.1 Telecommunications Systems

NET.4.2 VoIP

NET.4.3 Fax machines and Fax Servers

14.3.5. IND: Industrial IT

IND.2.1 General ICS components

IND.2.2 Programmable Logic Controller (PLC)

IND.2.3 Sensors and Actuators

IND.2.4 Machine

IND.2.7 Safety Instrumented Systems

14.3.6. INF: Infrastructure

INF.1 General Building

INF.2 Data Centre/Server Room

INF.3 Electrotechnical Cabling

INF.4 IT Cabling

INF.6 Storage Media Archives

INF.7 Office Workplace

INF.9 Mobile Workplace

INF.10 Meeting, Event and Training Rooms

15. Residual risk assessment/risk response

The basic and standard requirements of the IT-Grundschutz module have been defined so that suitable measures for normal protection requirements and typical information domains and application scenarios offer appropriate and sufficient protection. For this purpose, a preliminary investigation was carried out to identify which hazards the issues addressed in the modules are usually exposed to and how the risks that result from them can be appropriately countered. As a rule, users of the IT-Grundschutz profile no longer need to spend a great deal of time and effort investigating the security measures required for the vast majority of the information domain selected.

An additional need for analysis only exists in the following three cases:

- A target object has a high or very high protection requirement in at least one of the three basic values of confidentiality, integrity and availability.
- The IT-Grundschutz Compendium does not contain a sufficiently adequate component for a target object.
- Although there is a suitable module, the deployment environment for the target object is atypical for IT-Grundschutz.

Instructions for performing a risk analysis can be found in Section 16.2.

16. Directions for use

16.1. Directions on how to determine protection requirements

At a minimum, the requirements listed in this IT-Grundschutz profile cover the "standard protection" requirements of BSI Standard 200-2: Eventually, requirements relating to high protection requirements also need to be implemented.

An individual determination of protection needs according to the IT-Grundschutz method is strongly recommended. If a determination of the protection requirements defines an "increased protection requirement" for individual target objects (category "High" or "Very High"), then the basic and standard protection measures are no longer sufficient. A risk analysis needs to be carried out from this point, and eventually other appropriate measures identified and implemented.

Information on the protection requirement categories

Since the protection requirement is not usually quantifiable, IT-Grundschutz is limited to a qualitative statement by dividing the protection requirement into three categories:

Protection Requirement categories	Description
"Normal" (not marked)	The effects of damage are limited and manageable.
"High" (one security shield)	The effects of damage can be considerable.
"Very High" (two security shields)	The effects of damage can reach a catastrophic extent that represents a threat to existence.

Damage Scenario	Protection requirement category: "Normal"
Breaches of laws/regulations/contracts	Breaches of regulations and laws with minor consequences Minor breaches of contract with low maximum penalties
Impairment of the right of informational self-determination	This concerns personal data, the processing of which can compromise the data subject in his social standing or economic circumstances.
Impairment of personal integrity	An impairment appears not to be possible.
Impairment in the performance of functions	The impairment would be considered tolerable by data subjects. The maximum tolerable downtime lies at between 24 and 72 hours.
Negative interior or exterior effect	A slight or only internal effect on reputation or trust is to be expected.
Financial Impact	The financial damage remains tolerable for the organisation.

Table 1: Protection requirement category: "Normal"

Damage Scenario	Protection requirement category: "High"
Breaches of laws/regulations/contracts	Breaches of regulations and laws with significant consequences Breaches of contract with high penalties
Impairment of the right of informational self-determination	This concerns personal data, the processing of which can compromise the data subject in his social standing or economic circumstances.
Impairment of personal integrity	Impairment of personal integrity cannot be completely ruled out.
Impairment in the performance of functions	The impairment would be considered intolerable by individual data subjects. The maximum tolerable downtime lies at between one and 24 hours.
Negative interior or exterior effect	A broad effect on reputation or trust is to be expected.
Financial Impact	The damage causes considerable financial losses, but does not threaten existence.

Table 2: Protection requirement category: "High

Damage Scenario	Protection requirement category: "Very High"
Breaches of laws/regulations/contracts	Fundamental breach of regulations and laws Breaches of contract where the resulting losses due to liability are ruinous
Impairment of the informational right of self-determination	This concerns personal data, the processing of which poses a risk to the life and limb or the personal freedom of the data subject.
Impairment of personal integrity	Serious impairment of personal integrity is possible. Danger to life and limb
Impairment in the performance of functions	The impairment would be considered intolerable by all data subjects. The maximum tolerable downtime is less than one hour.
Negative interior or exterior effect	An nationwide impairment of trust or reputation is conceivable, possibly even of a nature that threatens the existence of the organisation.
Financial Impact	The financial damage poses a threat to the existence of the organisation.

Table 3: Protection requirement category: "Very High"

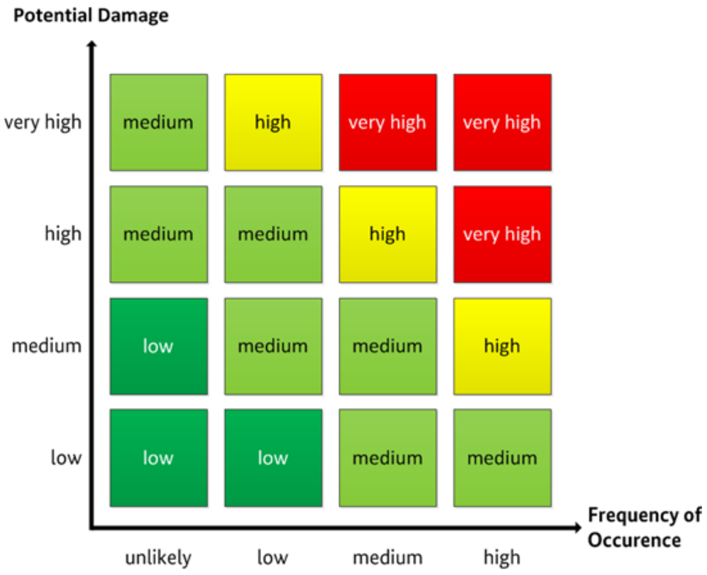
16.2. Directions for performing a risk analysis

A risk analysis represents the basic procedure for investigating security threats and their effects. BSI Standard 200-3: *Risk Management* offers an efficient methodology for this. We therefore make reference to BSI Standard 200-3 for specific procedures and a detailed description. Below is a short list of steps to be performed in a risk analysis:

- **Compile target objects:** he prerequisite for performing risk analyses in the context of standard protection is that the structural analysis includes the target objects in the information domain for which protection requirements have been identified, and, where possible, that suitable IT-

Grundschutz modules have been assigned to them during the modelling process. A risk analysis needs be performed on those target objects with a high or very high protection requirement in at least one of the three basic values of confidentiality, integrity and availability, or for which no suitable IT-Grundschutz module exists or which operate in deployment scenarios that are atypical for IT-Grundschutz.

- **Prepare risk overview:** The first step in a risk analysis is to identify the risks which an object or circumstance is exposed to. The risks the object or circumstance are subject to are to be described first for this purpose. The BSI has compiled a list of elementary risks to this end.
- **Complete risk overview:** Even though the process of compiling the elementary threats takes into account a variety of threats to which information and information technology are exposed, it cannot be ruled out that further threats will need to be considered. This is especially true if no suitable module exists for a target object or if the object is operated in atypical deployment scenarios. Following the first sub-step, you should therefore check whether other threats need to be investigated in addition to the relevant elementary hazards.
- **Estimate frequency and impact:** The level of risk results from the frequency of a threat and the threat of damage. A risk is greater the more frequently a threat occurs. Conversely, the risk decreases the less the eventual damage. In principle, both factors can be determined quantitatively, i.e. with precise numerical values, and qualitatively, i.e. with the aid of categories to describe the order of magnitude.
- **Evaluate the risks:** After assessing the frequency of occurrence and the damage impact of a threat, you can assess the risk that results from both factors. Not using too large a number of categories is also appropriate here with three to five categories being common. Often only two categories are used. BSI Standard 200-3 contains an example that contains four levels that you can adapt to the circumstances and needs of your organisation.


Potential Damage
Frequency of Occurence

Potential Damage	unlikely	low	medium	high
very high	medium	high	very high	very high
high	medium	medium	high	very high
medium	low	medium	medium	high
low	low	low	medium	medium

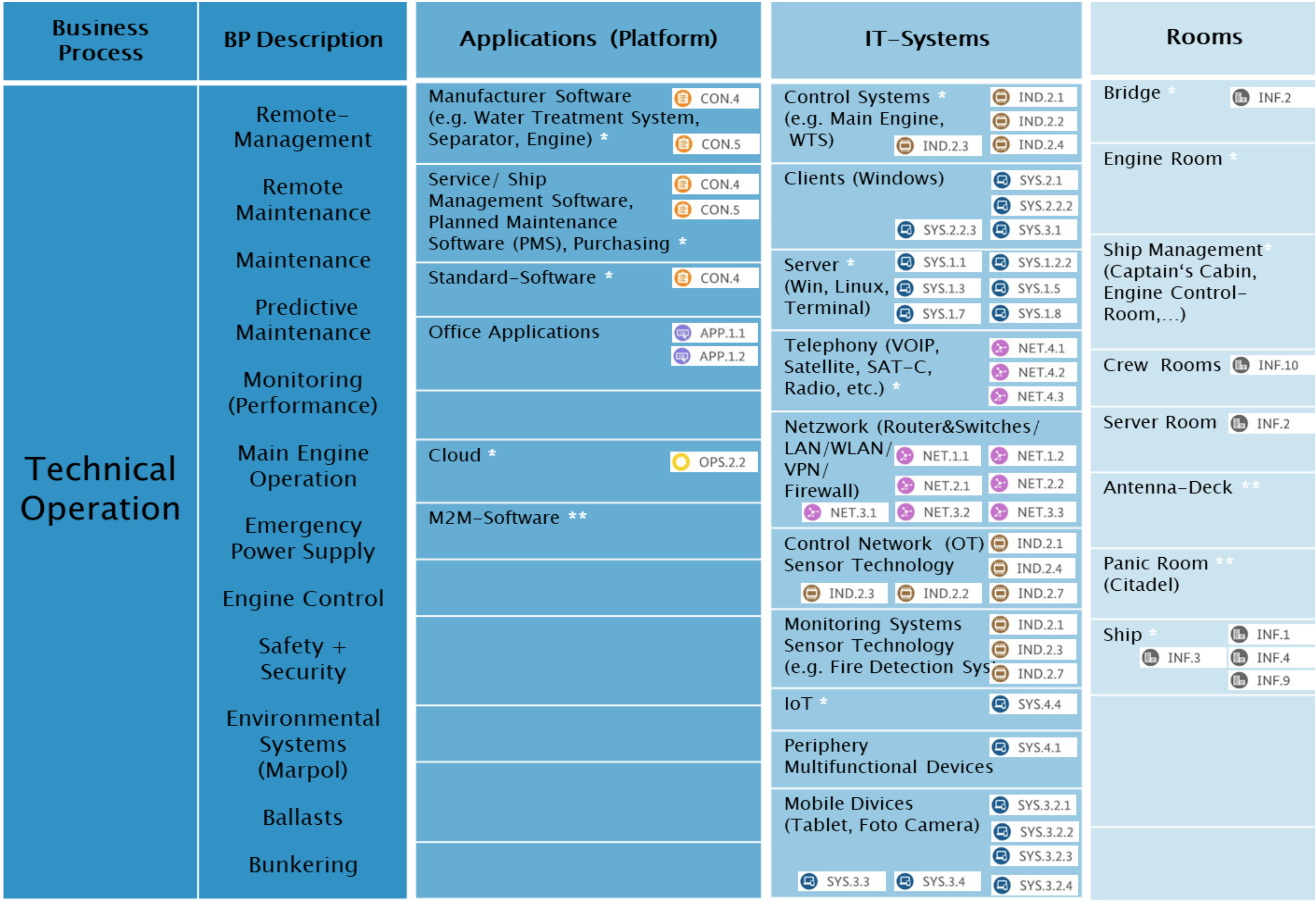
- **Address the risks:** Generally, your risk assessment will show that the existing security concept does not adequately cover all threats. In this case, you need to consider how to adequately address the remaining threats and make a reasoned decision to do so.
- **Consolidate the security concept:** As a conclusion to the risk analysis, the additional measures you have decided to implement need to be integrated into the existing security concept (= consolidation of the security concept) and the security process continued on the basis of this.

17. Annexes

The maps of the four business processes discussed here:

- **Technical Operation (17.1)**
- **Nautical Operation (17.2)**
- **Loading Operation (17.3)**
- **Communication (17.4)**

17.1. Annex 1: Business process map 'Technical Operation'



Business Process

Technical Operation

BP Description

- Remote-Management
- Remote Maintenance
- Maintenance
- Predictive Maintenance
- Monitoring (Performance)
- Main Engine Operation
- Emergency Power Supply
- Engine Control
- Safety + Security
- Environmental Systems (Marpol)
- Ballasts
- Bunkering

Applications (Platform)

- Manufacturer Software (e.g. Water Treatment System, Separator, Engine) * — CON.4, CON.5
- Service/ Ship Management Software, Planned Maintenance Software (PMS), Purchasing * — CON.4, CON.5
- Standard-Software * — CON.4
- Office Applications — APP.1.1, APP.1.2
- Cloud * — OPS.2.2
- M2M-Software **

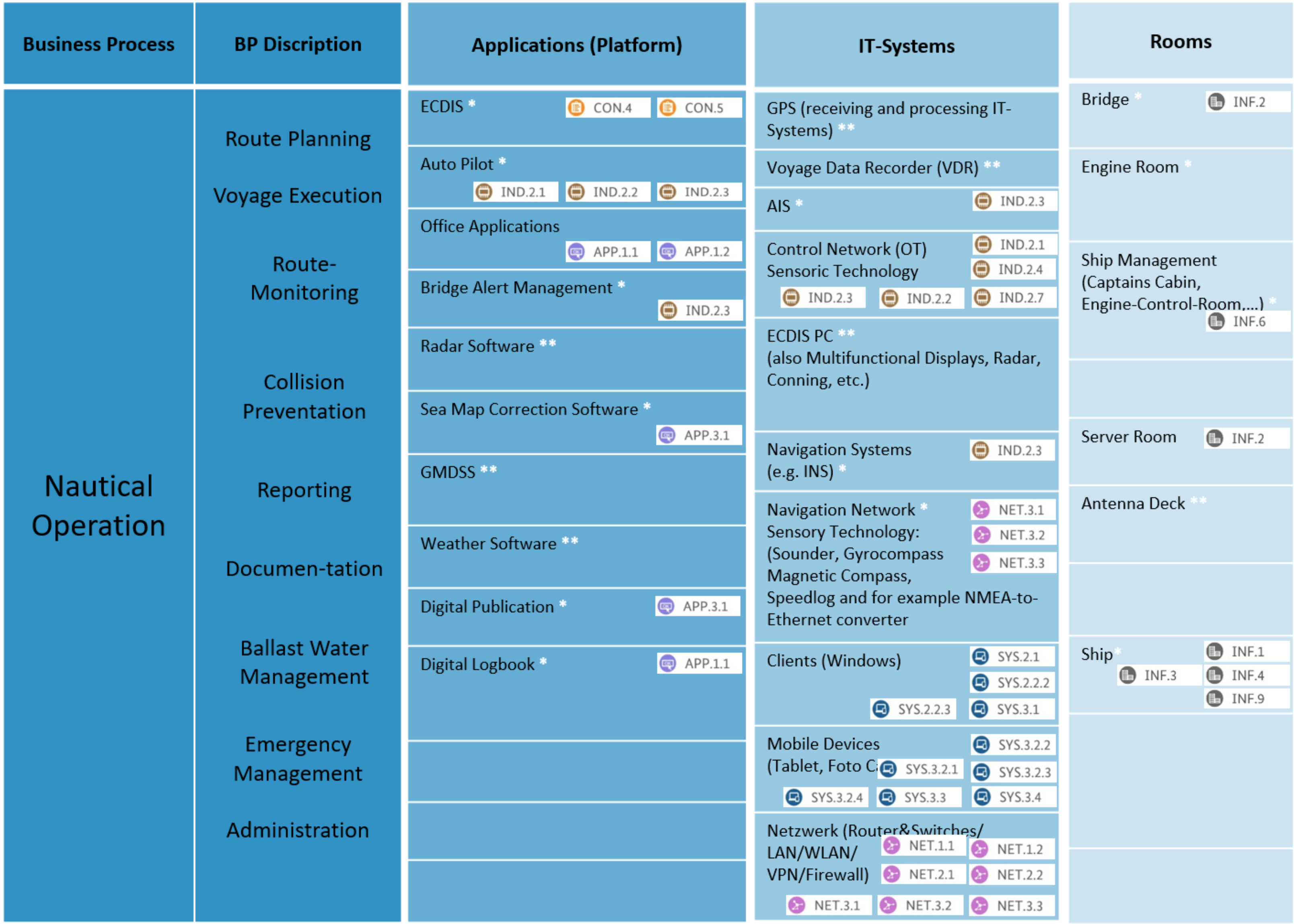
IT-Systems

- Control Systems * (e.g. Main Engine, WTS) — IND.2.1, IND.2.2, IND.2.3, IND.2.4
- Clients (Windows) — SYS.2.1, SYS.2.2.2, SYS.2.2.3, SYS.3.1
- Server * (Win, Linux, Terminal) — SYS.1.1, SYS.1.2.2, SYS.1.3, SYS.1.5, SYS.1.7, SYS.1.8
- Telephony (VOIP, Satellite, SAT-C, Radio, etc.) * — NET.4.1, NET.4.2, NET.4.3
- Netzwork (Router&Switches/ LAN/WLAN/ VPN/ Firewall) — NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3
- Control Network (OT) Sensor Technology — IND.2.1, IND.2.4, IND.2.3, IND.2.2, IND.2.7
- Monitoring Systems Sensor Technology (e.g. Fire Detection Sys — IND.2.1, IND.2.3, IND.2.7
- IoT * — SYS.4.4
- Periphery Multifunctional Devices — SYS.4.1
- Mobile Divices (Tablet, Foto Camera) — SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.3, SYS.3.4, SYS.3.2.4

Rooms

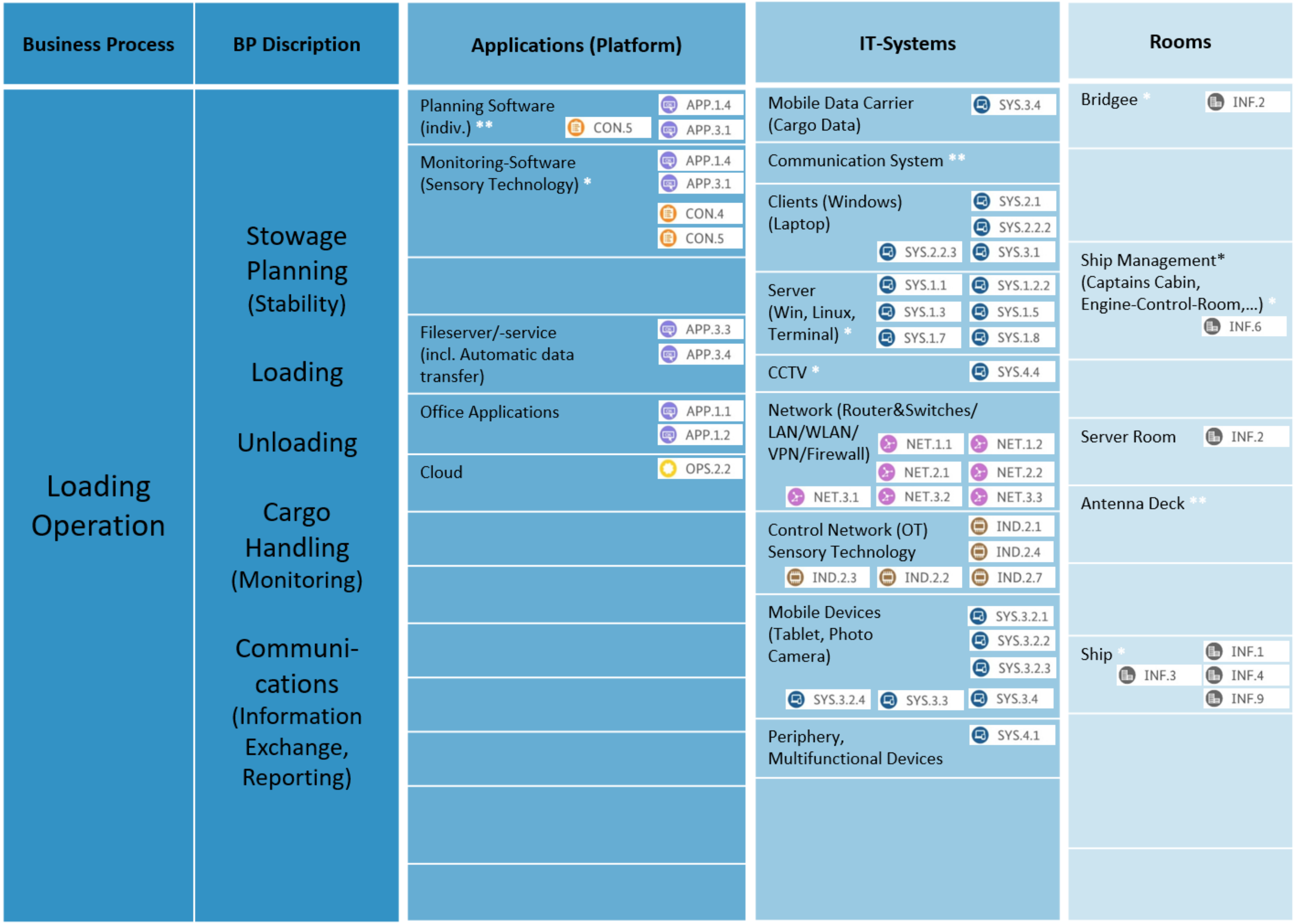
- Bridge * — INF.2
- Engine Room *
- Ship Management* (Captain's Cabin, Engine Control-Room,...)
- Crew Rooms — INF.10
- Server Room — INF.2
- Antenna-Deck **
- Panic Room ** (Citadel)
- Ship * — INF.1, INF.3, INF.4, INF.9

17.2. Annex 2: Business process map 'Nautical Operation'



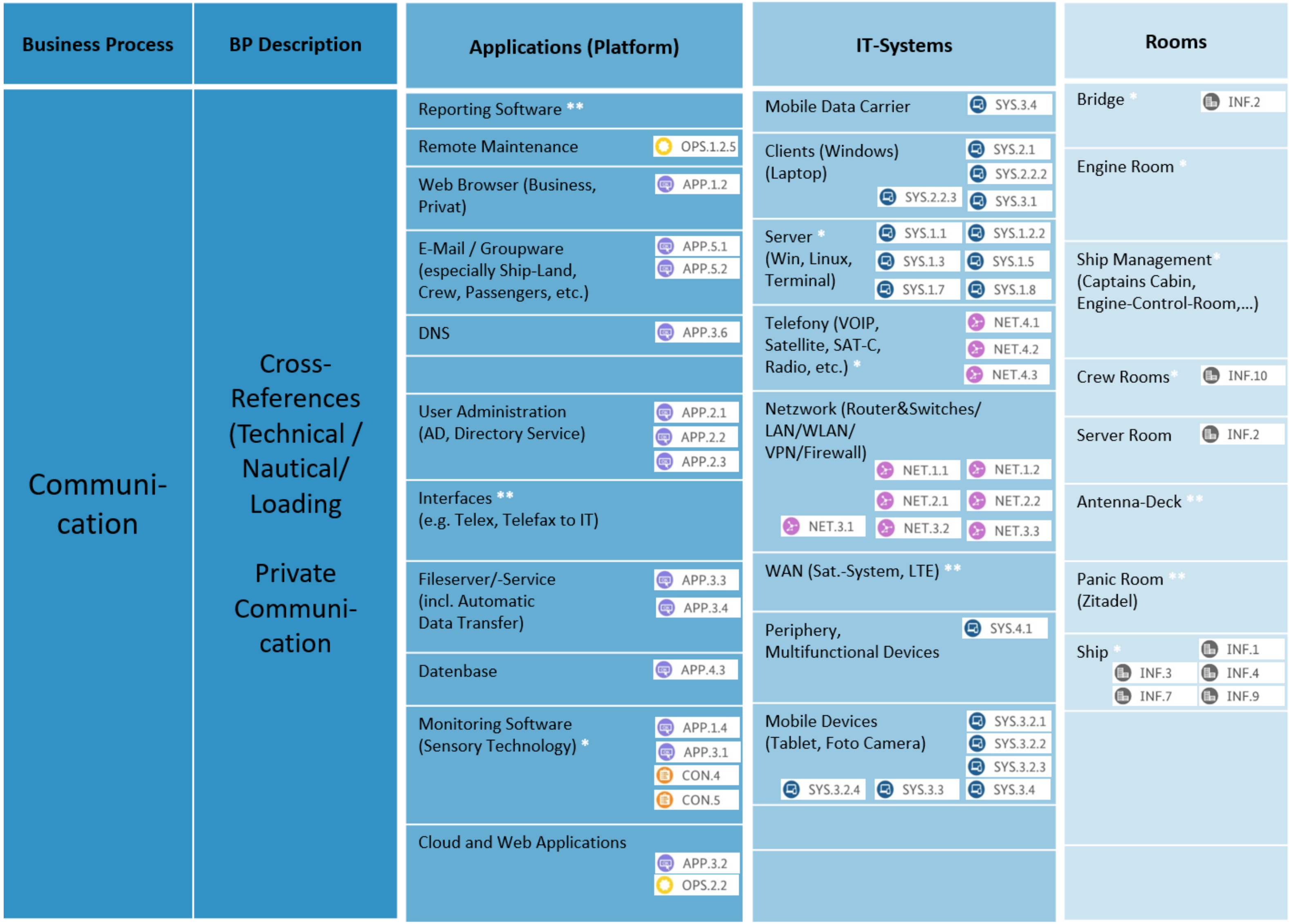
Business Process	BP Discription	Applications (Platform)	IT-Systems	Rooms
Nautical Operation	Route Planning Voyage Execution Route-Monitoring Collision Prevention Reporting Documen-tation Ballast Water Management Emergency Management Administration	ECDIS * CON.4 CON.5 Auto Pilot * IND.2.1 IND.2.2 IND.2.3 Office Applications APP.1.1 APP.1.2 Bridge Alert Management * IND.2.3 Radar Software ** Sea Map Correction Software * APP.3.1 GMDSS ** Weather Software ** Digital Publication * APP.3.1 Digital Logbook * APP.1.1	GPS (receiving and processing IT-Systems) ** Voyage Data Recorder (VDR) ** AIS * IND.2.3 Control Network (OT) Sensoric Technology IND.2.1 IND.2.4 IND.2.3 IND.2.2 IND.2.7 ECDIS PC ** (also Multifunctional Displays, Radar, Conning, etc.) Navigation Systems (e.g. INS) * IND.2.3 Navigation Network * Sensory Technology: (Sounder, Gyrocompass Magnetic Compass, Speedlog and for example NMEA-to-Ethernet converter NET.3.1 NET.3.2 NET.3.3 Clients (Windows) SYS.2.1 SYS.2.2.2 SYS.2.2.3 SYS.3.1 Mobile Devices (Tablet, Foto C SYS.3.2.2 SYS.3.2.1 SYS.3.2.3 SYS.3.2.4 SYS.3.3 SYS.3.4 Netzwerk (Router&Switches/ LAN/WLAN/ VPN/Firewall) NET.1.1 NET.1.2 NET.2.1 NET.2.2 NET.3.1 NET.3.2 NET.3.3	Bridge * INF.2 Engine Room * Ship Management (Captains Cabin, Engine-Control-Room,...) * INF.6 Server Room INF.2 Antenna Deck ** Ship * INF.1 INF.3 INF.4 INF.9

17.3. Annex 3: Business process map 'Loading Operation'



Business Process	BP Discription	Applications (Platform)	IT-Systems	Rooms
Loading Operation	Stowage Planning (Stability) Loading Unloading Cargo Handling (Monitoring) Communi-cations (Information Exchange, Reporting)	Planning Software (indiv.) ** APP.1.4 CON.5 APP.3.1	Mobile Data Carrier (Cargo Data) SYS.3.4	Bridgee * INF.2
		Monitoring-Software (Sensory Technology) * APP.1.4 APP.3.1 CON.4 CON.5	Communication System **	Ship Management* (Captains Cabin, Engine-Control-Room,...) * INF.6
		Fileserver/-service (incl. Automatic data transfer) APP.3.3 APP.3.4	Clients (Windows) (Laptop) SYS.2.1 SYS.2.2.2 SYS.2.2.3 SYS.3.1	Server Room INF.2
		Office Applications APP.1.1 APP.1.2	Server (Win, Linux, Terminal) * SYS.1.1 SYS.1.2.2 SYS.1.3 SYS.1.5 SYS.1.7 SYS.1.8	Antenna Deck **
		Cloud OPS.2.2	CCTV * SYS.4.4	Ship * INF.1 INF.3 INF.4 INF.9
			Network (Router&Switches/ LAN/WLAN/ VPN/Firewall) NET.1.1 NET.1.2 NET.2.1 NET.2.2 NET.3.1 NET.3.2 NET.3.3	
			Control Network (OT) Sensory Technology IND.2.1 IND.2.4 IND.2.3 IND.2.2 IND.2.7	
			Mobile Devices (Tablet, Photo Camera) SYS.3.2.1 SYS.3.2.2 SYS.3.2.3 SYS.3.2.4 SYS.3.3 SYS.3.4	
			Periphery, Multifunctional Devices SYS.4.1	

17.4. Annex 4: Business process map 'Communication'



Business Process

Communi-cation

BP Description

Cross-References (Technical / Nautical/ Loading

Private Communi-cation

Applications (Platform)

- Reporting Software **
- Remote Maintenance — OPS.1.2.5
- Web Browser (Business, Privat) — APP.1.2
- E-Mail / Groupware (especially Ship-Land, Crew, Passengers, etc.) — APP.5.1, APP.5.2
- DNS — APP.3.6
- User Administration (AD, Directory Service) — APP.2.1, APP.2.2, APP.2.3
- Interfaces ** (e.g. Telex, Telefax to IT)
- Fileserver/-Service (incl. Automatic Data Transfer) — APP.3.3, APP.3.4
- Datenbase — APP.4.3
- Monitoring Software (Sensory Technology) * — APP.1.4, APP.3.1, CON.4, CON.5
- Cloud and Web Applications — APP.3.2, OPS.2.2

IT-Systems

- Mobile Data Carrier — SYS.3.4
- Clients (Windows) (Laptop) — SYS.2.1, SYS.2.2.2, SYS.2.2.3, SYS.3.1
- Server * (Win, Linux, Terminal) — SYS.1.1, SYS.1.2.2, SYS.1.3, SYS.1.5, SYS.1.7, SYS.1.8
- Telefony (VOIP, Satellite, SAT-C, Radio, etc.) * — NET.4.1, NET.4.2, NET.4.3
- Netzwork (Router&Switches/ LAN/WLAN/ VPN/Firewall) — NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3
- WAN (Sat.-System, LTE) **
- Periphery, Multifunctional Devices — SYS.4.1
- Mobile Devices (Tablet, Foto Camera) — SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.2.4, SYS.3.3, SYS.3.4

Rooms

- Bridge * — INF.2
- Engine Room *
- Ship Management* (Captains Cabin, Engine-Control-Room,...)
- Crew Rooms* — INF.10
- Server Room — INF.2
- Antenna-Deck **
- Panic Room ** (Zitadel)
- Ship * — INF.1, INF.3, INF.4, INF.7, INF.9