Challenges of security certification in emerging ICT environments

DECEMBER 2016

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a center of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

The analysis in this document was produced in collaboration with:

- Coen Berenschot, Teun Ploeg, Willem Strabbing, Elena Henriquez Suarez, Knut Svein Ording, Svante Einarsson, Mate Csorba, Patrick Rossi
- Ben Kokx, Jose Miguel Rubio, Jose Luis Reyes
- Members of IEC TC57 working groups 10, 15, 17 and 19.

Furthermore, we would like to thank those who provided input and performed reviews and requested not to be mentioned above.

ISBN: 978-92-9204-183-0, doi: 10.2824/42310

Table of Contents

Executive Summary

Security certification is very limited in industrial environments despite the growing cyber attacks to what is considered EU Member State Critical Information Infrastructure (CII). There are "good" reasons for this situation, however, the community questions around the contribution of certification to the cyber security of the industrial CII production line remain unanswered. Today, without an EU approved standard, harmonised testing and corresponding certification, answering these questions is complicated and unclear. This is a major issue given the desire and policy agenda towards a more integrated and global digital infrastructure, which is needed to support the internal European market.

This study aims to provide a thorough description of the cyber security certification status concerning the most critical equipment in different critical business sectors. More specifically, five sectors have been selected to investigate in more detail and to consider a broad spectrum of different requirements and cases that could lead to certification drivers concerning these devices. The five sectors are[1] energy, ICT[2], health care, rail transport and water transport.

The key finding is that every sector has its own functional and security challenges which makes the target of a common certification framework a challenge. The energy sector, for example, largely depends on real-time interfaces on process automation level to provide a stable and reliable electrical power supply. The need for more real-time data exchange is increasing due to the decentralization of the power grid, increasing penetration of renewables and further integration of markets. On the other hand, the health care sector largely depends on informational systems and interfaces, like centralized patient databases that are used by companies that provide healthcare. Automation takes place on small scale, for example at hospitals to provide health monitoring. Transportation is mostly about logistics and safety. Finally, trains on a track need to be able to communicate with the generic infrastructure, while for the water transportation a vessel contains automation systems from office automation to process automation concerning electric power supply and vessel control. At the same time, ICT becomes the common processing platform which supports all these different functional and security requirements. This underlines the (increasing) need for a common approach on standards and frameworks for certification.

Based on desk research and expert validation, an analysis is done to study the existing frameworks and standards, and to identify certification drivers, best practices and candidate products for certification of the five selected sectors. During this study, common findings that apply to multiple sectors have been identified:

- A large part of the public infrastructure is used for data communication within and between critical infrastructures. This introduces additional challenges to a system versus a privately-owned infrastructure that is mostly considered as more secure.
- Standalone certified devices are considered trustworthy. However, after integration in a real computing environment this might be not the case. Appropriate planning and execution of system tests is critical, where device certification will help to get a certain level of device quality concerning cyber security.
- When it comes to building cyber security resilience in the selected sectors, it is observed that a small part of the security will be supported by the components or devices that compose the systems while the larger part of the security will depend on the processes and procedures that are in place.

[1] Based on the findings of the 2015 ENISA study, 'Methodologies for the identification of Critical Information Infrastructure assets and services', available at https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

[2] While ICT is not a vital sector per se, we found that this sector is of major importance since it provides a wide range of devices to other critical sectors.

- Many industries do not integrate security into their devices from the design phase. Thus, security by design is an approach that needs to be widely adopted by vendors. A holistic approach provides a certain level of security assurance at every level of the business value chain for critical infrastructures.
- Outsourcing of specific tasks or functions increases the risk of being vulnerable to cyber-attacks. Knowledge of the specific domain by those who deliver essential cyber security services is mandatory.
- An overall concern is the use of devices like laptops, tablets and phones as entry points for potential attacks or malware. This is a cross-sector threat where devices connected to complex and critical systems are mostly unmonitored and can cause serious risk to the overall stability of such complex systems.

For each sector, a list of devices was identified that should be considered candidates for certification. Although this list is not necessarily complete and exhaustive, these devices are found to have a large impact when compromised or in case they fail to operate. Accordingly, the identified devices included in the candidates' list provide a good starting point for the investigation to a common approach for certification, because within critical infrastructures every device could potentially endanger the whole system.

Based on the analysis of the drivers for certification and the market situation, it is found that the following devices are most critical for certification in each sector: For Energy - Electricity, smart meters and Intelligent Electronic Devices (IED); for health care, Clinical Information Systems (CIS); for ICT: firewalls, routers and switches; for transport – railway, Automatic Train Protection (ATP); and for transport – maritime, Integrated Bridge Systems (IBS).

The following common key recommendations are determined for these sectors:

- Organisations should strive for certifying their management system because it is a powerful tool that helps companies to achieve their business goals. **Process certification and compliance is vital** to support product quality, and it is often a ticket to the market. For markets large enough, product manufacturers can test and certify their products only once as they can have them accepted in many other markets or countries thereafter[3].
- Both vendors and asset owners should take a holistic view when it comes to security certification and not merely focus on the functional element of the devices they use. Only after **verification** of a system in its entirety, including procedures for operation and maintenance, it can be considered **cyber secure**.
- Organisations should invest more on improving the cyber security education of their engineers. This is because they usually do not have cyber security culture as they are often confronted with new technologies, or other domains unknown to them, until it is too late to adopt mitigation measures. Therefore, they need to be educated, to become aware of cyber risks and to realize that the system is as strong as each individual component, and that actions and decisions taken for a sub-part of the system can have a major impact on the overall performance of the system itself.
- Cyber security service providers are recommended to implement an IT service management framework in their organizations as a proof that their services meet customers' needs.
- Whenever this is financially justified, customers should look for the use of security service providers who provide a **follow-the-sun support**[4] team in order to ensure maximum availability of their services. Furthermore, they should seek for security service providers with an IT service management system which is based on international and widely known standards e.g. ITIL, ISO/IEC 20000 etc.

[3] Specific for EU Product Directives is the requirement on CE -marking the product

[4] Follow-the-sun is a type of global workflow in which tasks are passed around daily between work sites that are many time zones apart.

1. Introduction

There are many challenges when it comes to voluntary EU wide certification for cyber security. The major gaps and challenges revolve around the fragmentation and different approaches in the member states as well as the lack of EU guidance by trusted oversight entities. The cybersecurity strategy of the European Union (EU) states the need to develop industrial and technical resources for cybersecurity in emerging information communication technology (ICT) environments (COM(2006)786). To realize an open, safe and secure cyberspace, the prime focus of the strategy is "to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally" (JOIN(2013) 1) .

ENISA has been involved in the area of certification by, among others, supporting activities such as the workshop on security certification for smart grid devices (2012), the joint EC/ENISA SOG-IS and ICT certification workshop (2014) and the report on smart grid security certification (2014). One of the common findings of these activities was the lack of systematic recording of the major challenges, together with the lack of a harmonized certification framework in some critical business sectors.

Currently there exist different security standards and frameworks for certification from business sector to business sector. Not surprisingly, business sectors differ a lot concerning the use and importance of the ICT platforms, like type of system, components of different vendors, age, technologies and communication protocols. For instance, there are sectors that use and require automation systems for the automation and the safety of their critical operational processes, and disruption of these systems could lead to large societal impacts. Within other sectors, emerging ICT is used for centralized databases, markets and for communication between companies, resulting into a variety of interfaces between subsectors and companies. Furthermore, differences can be spotted between the type of system used, like information technology (IT) and near real-time automation systems as operational technology (OT). These varying ICT landscapes make it complex to develop and implement a common and widely accepted certification framework in this area.

Consequently, there is no common approach on standards and frameworks for certification within the European Union, and no certification program that focuses on the emerging ICT environments such as IoT, industry 4.0 etc. This is a major issue, as specified in (JOIN(2013) 1), "lack of a well-functioning mechanism of certification" is an inhibitor to the functioning of the European market as a whole. In line with the JOIN(2013) 1 and 2016/1148/EU, there is the desire to have a more integrated and global digital infrastructure, as a means to support the global European market. Accordingly, given the current situation and further developments, common cyber security practices and certification schemes are of great importance because security certification schemes are considered as a cyber security enabler which may:

- bring transparency into the processing taking place in a complex computing environment (supporting an answer to the "how secure" question),
- align IT and Engineering personnel to common security goals,
- help clean up responsibility questions (who is responsible for what?) and
- accelerate a secure introduction of emerging ICT technologies.

Addressing the harmonization issue, requires an understanding of the current challenges for security certification (the "good" reasons) and, subsequently, the identification of an implementation strategy which delivers results in a coordinated, balanced and cost-efficient manner for the society and the industry.

1.1 Objective

This report aims to provide decision makers with a thorough description of the security certification status concerning the most impactful equipment in five different critical business sectors. Results of this study should help to improve and harmonize the certification standards and frameworks in place, and pave the way towards a common approach to security certification in these sectors in the EU. Finally, both current and upcoming certification schemes will be considered while investigating the differences and similarities in the five selected critical sectors.

1.2 Methodology & deliverables

This report consists of two parts and adopts both a theoretical and empirical approach to investigate and answer questions around the relation of certification and security. The main methods applied are desk research and an observational study using questionnaires and interviews. Desk research was performed to collect publicly available existing standards and frameworks for certification, and to identify existing certification practices and challenges in the selected sectors. Of great help in selecting the areas of interest was the ENISA report on identification of critical infrastructure assets and services (JOIN(2013) , 2016/1148/EU).

Subsequently, a questionnaire was developed to identify challenges, needs, success stories and lessons learned of certification in the selected sectors. This questionnaire was used during interviews with experts of the selected sectors, after a careful identification of a list of experts from the relevant stakeholders within the selected sectors. The information gathered from the experts was used to validate the desk research about current challenges, risks and needs for security and conformity assurance, and collects best practices and lessons learned.

To meet the objective of the study, the following tasks were performed:

- Selection of five sectors, that cover most aspects concerning the different types of ICT environments for which conformity assessment is considered as a key enabler for the economic development.
- For each sector, identification of:
    - Elements of commonly used architectures
    - Different conformity assessment frameworks
    - Challenges to conformity assessments
    - Success stories and lessons learned
    - Useful conclusions on how to overcome the identified challenges
- Creation of an overview of existing standards and frameworks for certification concerning critical infrastructure protection in emerging ICT environments.

In order to be able to define clear recommendations based on the findings, the following questions need to be answered:

- What are the needs for different conformity assurance standards and techniques for each sector?
- What are different conformity assessments types for each sector?
- Which organizations are relevant to security certifications in each sector and what is their relationship?
- What is the role of existing international and European standards towards a harmonized certification approach?
- What are the main challenges facing the existing standards, guidelines, regulations and certification programs?
- What are the main incentives and barriers for developing the market of security certifications in Europe?

Results of this research have led to a clear overview of the challenges and the gaps in cyber security certification schemes.

1.3 Target audience

This report provides relevant information and recommendations for the Member States involved in defining certification schemes and the development of test programs of components in critical infrastructures. Furthermore this report is of interest to asset owners and operators engaged in securing or selecting secure component by providing an overview of existing components used today in critical infrastructures and possible existing certification schemes and standards.

1.4 Structure of this document

This report is structured as follows. Chapter 2 outlines which sectors are selected for further investigation. The subsequent chapters 3 – 7 are organized by sector and provide an overview and main findings of the sectors namely energy – electricity, health care, ICT, transportation – railway and transportation – water transport respectively. Finally, chapter 8 presents common findings and key recommendations.

2. Selected sectors

The latest Network Information Systems (NIS) directive gives an overview of sectors and subsectors that are seen as essential services. According to the NIS directive (2016/1148/EU), an essential service is an asset or system which is essential for the maintenance of vital societal functions. Damage to essential services, their destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, may have a significant negative impact on the security of the EU and the well-being of its citizens.

The selection of the sectors for this study, is based on the results of the ENISA study on the identification of critical infrstructures[1]. The following sectors and subsectors have been selected, using the naming convention as used in the NIS directive:

- Energy – Electricity
- Information and Communications Technology[5]
- Health Care
- Transportation – Rail transport
- Transportation – Water transport

Each sector is described in more detail in the following chapters 3 – 7 by providing a general overview of the sector, identification of the most impactful devices (that most likely require certification), and findings on certification drivers, best practices and recommendations to harmonize the cyber security approach in the EU. Accordingly, the following information is presented for each sector:

GENERAL INFORMATION	
Description	A short overview about the product, what is it doing, what is it used for etc.
Products	An overview of products that have been certified or assessed by these practices
Candidate products	An overview of products that could potentially be certified or assessed targeting these practices
Documents	A list of the standards, technical reports, sets of rules, boundaries, etc. that can be applied for certification of products
Certification authority	The authority that defines the certification rules and issues the final certificate upon successful completion of testing that issues a certificate
Regulatory authority	The entity that setup and regulates the certification scheme
Certification schemes/frameworks	The methodology and rules by which a certificate is granted to who undertakes the process (only for existing)

[5] It should be noted that the NIS directive does not state ICT. Sector ICT has been selected, because it fulfills an important role by providing critical devices to each of these sectors.

Certification drivers and issues	
Certification drivers	The following items[6] are considered when identifying certification drivers: • System criticality (does a Cyber Security attack imply a critical damage?) • Number of devices (is it in every house?) • Safety issues (does it affect people lives?) • Security issues (does a Cyber Security attack endanger people/country security?) • Access vector (is it connected to the internet?) • Environmental issues (does a Cyber Security attack endanger the environment?) • Intersystem dependencies (does a Cyber Security attack indirectly affect a connected system) • Regulations (does the law mandate a certification scheme?)
Recommendations	
A list of advice on what can be improved or addressed in the whole environment.	

[6] Only the items which exist at the time of writing this report appear in the certification key drivers' analysis tables per each device. Those who are empty are omitted from the analysis in order to avoid unnecessary duplications.

3. Energy - Electricity

The energy electricity sector's main activities are electricity generation and the delivery of this generated electricity to the various customers. Currently the energy sector experiences an energy transition from a fossil fuel based and centralized generation towards a more renewable and decentralized generation. This transition has a strong impact on the network infrastructure and related cyber security-related requirements. Figure 1 gives and overview of the current energy value chain with its major components.

In the centralized system, the energy is produced by the power plants and delivered through the transmission and distribution grid to the customers, so 'from left to right' in the figure. The current energy infrastructure deals increasingly with bidirectional power flows.

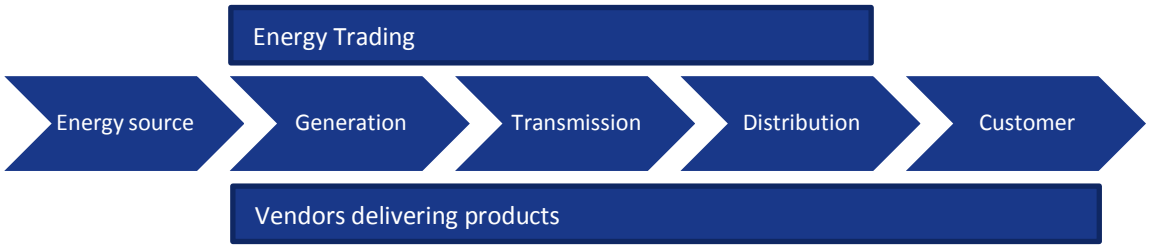

Figure 1 The energy power value chain

Generation, transmission and distribution are physical processes that execute the energy conversion and delivery to the customers. These processes are highly automatized by Supervisory Control and Data Acquisition (SCADA) systems, Energy Management Systems (EMS), Distribution Management Systems (DMS) and Grid Management Systems (GMS). Besides automation of the individual processes, the grid is automated to stabilize the frequency and voltage levels to prevent black-outs. This is the responsibility of the Transmission System Operators (TSO). This control requires real-time communication interfaces between different ICT systems both within the companies and between the companies active in the electricity sector.

Emerging ICT infrastructure has been observed in all active components across the energy power value chain as depicted in Figure 1. Devices like Intelligent Electronic Devices (IED), Remote Terminal Units (RTU), data concentrators, data historians, and others communicate within the value chain all the way down to the customers, i.e. the (smart) meters. Besides, as well the supporting IT systems that facilitate the production and distribution of electricity are involved, like energy trading and metering. The communication standards and interfaces in this sector are among others IEC 60870-5, IEC 61850, TASE.2/ICCP and DLMS.

The energy sector is a large sector with complex ICT usage and requirements, wherein a lot of standards and frameworks have been defined and are being used. It can be stated that the energy sector faces a lot of challenges regarding certification schemes and practices.

3.1 Desk Research

The energy sector is highly automated with multiple centralized and decentralized OT systems in power plants and substations. IT and OT overlap and intertwine to deal with the future electricity market and demands. Reliability of the power supply us essential for several reasons. Figure 2 shows a global the global infrastructure of the energy sector. It shows this sector is largely depending on subsectors.

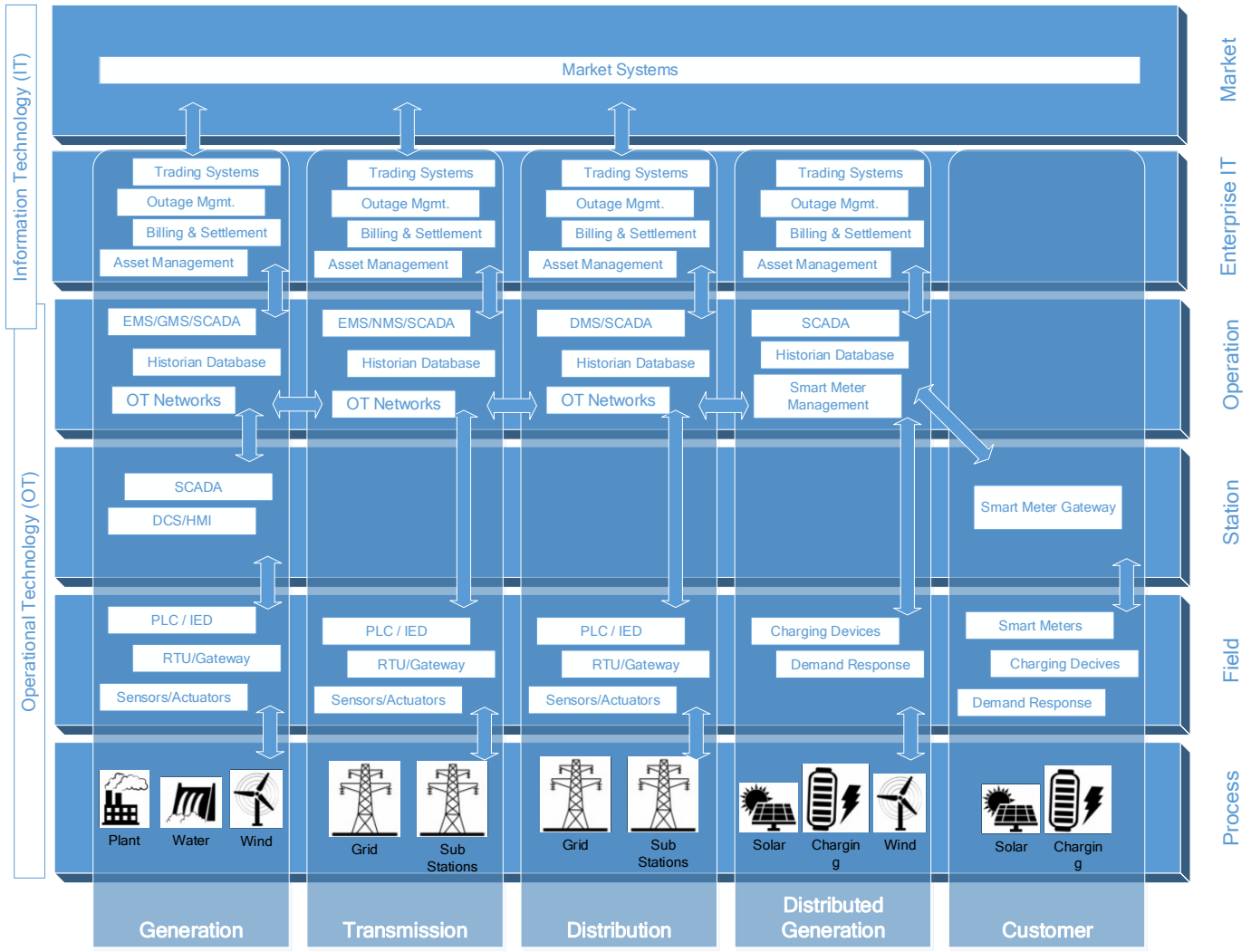

Figure 2 Global and simplified infrastructure of the Energy Sector

Every component in the energy value chain is important when it comes to ensuring that the electric grid is not being compromised. Especially, the operational systems, performing monitoring and control of the physical power system, can be targeted to create a black-out which has big impact on society.

The following devices are relying on high-speed and secure infrastructures to function properly and are considered essential for a correct and reliable functioning of the electrical grid:

- Intelligent Electronic Devices
- Remote Terminal Units
- Smart Meter communication
- AMI components
- Virtual Power Plants

3.1.1 Intelligent Electronic Devices (IEDs)

Description	IEDs are devices based upon a microcontroller, an operating system and a functional application and are responsible for monitoring, control and protection of electrical assets or primary components. Connected sensors provide process information via hardwired IO or via digital messages. These devices are required to be always on and available, and are

	considered essential for the correct operation of a modern digital substation or power plant.
Products	• Protection relays • Bay controllers • Tap-changers • (Auto) re-closers • Frequency and voltage controllers
Documents	• IEC 62351: Power systems management and associated information exchange – Data and communication security • IEC 62443: Security for industrial automation and control systems • IEEE 1686: Substation Intelligent Electronic Devices Cyber Security Capabilities • NERC CIP • NIST IR guidelines
Certification authority	UCA International Users Group
Regulatory authority	The certification based upon IEC 61850 is market driven
Certification schemes/frameworks	IEC 61850 conformance test program for communication interfaces IEC 61850-3 type test program

3.1.2 Remote Terminal Units (RTUs)

Description	RTUs are like IEDs, micro-processor based and responsible for communication between a central and remote location and translating the received commands from the central location to analogue and digital signals for the remote location. In addition, measurements and process information generated in the remote location is processed for transmission to the central location. The centrally located operators require correct information in order to make important decisions to maintain the stability of the remote sub-grids. Instable sub-grids may cause an instability to the whole grid. When there is no communication with the remote locations, it is necessary to have staff on-site remotely.
Products	• SCADA Front End • Station RTUs
Documents	• IEC 62351: Power systems management and associated information exchange – Data and communication security • IEC 62443: Security for industrial automation and control systems • NERC CIP • NIST IR guidelines • RFC2196
Certification authority	The certification for RTUs is market driven, independent test labs issue test reports upon completion
Regulatory authority	The certification for RTUs is market driven, independent test labs issue test reports upon completion
Certification schemes/frameworks	Ad hoc type testing of communication interfaces and interoperability testing based upon standardized test procedures

3.1.3 Smart Meters

Description	Smart meters measure electrical consumption at different locations and for different purposes. The smart meter has a connection to the ICT systems of the electrical utility.
Products	Domestic and industrial smart meters' communication interfaces
Candidate products	Different types of communication interfaces based upon national regulation
Documents	• IEC 62351: Power systems management and associated information exchange – Data and communication security • NIST • IEC 62056: DLMS UA Green Book Ed. 8.1 and Blue Book 12.1 • Smart Meters Coordination Group, SM-CG Technical Reports
Certification authority	Device Language Message Specification, DLMS User Association
Regulatory authority	The certification for smart meters is market driven, independent test labs and the DLMS user association issue test reports
Certification schemes/frameworks	Ad hoc type testing of meter communication interface and metering application

3.1.4 AMI Components

Description	The Advanced Metering Infrastructure comprises of different component that enable Smart Metering and Home Automation.
Products	• Metering End-Devices • Home Automation End-Devices • Local and Neighbourhood Access Points • Data Concentrator • Head End Systems
Documents	• Functional reference architecture for communications in smart metering systems, CEN/CENELEC/ETSI TR 50571, December 2011 • ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation) • SM-CG/ESMIG: Minimum security requirements for AMI components • SM-CG Sec0064: Smart Meters Co-ordination Group - Privacy and Security approach – part I (security requirements collected from different countries) • SM-CG Sec073: Smart Meters Co-ordination Group - Privacy and Security approach – part II (certification approaches) • SMCG_Sec0084: Smart Meters Co-ordination Group - Privacy and Security approach – Part III (clustering requirements to threats) • SMCG_Sec00103: Smart Meters Co-ordination Group - Privacy and Security approach – Part IV (minimum requirements)
Certification authority	Common Criteria Bodies in each country, e.g. BSI in Germany and NLCSA in the Netherlands.
Regulatory authority	members of SOGIS, members of the CC MRA, IECEE

Certification schemes/frameworks	Multiple (Dyryavyy, 2015b)

3.1.5 Virtual Power Plants

Description	Virtual Power Plants (VPP) balance their own power internally using a combination of controllable generation and load devices (such as wind turbines and solar panels, heat pumps and batteries) and contribute to the regulation of their external grid by absorbing and injecting energy in the power grid, while trading this commodity at the classic wholesale market. Additionally, they contribute to frequency control with ancillary services.
Candidate Products	• Virtual Power Plants • Balancing and control software • Communication devices
Documents	• VHP Ready Specification 3.0 (Vattenfall, 2014)
Certification authority	VHP Ready. The alliance will rely on independent accredited bodies to test compliancy of the VPP requesting connection
Regulatory authority	Currently there is no regulation
Certification schemes/frameworks	Each VPP that wants to participate in the scheme is required to undertake a certification process according to VHP Ready standard, and the standard contains cyber security aspects.

3.2 Findings

Within the energy sector the rise of ICT systems is eminent. IEDs, RTUs, data concentrators, data historians, and other devices communicate within the value chain all the way down to the customers, i.e. the (smart) meters. The supporting IT systems – the ones that facilitate both the production and distribution of electricity, and the sales and settlement of energy – are interconnected. The most important communication standards and interfaces in this area are: IEC 60870-5, IEC 61850, TASE.2/ICCP and DLMS.

3.2.1 Intelligent Electronic Devices (IEDs)

3.2.1.1 Certification drivers

- System criticality: is **high** because IEDs are installed in most substations and operate autonomously based upon locally acquired process information or via a local process controller. Remote commands issued from the central location are received through an interface between the central and remote location which implies that a third party can control the critical assets connected to the IEDs. So especially when multiple IEDs are compromised and malfunction this could cause local outages and even a complete blackout.
- Number of devices: **varies** based on the voltage level and capacity of the substation
- Safety issues: of **severe** impact because both a local outage and a blackout could cause several safety issues including interrupted life-support and dialysis machines, stopped elevators, electronic lock-ins, heating or cooling issues depending on the season.
- Security issues: of **severe** impact in case of a longer lasting blackout, as it could interrupt critical systems used for national security beyond the capacity of UPS's and emergency generators.
- Access vector: is **limited** because IEDs are normally not directly connected to public network infrastructures like the internet.

- Intersystem dependencies: are **high**, since data is communicated and sharing between IEDs, substations and control centers.

3.2.1.2 Findings

Station and process networks are normally designed as a standalone network. IEDs are interconnected within the same substation without direct connection to other systems outside the substation. Depending on the voltage level there is connectivity with the outside world using a RTU, gateway or proxy, this is done using public and private networks. Due to the standalone nature of the network the need for certification within the substation is **lower** as compared to the equipment connected to public infrastructures. Existing conformance test schemes do not include compliance testing of cyber security aspects on device level.

3.2.1.3 Recommendations

End-users would like to see that IEC 61850 is extended with specific parts related to security for IEDs (IEC 62351 and IEC62443 test procedures) and the used communication protocols instead of vendor specific solutions that prove to be non-interoperable. It is recommended that the UCA International Users Group (UCAIug) **incorporate testing cyber security aspects** on devices in the existing conformance test programs.

It is recommended for **asset management system to include records of the installed IEDs** with the current software/ firmware versions including the used configuration tools. Without this recording it is difficult to identify the systems that are exposed to a detected vulnerability and apply updates or execute replacement programs. Additionally, the maintenance organization will need to have skilled engineers that can **manage software/ firmware updates**.

An identified **good practice** is to **equip every substation network** with an IDS to monitor the network for unexpected activity or protocols.

3.2.2 Remote Terminal Units (RTUs)

3.2.2.1 Certification drivers

- System criticality: is **high** because RTUs act as a remote controller serving a control center which needs to perform actions in the remote location. When the connection between the central and remote location is compromised a malicious third party can gain access to the SCADA front-end and control the complete SCADA system or the station RTU and has access to critical assets within the connected substation and because malicious manipulation of the exchanged energy measurements can harm the whole network stability
- Number of devices: is **high** because almost all utilities use RTUs to monitor substations from a central location.
- Safety issues: of **severe** impact because both a local outage and a blackout could cause several safety issues including interrupted life-support and dialysis machines, stopped elevators, electronic lock-ins, heating or cooling issues depending on the season.
- Security issues: **severe** security issues in case of a longer lasting blackout, as it could interrupt critical systems used for national security beyond the capacity of UPS's and emergency generators.
- Access vector: is **high** because RTUs rely increasingly on communication over public network infrastructures. Public networks are significantly more accessible than private networks.
- Intersystem dependencies: are of **medium** size because RTUs are limited to the control of substations and power plants[7].

[7] Taking into consideration a scenario where a transmission operator balances the network upon regular measurements of the produced and consumed energy (for example like expected in the scenario of e-price).

3.2.2.2 Findings

Due to the standalone nature of substations and the network within the substation, cyber-security is currently not perceived as a must, but **attention is increasing** for it: electrical utilities are getting more and more aware of the risks associated with the use of public infrastructures for critical communication with SCADA and RTU systems. The providers of these products are following the developments of IEC 62351 and IEC 62443, several manufacturers of substation equipment including RTUs have started the implementation of these standards in their products. Many of these products are in the phase of being field-tested in pilot projects.

Compliancy test procedures are still under development and will contribute to higher level of device testing before massive deployment in substations (test procedures IEC 62351 and IEC 62443).

3.2.2.3 Recommendations

It is recommended that testing labs extend **test programs** to include **integrated system testing.**

A detailed network design before roll out is crucial to the level of cyber security of a substation network and thus the entire substation. **Manufacturers should invest more resources in improving security** of these RTUs due to the wide-spread character of these devices.

Identified **good practices** are the **use of IPSEC** between devices for a secure exchange of data, **segment the network** in smaller subnets and **isolate risk-areas** into one domain, **access control lists** and the **use of protocol convertors** on application level.

3.2.3 Smart meters

3.2.3.1 Certification drivers

- System criticality: is **low** because attacking a single meter does not influence the network. However, there might be a massive attack, where meters could push plenty of wrong data to Head End System. As such, they could be used to attack the central systems of the utility.
- Number of devices: **several millions** of smart meters are planned to be used in all households and non-industrial businesses. The meters are developed in a multi-vendor environment, to be deployed in all EU electricity grids. Interoperability is crucial to allow millions of devices to communicate, and the concept can be extended to the cyber security profiles.
- Safety issues: are of **severe** importance because some smart meter types have disconnect-switches. They can disconnect the end-user from the electrical grid. A massive which targets the disconnection of consumers combined with extreme climate situations, can lead to health issues or even deaths of elderly and sick people when air conditioning or heating systems are disconnected.
- Security issues: are of **medium** severity because alarm systems of private property could be disabled by tampering with a meter which includes breaker functionality.
- Access Vector: is **medium/high** because its connectivity depends on communication infrastructures in place. Meters could be connected directly to the Head End System via GPRS, CDMA, or LTE technology, or they could communicate (via power line carrier) to a Data Concentrator, which collects and sends the data to the Head End System via public network. In either case, public infrastructure is used due to the high number of devices. The meters are also equipped with a local interface for maintenance and in many countries, an interface for in-home devices or third party devices like in-home displays and local energy management systems.
- Intersystem dependencies: are **high** because several metering (sub)systems depend on the smart meter: The Head End System (i.e. the system that reads out the meters and collects the data) is connected to an MDM (meter data management system). The MDM is connected to GIS (Geographic information system), CRM (Customer Relation Management), and other systems. The energy consumption data collected and

transmitted by the meters is the source data to bill customers, provide network access and plays an important role in the settlement mechanism of the whole energy market.

3.2.3.2 Findings

Conformance testing of the application layer is performed under the oversight of the DLMS user association, while ESMIG and the SMCG are developing European specifications for smart meters and AMI. DLMS can be used with various communication technologies including ZigBee, 3G PLC and GPRS. The standardization and conformance testing of these communication technologies are managed by other standardization bodies.

The DLMS standard includes definitions of different security mechanisms for authentication, encryption and digital signatures.

3.2.3.3 Recommendations

It is recommended that the DLMS user association **actively updates and maintains** the official **conformance test tool** (CCT), since the tool set is often out date when compared to the latest revisions of the DLMS standard.

3.2.4 Advanced Meter Infrastructures (AMI)

3.2.4.1 Certification drivers

- System criticality: is **low** because attacking a single meter does not influence the network. However, there might be a massive attack, where meters could push plenty of wrong data to Head End System. As such, they could be used to attack the central systems of the utility.
- Number of devices: **several millions** smart meters are planned to be used in all households and non-industrial businesses. The meters are developed in a multi-vendor environment, to be deployed in all EU electricity grids. Interoperability is crucial to allow millions of devices to communicate, and the concept can be extended to the cyber security profiles.
- Safety issues: are of **severe** importance because some smart meter types have disconnect-switches. They can disconnect the end-user from the electrical grid. A massive which targets the disconnection of consumers combined with extreme climate situations, can lead to health issues or even deaths of elderly and sick people when air conditioning or heating systems are disconnected.
- Security issues: of **medium** severity because alarm systems of private property could be disabled by tampering with a meter which includes breaker functionality.
- Access Vector: is **medium** because its connectivity depends on communication infrastructures in place. Meters could be connected directly to the Head End System via GPRS, CDMA, or LTE technology, or they could communicate (via power line carrier) to a Data Concentrator, which collects and sends the data to the Head End System via public network. In either case, public infrastructure is used due to the high number of devices. The meters are also equipped with a local interface for maintenance and in many countries, an interface for in-home devices or third party devices like in-home displays and local energy management systems.
- Intersystem dependencies: are **high** because several metering (sub)systems depend on the smart meter: The Head End System (i.e. the system that reads out the meters and collects the data) is connected to an MDM (meter data management system). The MDM is connected to GIS (Geographic information system), CRM (Customer Relation Management), and other systems. The energy consumption data collected and transmitted by the meters is the source data to bill customers, provide network access and plays an important role in the settlement mechanism of the whole energy market.

3.2.4.2 Findings

The architecture of the smart metering infrastructure varies from country to country with the use of different applications (i.e. DLMS, Meters and More or OSGP), different communication technologies and different regulatory requirements.

3.2.4.3 Recommendations

Current conformance schemes are focusing solely on the smart meter side, and do not cover the other components inside the AMI. It is recommended that certification organizations extend the scheme **with test cases for DLMS based data concentrators and head-end-systems.**

3.2.5 Virtual Power Plants (VPP)

3.2.5.1 Certification drivers

- System criticality: is **high**, because both the flow of electricity and the related information is critical for the grid stability. Incorrect information from the VPP in regards to its generation could create instabilities in frequency control causing outages of the grid and cause a blackout due to unbalance.
- Number of devices: **varies** on the local electrical infrastructure
- Safety issues: of **severe** importance because a local outage could cause several safety issues including interrupted life-support and dialysis machines, stopped elevators, electronic lock-ins, heating or cooling issues depending on the season.
- Security issues: of **severe** severity in case of a longer lasting blackout, as it could interrupt critical systems used for local security beyond the capacity of UPS's and emergency generators.
- Access vector: is **high**, since VPPs communicate using the public infrastructure.

3.2.5.2 Findings

Currently the VHP ready standard is not mature and finalized yet, therefore there is currently no compliance scheme available. It is currently focusing on security rules and best practices imposed by other standards like IEC 62351.

3.2.5.3 Recommendations

It is recommended to **integrate the cyber security rules and standards** focusing on power systems, such as IEC 62351, in the VPP certification scheme.

4. Sector: Health Care

Healthcare environment is a vast ecosystem comprised by numerous components. Collaboration among various stakeholders, numerous interconnected assets and high flexibility requirements do not only lead to complexity and dynamics but also to blurred organisational boundaries. At the same time, personal health information is deemed even more valuable than financial information and, apart from access to sensitive information, access to prescription drugs or possession of expensive medical devices may also be considered worthwhile by attackers. Consequently, information security is a key issue for healthcare organisations.

To enable swift, correct and complete exchange of information both among specialists and physicians inside the hospital walls , and physicians with third parties (i.e. insurance companies), ICT is offering great variety of solutions and products. Both the patient data confidentiality and integrity are very important to ensure that the information is kept secure and only available to authorized parties while the data needs to be trusted and acted upon. Figure 3 gives an overview of the different components in the health care sector.

The ICT environment of the health care sector consists mostly of suysstems and devices to record, analyse and share information. However, mainly within hospitals, automation of clinical systems and medical equipment (OT) are available, to improve the health care provision to the patients.

Safety and availability are important factors for hospitals, and the increasing dependency on ICT systems, means that any failure will have a great impact on their operation.

Another major issue affecting cyber security in the case of healthcare is the lifespan of medical devices and equipment. Medical devices like CAT scanners, MRI machines etc can stay as part of a hospital for more than a decade. This means that new vulnerabilities arise as attackers become more sophisticated. Moreover this shows that intensive focus should be given in the patching and updating management of these devices. The very thin line between usability and security is becoming now more transparent as patching comes second (or even lower) in priority especially as the machines might need to be available at any given moment.

In the healthcare landscape the priority is the life of the patient; seldom are the cases were a physician would follow all the security procedures attached to medical devices if in case of emergency. These users are made to create workarounds and this was realized early enough. To increase safety and availability, many procedures were put in place to mitigate human errors and workarounds.

For all the reasons presented above standardization and the requirement for security certification in medical devices and systems will increase.

4.1 Desk Research

Within the health care sector, both data exchange and storage of health information are becoming increasingly important. . Inside a hospital many systems are interconnected in order to exchange information and patient's data; in some cases this can exceed the hospital's walls.

Contrary to the energy sector, the health sector has relatively limited (connected) OT systems as the main systems are administrative. The ICT landscape is complex due to the existence of various systems from multiple vendors and different lifespans. From this perspective, it is important having security certification in place to secure and protect the medical equipment, the patients' data and the administrative systems. Figure 3 shows a generic health care provision architecture with all relevant devices.

The following systems are considered the most favorable for security certification:

- Interconnected clinical information system, which include:
  - hospital information system,
  - lab information system,
  - picture archiving and control system
  - radiology information system,
  - pharmacy information systems,
  - pathology information systems,
  - blood bank and
  - research info system.
- Networked medical devices which include:
  - wearable medical devices,
  - Implantable medical devices,
  - stationary medical devices,
  - mobile medical devices,
  - supportive devices.

4.1.1 Interconnected clinical information system

Description	Large and complex information systems and tools which are the foundation of hospitals and medical institutes core administrative and medical-support processes. Every day these systems process many transactions in which data are entered, manipulated, and stored for both operational and informational purposes.
Products	Information systems and databases
Candidate products	Clinical networked information system (patients' databases)
Documents	• ISO 13485 • ISO 33716 • ISO 14971 • ISO 9001 • Medical Device Directive (MDD) 93/42/EEC • Canadian Medical Devices Conformity Assessment System (CMDCAS) • Medical Device Single Audit Program (MDSAP) • In Vitro Diagnostic Directive 98/79/EC
Certification authority	Certification is based upon national laws and directives.
Regulatory authority	Regulation is based upon national laws and directives regarding privacy and security of personal data.

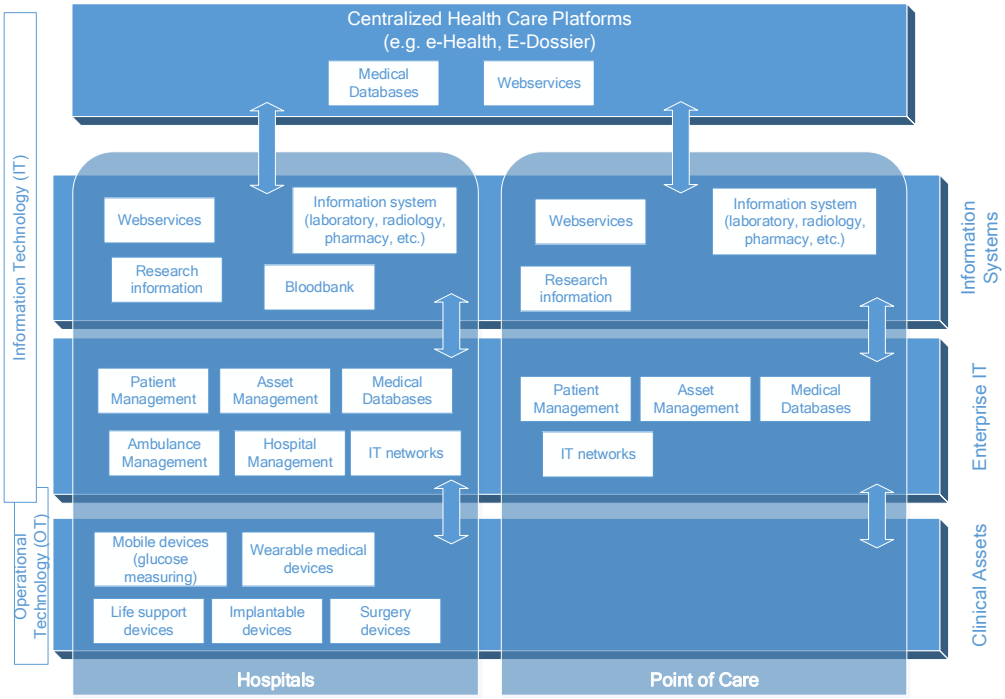

Figure 3 Global and simplified architecture Health Care

4.1.2 Networked medical devices

Description	Implanted chips, hearing aid devices, insulin pumps and other electronics used to regulate body processes will feature a data connection. Miniaturizing a communication module into such devices will be easy and will allow better monitoring and controlling of the health of the patient. Adding communication will make the device more vulnerable for remote connections that could lead to unwanted effects.
Products	• Pacemakers • Hearing aid devices • Valves
Documents	• ISO 13485 • ISO 33716 • ISO 14971 • ISO 9001 • Medical Device Directive (MDD) 93/42/EEC • Canadian Medical Devices Conformity Assessment System (CMDCAS) • Medical Device Single Audit Program (MDSAP) • Active Implantable Medical Devices 90/385/EEC
Certification authority	Certification is based upon national laws and directives.
Regulatory authority	Regulation is based upon national laws and directives regarding privacy and security of personal data
Certification schemes/frameworks	ISO 800001 UL 2900

4.2 Findings

Within the health sector the companies are more and more dependent on ICT. When ICT systems fail it is possible that hospitals cannot take in any patients anymore. Hospitals are more and more subject to ransomware infections. Furthermore, the medical equipment is also able to be connected to the IT network. Remote operation and monitoring improves the efficiency of the health care. It also implicitly creates extra risks to these medical devices. Safety and availability is important for hospitals and human errors are already mitigated by procedures. That means that standardization and the requirement for security certification will increase. That holds for the central databases and functionality as well. The lack of Role Based Access Control even if in the hospital terminals people having different roles can access the same data.

4.2.1 Interconnected clinical information system

4.2.1.1 Certification drivers

- System criticality: is **high** because the system contains all relevant information needed to run a hospital or a clinic
- Number of devices: is **limited** because the machines hosting the information are powerful and centralized.
- Safety issues: are of **high** importance because when information is tampered, altered or deleted this can lead to wrong decisions or no information on a patient.
- Access vector: is **high** because it is a pure IT system with many entry points and it is implemented via a public communications infrastructure

4.2.1.2 Findings

The criticality of the system is **high**, because unavailability has a direct impact on the provision of care, even in situations where protocols apply to work without access to the information system.

Database systems used in clinical networked information systems are based upon different technologies and providers, they do not share a common (architectural) model or interface between the different components, the lack of standardization leads to difficulties and additional costs when databases need to be integrated.

4.2.1.3 Recommendations

The definition of a common data-model and profiles regarding authentication and protection of data will realize an information system used by member states that allow a standardized way of data exchange.

4.2.2 Networked medical devices

4.2.2.1 Certification drivers

- System criticality: is **high** because attack on an implantable medical device has no direct impact on a larger system but only on the actual component
- Number of devices: are **many** because the use of this type of devices gets spread and common
- Safety issues: are of **high** importance because acting on the embedded application running in the device it will put the patient at risk
- Access vector: is **high** because communication interfaces are active and allow remote access

4.2.2.2 Findings

Many implantable medical devices have already wireless capabilities. Patients and care providers are becoming more and more security aware. Lack of standardization have triggered concerns and raised questions whether products fulfills safety and security standards like the ISO80001.

4.2.2.3 Recommendations

The basis for a secure product comes from good engineering practices and proper risk management, instead of focusing on device security the product developer shall be subject to applicable security and development standards like the Secure Software Development Life Cycle (SSDLC) approach (Davis, 2005).

5. Sector: Information and Communications Technology

The ICT sector's main products are software, including firmware, databases and digital certificates, and hardware such as routers, firewalls, switches, servers and workstations. The usage of these generic components is increasing at all (process) automation levels in all sectors, which is mainly due to cheaper prices and component standardisation. In the context of this report, the ICT sector can be divided in the following subsectors:

- Network device manufactures
- Chip manufactures
- Software manufactures
- Process automation software manufactures
- Support and maintenance companies

Unlike the rest of the sectors, ICT is not an essential service in itself in the terminology of NIS directive, but it supports other essential services. Accordingly, the ICT infrastructure can be considered as cross cutting component, since it delivers products and services to the other essential services. This requires specific certification criteria defined by these sectors, while within the ICT business area a lot of frameworks and standards exist that are widely used for development, maintenance, manufacturing and support activities. Therefore, it is important to understand that the scope of the ICT for this study is on end-products.

The ICT infrastructures used by different NIS essential services, heavily depend on network and computing equipment. The focus within this study will be on the (generic) network and computing devices produced within the ICT. In this study the widely accepted security requirements will be considered: availability, confidentiality, authenticity, and integrity.

5.1 Desk Research

For this study, ICT provides the necessary equipment and functionality to create the required automation in both the IT and OT world. ICT equipment, like network components and servers are more and more standardized and become cheaper and more powerful every year. The use of common ICT components is done at all levels within complex computing environments. Standardization of network communication is adopted at every automation layer and enables the possibility to interconnect components, systems and make the bridge between the OT and the IT world.

ICT components like routers and switches are critical for the correct operation of any system. Security certification on these impactful devices contributes to the overall security and reliability of the ICT system and the operational environment it supports. Furthermore, many applications and system depend on correct functioning encryption mechanisms, in order to use these systems, digital certificates need to be generated, maintained and managed. To create digital certificates which are compliant with relevant standards and can be safely used in any system made by any manufacturer the certification of Hardware Security Modules becomes relevant. ICT components that will require security certification are: switches / routers, firewalls, Hardware Security Modules, Unidirectional Network Systems and next generation firewalls.

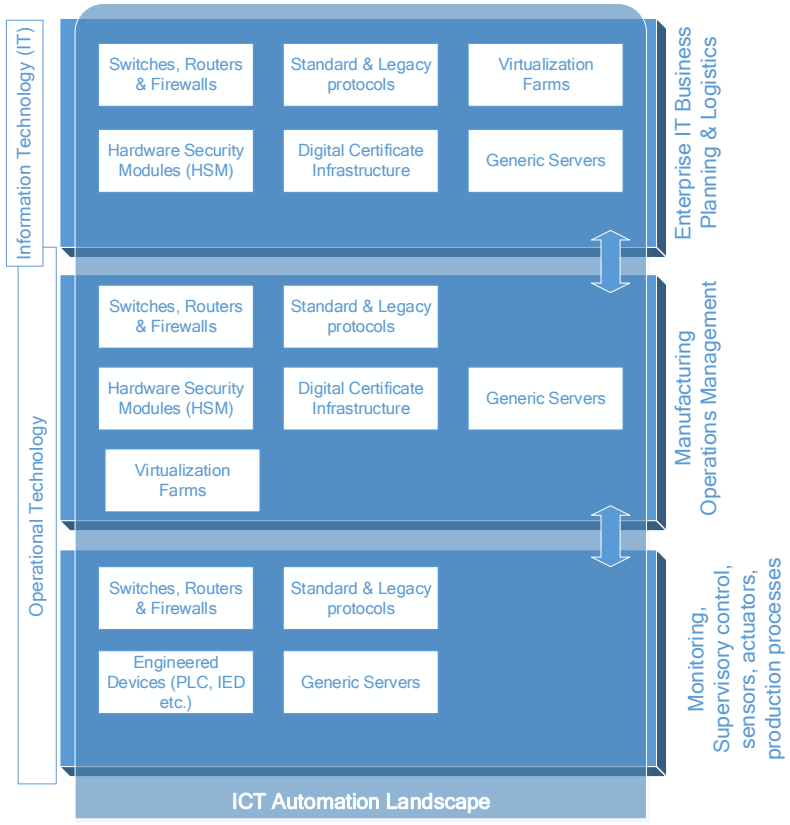

Figure 4 Global and simplified architecture ICT (based on ISA-95 / IEC62264)

5.1.1 Switches and Routers

Description	Switches and routers are essential complex infrastructure components which ensure fast and reliable inter-device communication and data exchange within the same and other networks.
Candidate products	Industrial switches and routers
Documents	• IEC 61850-3 • IEC 61850-90-4 • NERC CIP • RFC2196 • IEEE 802.1
Certification authority	Accredited test labs
Regulatory authority	Industry associations
Certification schemes/frameworks	Ad hoc conformance testing against layer 2 and layer 3[8] communication standards, self-certification

5.1.2 Firewalls

Description	Firewalls are devices used to monitor and control the incoming and outgoing network traffic based on predetermined security rules.

[8] According to OSI layered standard architecture

Candidate products	Industrial firewalls or switches/routers with firewall functionality
Documents	• IEC 61850-3 • NERC CIP • RFC2196 • IEEE 802.1 • ISO/IEC 15408
Certification authority	Accredited test labs and Common Criteria MRA members
Regulatory authority	Industry associations
Certification schemes/frameworks	Ad hoc conformance testing against Ethernet standards and applicable RFCs, Common Criteria, and self-certification

5.1.3 Hardware Security Modules (HSM)

Description	In the process of the generation of keys to be used in cryptography, dedicated hardware featuring crypto processors is used. As well as the generation function, covering a crucial function in the process of securing assets, this hardware normally offers very strong security measures, such as deletion of keys in case of tampering, backup, and redundancy. This hardware is a physical computing device that manages digital keys for strong authentication. It could be part of a Public Key Infrastructure (PKI).
Products	• Dedicated hardware • Plug-in card • External device attached to a computer or network server
Documents	• ISO/IEC 15408 • FIPS 140-2 • PCI Security Standards Council
Certification authority	Accredited test labs and Common Criteria MRA members
Regulation authority	Industry organizations or user groups
Certification schemes/frameworks	Common Criteria

5.1.4 Unidirectional Network System

Description	A unidirectional network device allows data to travel in one direction. The data is not able to travel the other direction, because it is physically not possible. Therefore, these devices provide more security and cannot be configured to pass the data in a bidirectional manner.
Products	• Data diode • Unidirectional network devices
Documents	• RFC 3077 • NERC CIP • ISO/IEC 15408
Certification authority	Accredited test labs and Common Criteria MRA members

Regulation authority	Industry organizations or user groups
Certification schemes/frameworks	Common Criteria

5.1.5 Next Generation Firewall

Description	A next generation firewall (NGF) is an integrated network platform. It combines a standard firewall with other types of network filtering functionalities, like an application firewall using deep packet inspection (DPI) and intrusion prevention system (IPS) for example. Furthermore, the device could be capable of deeper inspection compared to a traditional firewall such as encrypted data inspection (TLS/SSL), website filtering, malware and antivirus inspection.
Products	• Firewall • Routers • Switches • Computer systems
Documents	• ISO/IEC 15408 • FIPS 140-2
Certification authority	Accredited test labs and Common Criteria MRA members
Regulation authority	Industry organizations or user groups
Certification schemes/frameworks	Common Criteria

5.2 Findings

ICT provides the necessary equipment and functionality to create the required automation in both the IT and OT world. Common ICT equipment, like network components and servers are more and more standardized and become cheaper and more powerful every year. The use of common ICT components is done at all levels within a complex industrial environment.

Standardization of network communication is adopted at every automation layer and enables the possibility to interconnect components, systems and make the bridge between the OT and the IT world. Common ICT components like routers and switches are critical for correct operation of any system. Certification of these impactful devices contributes to the overall security and reliability of the OT and IT system.

Therefore, ICT infrastructure is considered to be a (critical) horizontal (cross sector) element which requires certification on a high level of trustworthiness. Delivery of ICT equipment, software and services to the rest of the business areas requires specific certification criteria defined within these areas. ICT area is large and diverse; therefore, it is important to narrow down the scope of ICT for the study.

The study focused on the following common ICT components that play a crucial role in the rest of the ICT landscape:

- Routers and switches
- Firewalls including next generation firewalls
- Unidirectional network system
- Hardware Security Modules
- Key generation software

- Digital certificates

More information on the specific findings related to the mentioned ICT components can be found below.

5.2.1 Routers and switches

5.2.1.1 Certification drivers

- System criticality: is **high** due to the fact that when switches are not working securely there will be no reliable and secure communication between devices or between networks which will endanger the stability of the supporting application or function.
- Number of devices: are **many** because every network requires one or more switches
- Safety issues: are **many** because insecure communications in an OT environment can lead to interruption of critical infrastructures or applications
- Security issues: are **many** because insecure communications in an OT environment can lead to interruption of critical infrastructures or applications
- Access vector: is **high** because the switch is reachable via the network
- Intersystem dependencies: are **high** because attacking a network switch or router all connected end-devices will be affected

5.2.1.2 Findings

There is **limited market demand** for certified networking equipment in OT environments on routers and switches to be tested and certified against specific security standards. Often the **only** mandatory requirements are to be suitable for industrial environments, the support of specific management protocols like SNMP and the support of encryption.

5.2.1.3 Recommendations

Incorporation of security standards in product certification and type-testing is essential to ensure that used network equipment is meeting cyber security standards. End-users also identified that security assessments (when equipment is in operation) to verify compliance to security standards is crucial. These assessments shall be periodically planned and executed and when changes to the system are made (for example firmware or configuration changes).

Furthermore, for network components a patch management system and procedures need to be in place, both at the vendor side and at the user side. Crucial to the stability and security of a complex system is also centralized monitoring and management.

5.2.2 Firewalls

5.2.2.1 Certification drivers

- System criticality: is **high** because remote access to a system or domain might not be possible anymore, but autonomous systems will remain available with access controls
- Number of devices: are **many** because private and public networks use firewalls to protect the network from attacks and to control who has access to the network
- Safety issues: are of **high** importance because remote control and operation will not be available due to an outage of the component but the stability and reliability of the connected systems will not be affected
- Security issues: are of **high** severity because the firewall controls the access to the network
- Access vector: **varies** depending on the network topology. Firewalls are connected to many different type of network infrastructures and have an effect on the overall stability of a complex system.
- Intersystem dependencies: are **high** because by attacking a firewall all connected end-devices will be affected

5.2.2.2 Findings

For firewalls the same conclusion applies to network switches and routers, there is limited market demand for certified network equipment in OT environments.

For firewalls patch management is also a critical issue, exploits are publicly available and therefore OT firewalls will require a faster patch cycle, this will have impact on the uptime and availability of the OT system.

There is **limited request from the market** to ask for routers, switches and firewalls to be tested and certified against specific security standards. Often the only mandatory requirements are to be suitable for industrial environments, the support of specific management protocols like Simple Network Management Protocol (SNMP) and the support of encryption.

5.2.2.3 Recommendations

Audits, functional testing and compliance testing of firewalls should be planned and executed together with other active network components, like the aforementioned switches and routers. There are risks that firewalls can be bypassed because of misconfigured switches and routers or even become unavailable due to high loads of network traffic in case of a Denial of Service (DOS) attack.

Audits on the existing rule base should be performed to ensure that all firewall rules are up to date, validated and functional before applying rules to production firewalls. Firewalls with build-in Intruder Detection Systems (IDS) and/or Intruder Prevention Systems (IPS) should be subject to the same audits, to reduce the risk of false positives due to less known OT traffic and/or protocols.

Make use of role-based-access to ensure that people or devices with access to the system cannot compromise the overall system. In case of a security-event only limited parts of the system are affected.

A good practice is to use different firewall brands or products for the IT and OT infrastructure, in case a vulnerability is detected this will not compromise the complete line of defense.

5.2.3 Hardware security modules

5.2.3.1 Certification drivers

- System criticality: is **high** because compromise of an HSM will reduce the trust to public key infrastructure supported by the keys issued by the compromised HSM
- Number of devices: is **high** because every device implementing cryptography might rely on an HSM to secure its applications
- Security issues: are of **high** severity because a comprised HSM reduces trust in the complete public key infrastructure
- Access vector: is **low** because HSM is a critical asset with limited access by unauthorized users
- Intersystem dependencies: are **low** for typical ICT infrastructures but very high for applications which use digital keys

5.2.3.2 Findings

Should an organization decides to deploy a PKI, then the correct design and setup of this infrastructure, including the HSM, becomes critical. In case of a security event related to the HSM the entire HSM needs to be replaced which is a major effort.

5.2.3.3 Recommendations

Failure of the HSM will lead to unavailability of the provision of digital keys. Therefore, it should be placed in a separate environment that can be accessed by a limited number of people. When used in critical process automation environments redundancy concept are needed to meet the availability requirements.

5.2.4 Unidirectional network system

5.2.4.1 Certification drivers

- System criticality: is **high** because unidirectional network devices are mostly used to secure, separate and protect critical networks, however compromising these devices will not lead to bi-directional communication due to the physical design of the hardware
- Number of devices: is **low** because separation and protection of network segments will require only two redundant unidirectional network systems
- Security issues: are of **low** importance because the device has physically blocked bi-directional data flow
- Access vector: is **low** because the device will operated in a protected environment with access by only be limited authorized persons
- Intersystem dependencies: are **low** because a unidirectional network system does not depend on other systems.

5.2.4.2 Findings

Unidirectional network devices are **not widely used** yet. Within critical automation environments these devices are used more and more to separate for example office networks from process networks.

5.2.4.3 Recommendations

Because of the emerging characteristic of the unidirectional network device, it is required to make sure it is **well designed** and bi-directional data must be made physically impossible. Appropriate configuring, testing and implementation is important. Before widely used it should be part of a certification plan while it plays an important part to secure interfaces of connected networks.

5.2.5 Next generation firewall

5.2.5.1 Certification drivers

- System criticality: is **high** because it provides more protection compared to a traditional firewall and protects against known and unknown attacks by monitoring the network traffic
- Number of devices: expected to be **many** because a next generation firewall (NGF) could be used in each network interconnection (for example in demilitarized zones (DMZ))
- Security issues: are of **severe** importance because a NGF is highly configurable and mistakes are easy to make, compromising this device could lead to undetectable attacks
- Access vector: is **low** because NGF is a critical asset with limited access by unauthorized users
- Intersystem dependencies: are **high** because by attacking a NGF all connected end-devices will be affected

5.2.5.2 Findings

A Next-Generation Firewall (NGFW) is an integrated network platform that is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS). The goal of next-generation firewalls is to include more layers of the OSI model, improving filtering of network traffic that is dependent on the packet contents (Rossi 2012).

Next generation firewalls provide a lot more protection and will be increasingly used within IT and OT networks. For operational systems, NGFWs could provide high detection of anomalies due to the fact the OT systems are highly predictable.

5.2.5.3 Recommendations

At least one of the firewall in the DMZ should be a next generation firewall. For operational systems this type of firewall could be used to detect anomalies. A NGF should be part of a continuous monitoring and update process to ensure the NGF meets all the operational and process requirements.

6. Sector: Transportation – Railway

The Railway sector's main activity is the transportation of passengers and goods using a fixed track infrastructure. The railway infrastructure usually is a shared common infrastructure that is used by different railway companies. Most railway infrastructures are able to provide electric power to the locomotive. Not all locomotives depend on electric power, they can also depend on diesel engines for example. A variety of trains can make use of this shared track.

Trains are vehicles operated by a driver or by automated systems in closed loop environments for example on airports. Currently, the railway sector uses the following ICT functionality to manage the transport:

- Central monitoring and control
- Safety systems
- Signaling and control systems
- Traffic control and communication
- Logistic optimization
- Passenger information (real-time)
- Ticketing, billing and check
- On-Board communication
- On-Board surveillance
- Asset management (vehicles and infrastructure)
- Digital tickets

Rail transportation contain large informational and operational systems. Informational systems used to provide their customers with real-time information. Operational systems are focused on the safety of the track to make sure no collisions will occur and obstacles are on the track. Within the passenger trains conductors need to check the valid passes of the passengers. Digital tickets are used more often which require a reliable and available infrastructure.

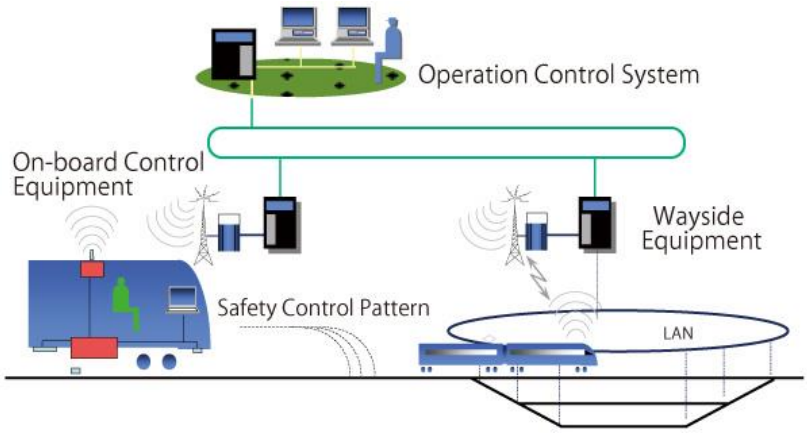

Figure 5 Overview of railway systems

Attacks on operational systems could lead to disruption or unavailability of the rail transport itself. When informational systems are attacked it can lead to unavailability of services for the passenger, like being unable to buy a ticket or digitally check a ticket into the system. Railway is an important way of transportation and could lead to disruption of the society.

Since transportation is part of the backbone supporting every country, many economies and business sectors will stop functioning without proper transportation in place. Consequently, cyber-attacks on transportation systems, which is a major threat, create a large impact on society and people's daily life. Besides direct effects, like delays, accidents, injuries or even deaths, it can lead to indirect effects, like socioeconomic effects. Currently there is no standardized approach to address security guidelines in the transportation sector. The NIS Directive addresses elements to reporting of cyber security related issues or events, but it does not address the matter of a standardized testing and certification approach.

6.1 Desk Research

The transportation sector consists of several subsectors like rail and maritime transport and aviation, and in all these sectors ICT plays an important role. The destruction of the transportation infrastructure will have immediate effect on people and economy. Figure 6 shows a general architecture of the rail transportation system. In the rail subsector the role of the infrastructure provider as well as the transportation company using the infrastructure are equally important to protect the subsector against cyber-attacks.

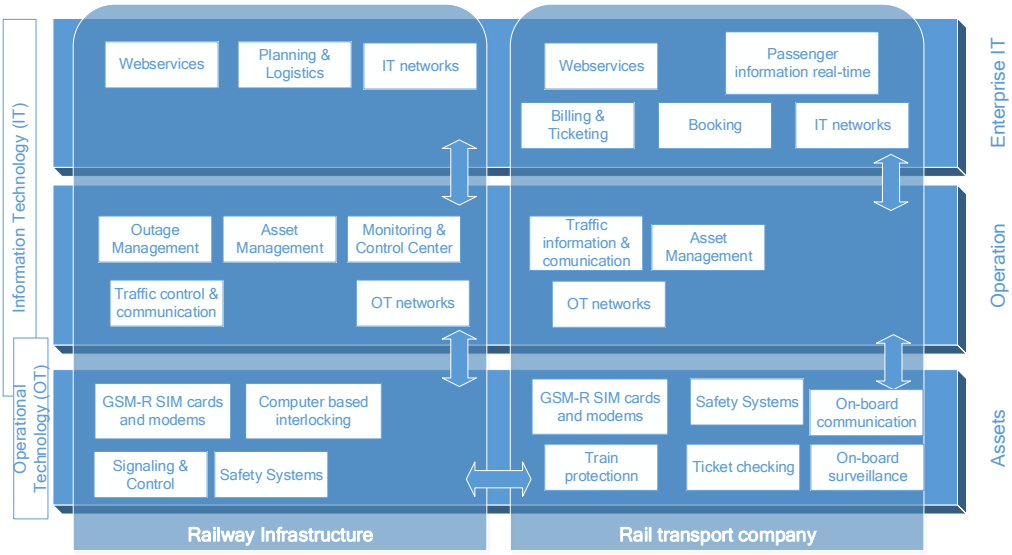

Figure 6 Global and simplified architecture rail transportation

The following devices are considered to be essential for a reliable and safe operation of the rail transportation, thus making them good candidates for certification:

- Automatic train protection
- Computer based interlocking
- GSM-R SIM cards and modems

6.1.1 Automatic train protection

Description	Automatic train protection (ATP) is installed in trains and along railroads to prevent collisions when the train driver is ignoring signals or not following the speed indications
Products	All industrial controllers are used as part of safety systems like ATP in the railway systems in the EU. The controllers allow for simple implementation of safety systems on PC-based solutions, like the train protection system SIBAS which is widely adopted for use in Europe.

Documents	Standards that are used in development work • EN 954-1 up to Cat. 4 • EN ISO 13849-1 up to PL e. • IEC 62061 up to SIL 3, • IEC 62443
Certification authority	AREMA, FRA, HMRI, IRSE, UIC
Regulatory authority	The authority of railway safety regulated at national level and on European level.
Certification schemes/frameworks	AREMA Communications & Signals Manual of Recommended Practices

6.1.2 Computer based interlocking

Description	Computer based interlocking (CBI) is a signalling system which has important safety function. It is designed to prevent the conflicting routes of trains.
Products	• SSI (Solid State Interlocking) • Mircrolok II • Smartlock • Alister CBI
Documents	Standards that are used in development work • NERC CIP AS • 61000-6-2 • AS IEC 61131 • AS ISO/IEC 27001 IT • AS ISO/IEC 27002 IT • AS ISO/IEC 18028 IT
Certification authority	Notified bodies such as • Lloyd's Register Verification Limited • ECA - ENTIDAD COLABORADORA DE LA ADMINISTRACION S.L. • BUREAU VERITAS • RINA Services • IIS CERT • VTT Expert Services • EISENBAHN-CERT • TÜV SÜD Nederland
Regulatory authority	ERTMS association, EU Agency for railways
Certification schemes/frameworks	Certification schemes are defined by the ERTMS association

6.1.3 GSM-R SIM cards and modems

Description	GSM-R SIM cards and modems are used in modern train systems to enable high-speed and bidirectional communication between traffic controllers and train drivers, delivers

	information about the train status such as speed and location. In theory it also could be used to make trackside signals.
Products	• GSM-R modems • Repeaters • Base stations • Mobile devices • SIM-cards
Documents	• GSM R FRS7.1 • GSM R SRS 15.1
Certification authority	GSM-R Industry group
Regulatory authority	Regulation regarding certification of communication equipment is defined on national regulation
Certification schemes/frameworks	GSMA

6.2 Findings

Within the broad area of transportation, several sub areas like land and rail traffic, maritime and aviation can be identified where ICT plays important and major roles.

The maritime sub area is highly standardized and legislated compared to the other sub areas. Logistics and planning systems play an important role within the maritime sub areas and here different ICT systems depend on always-on and real-time information delivery from connected components and other systems. Furthermore, the consistency and reliability of the information is of great importance.

In the rail sub area, the role of the infrastructure provider as well as the transportation company using the infrastructure are equally important to protect the sub area against cyber-attacks. The wellbeing and functioning of the city depends on a correct working transportation system.

6.2.1 Automatic train protection (ATP)

6.2.1.1 Certification drivers

- System criticality: is **high** because it takes care of critical transportation functions and malfunction may cause severe accidents which jeopardize human life or nature (in chemical transportation for example).
- Number of devices: is **high** because these systems are used all over in Europe
- Safety issues: are of **severe** importance because security vulnerabilities discovered can allow attacker to control railway automation which will jeopardize people safety and nature.
- Security issues: **many** security issues because system functionality can be modified or controlled by an attacker to cause an accident
- Access vector: is **high** therefore there are well known attack vectors, such as:
    - Safety system has several security weaknesses, including the ability to control the device without authentication, and the use of known protocols such as XML over HTTP, which makes it possible to create tools for controlling the device.
    - Product has fail-safe software controller which automation tasks include also fail-safe control functions and parallel data processing and the integration of the user's own technological functions. Devices used in railway systems can be exposed to attacks due to the use of default credentials because security features are not there or they are not taken into use, such as RCE vulnerabilities.

- Environmental issues: are of **severe** importance because if system is hacked or it cannot handle malware infection it might start to function wrong way and cause severe accident which might affect to nature as well in case of chemical transportation.

6.2.1.2 Findings

Industrial controllers are used as part of safety systems like ATP all over the railway systems in the EU. The controllers allow for simple implementation of safety systems on PC-based solutions, like the train protection system SIBAS which is widely adopted for use in Europe. The new ERTMS system make use of open standards and will gradually replace legacy systems in use within Europe.

6.2.1.3 Recommendations

ATP systems shall be evaluated via conformance testing and system testing to ensure the devices follow up the rules set up in standards. Automation systems securing needs also architectural based solutions like segregation and network flow surveillance (E.g. IDS), good configuration management, patching but also communication with other devices should be inspected carefully.

6.2.2 Computer based interlocking (CBI)

6.2.2.1 Certification drivers

- System criticality: is **medium** because attacks against CBI can be conducted by a malicious actor who has physical access to the system or by using social engineering.
- Number of devices: is **high** because devices are used all over Europe.
- Safety issues: are of **high** impact because when an attacker has knowledge about railway automation or routing protocols, access to the system can be reused to re-route trains and cause conflicting routes resulting in collisions are crashes.
- Security issues: are of **medium** severity because when the systems fail the driver is available to take control and prevent incidents.
- Access vector: is **high** because public networks are used
- Environmental issues: are of **high** impact because chemical train accidents might cause severe issues
- Intersystem dependencies: are of **medium** size.

6.2.2.2 Findings

Many standard off-the-shelf products are used, all running standard operating system hardware and using common communication protocols like TCP/IP, soap based web services. Adequate patch-management and version control are not in place.

6.2.2.3 Recommendations

Cyber security should be evaluated via conformance testing, penetration testing and inspected that devices follow up the rules set up in standards. Standards also should be different for automation devices than IT systems and environment. Automation systems are not set up same way as IT systems and their configuration, and communication with other devices should be inspected carefully.

Adequate cyber security training and information security awareness should be conducted regularly, to take care of password policies and avoid human based mistakes. Device security testing and overall system hardening to prevent attack vectors need to be done.

6.2.3 Communication equipment based upon GSM-R

6.2.3.1 Certification drivers

- System criticality: is **high** because the communication is the backbone for all other connected systems in or around the trains
- Number of devices: **many** devices that are installed within Europe
- Security issues: are of **high** severity because of the number of devices in the field a vulnerability will have a major impact
- Access vector: is **medium** because the networks are operated privately and there is limited connectivity with public infrastructures
- Environmental issues: are **many** because any intentional or unintentional cyber related activity can jeopardize safety if vulnerability in system can cause malfunction and affect to train operations. However, if connection is lost it stops train
- Intersystem dependencies: are **high** because an attack via other systems such as via mobile phones is possible but European Train Control System (ETCS) automatically stop if the connection between the train and the control center is interrupted

6.2.3.2 Findings

GSM-R SIM cards and modems are used to connect trains to control centers and therefore have important role in security. Even though SIM cards are encrypted it is always possible to cause jamming attack in order to prevent train and the control center communication[9]. For example, a train using the European Train Control System (ETCS) will stop if the connection is lost between train and control center. This can cause issues when the train start moving again with wrong time schedules and cause a collision. Furthermore, the lack of policies or best practices on using non-standard PIN are problematic, when the default PINs are used and devices are managed via SMS it is easy to get access.

Firmware updates cause another risk, in GSM-R devices. Also the firmware can include hardcoded private keys for SSL certificates and remote admin rights when a man-in-the-middle type attack can be done. Also key management will cause security issues. Because there are modems used for GSM-R that could also be vulnerable to the types of mobile phone type of attacks.

6.2.3.3 Recommendations

Even though systems were separated from the Internet, security holes, wrong configuration and inadequate hardening might offer attack vector, also radio frequency type attacks are possible to conduct if weak encryption is in use.

Proper version and configuration management systems shall be in place, together with PIN management to avoid the problematic use of standard PIN codes.

It is important to evaluate railway systems security as a whole, because weaknesses in communications between other trains might cause collisions. Even though systems were separated from the Internet, security holes, wrong configuration and inadequate hardening might offer attack vector, also radio frequency type attacks are possible to conduct if weak encryption is in use.

[9] Vulnerabilities in GSM-R have been extensively covered by the 32C3 conference talk “The Great Train Cyber Robbery", 27/12/2015, available at http://www.slideshare.net/AlexanderTimorin/the-great-train-cyber-robbery-scadastrangelove.

7. Sector: Transportation – Water transport

The water transport area consists of offshore and onshore systems which include management, communication systems and operational systems that perform navigational and automation purposes. Within this report, the focus is given to the vessel within the Maritime sector. Figure 7 gives an overview of the vessel's systems and its onshore connection. In a sense the ship behaves as a floating island operated through interacting IT and OT systems. A large variety of systems are required, such as electric power generation, electric power distribution, vessel motion control, automatic navigation track-keeping, safety systems, stability systems, IT networks, control (OT) networks, internet connection, etc. The combination of these different systems makes it a complex computing environment.

Shipping of goods within Europe is still increasing and represents more than half of the maritime transport that is carried out. Furthermore, maritime shipping increasingly relies on ICT to optimize operations and enable essential maritime operations; navigation, propulsion, traffic control management, etc. Due to the increasing ICT, the maritime sector becomes more vulnerable to cyber threats. As the maritime area is critical for the European society (2016/1148/EU), significant cyber-attacks could lead to disastrous consequences on the safety, economics and the European economy.

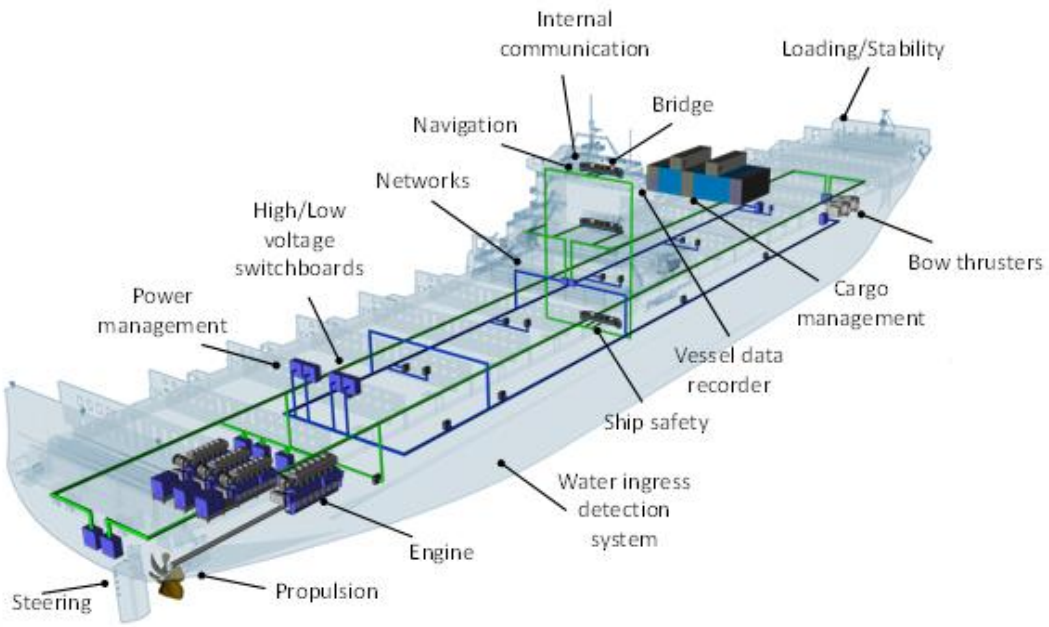

Figure 7 Overview of systems on a vessel

The maritime industry is continuously driving towards an increase the availability, security and reliability of the software dependent systems, cyber security **recommended practices** have recently been published, describing the first steps towards performing risk-based assessments of cyber security for the maritime assets (Dyryavyy, 2015a). Existing standards and recommendations can give a certain level of cyber security resilience of on-board systems.

7.1 Desk Research

The maritime sector has been selected as a study focus on the vessels systems. Figure 7 shows a general architecture of a vessel system. It shows the different devices needed for a safe and reliable operation. A vessel contains a diverse variety of different systems, ranging from power management to propulsion and from navigation to entertainment

systems. The information technology and operational technology is increasingly interconnected. This brings more risk of unauthorized access to these systems. Safety, environmental and commercial consequences of a cyber incident may be significant. On board systems could include (Bimco, 2016):

- Cargo management systems
- Bridge systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communication systems

Each of these systems play an important role on a vessel. Failure or compromising one of these systems can have severe consequences. These systems could be considered for certification. The following four systems have been selected for the focus of this study:

- Integrated Bridge Systems (allows centralized monitoring and various navigational tools)
- Cargo management systems
- Passenger servicing and management systems
- Propulsion and machinery management

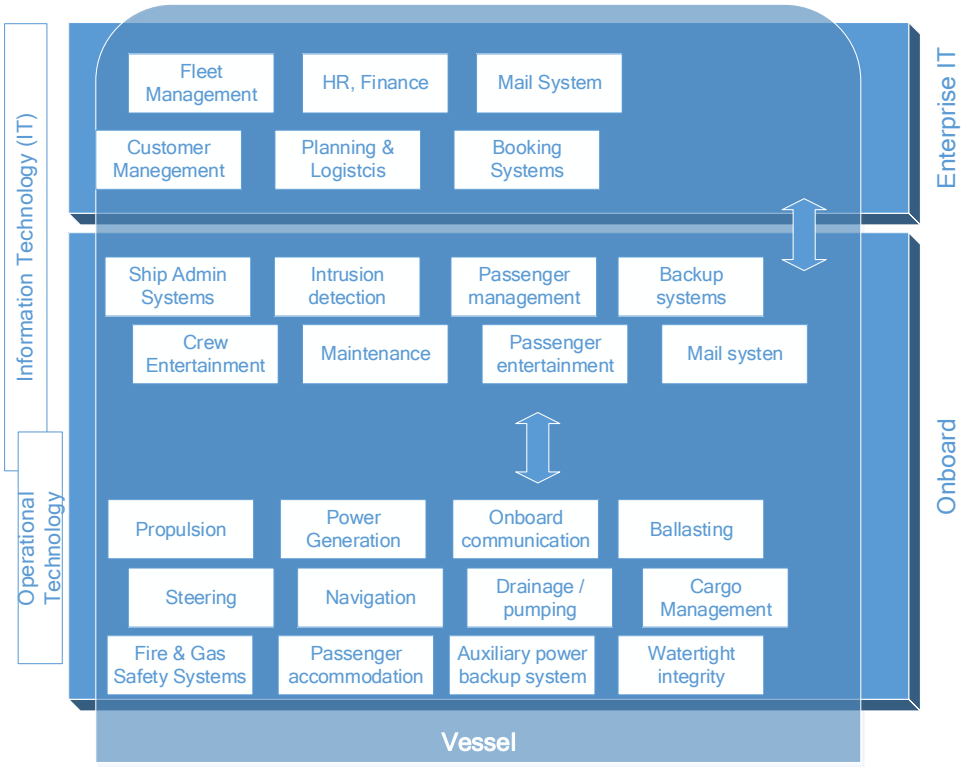

Figure 8 Global and simplified architecture maritime vessel

7.1.1 Integrated Bridge Systems

Description	Integrated Bridge Systems (IBS) is a combination of systems that are interconnected. Allowing centralized monitoring of various navigational tools. IBS acquired and control sensor information such as passage execution, communication, machinery control and safety and security. It is a navigation system that links other systems to provide all details belonging to the ship's navigation at one place. These other systems include Electronic Chart Display and Information System (ECDIS), Global Navigation Satellite (GNSS), Automatic Identification System (AIS), Voyage Data Recorder (VDR) and Radar/ARPA (Automatic Radar Plotting Aid).
Products	• Electronic Chart Display and Information System (ECDIS) • Global Navigation Satellite (GNSS) • Automatic Identification System (AIS) • Voyage Data Recorder (VDR) • Radar/ARPA (Automatic Radar Plotting Aid).
Documents	• DNVGL-RP-0496 (DNV-GL, 2016) • BIMCO guidelines (Bimco,2016) • BSI-Standards • ISO 27001/27002/27005 • ISO 1069:1973 • IEC 62443 • IEC 62351
Certification authority	Certification is based upon national and international standards and regulation and execution by certification labs such as DNV GL, Bureau Veritas, Lloyds Register, ABS, TÜV
Regulatory authority	Regulation is defined on national level
Certification schemes/frameworks	• ISO 27001/27002/27005 • DNVGL-RP-0496 • IEC 62351

7.1.2 Cargo management systems

Description	The cargo management system is used for the management and control of the cargo. This digital system could interface with a variety of systems ashore. It may include shipment-tracking tools that is available via the internet to shippers. A real-time system that makes sure the cargo is administered correctly and no unauthorized cargo can be loaded.
Products	• Dedicated applications • Web-based applications
Documents	• ISO 27001/27002/27005 • IEC 62443 • IEC 62351 • BIMCO Guidelines • BSI-Standards • ISO 8431:1988

Certification authority	Certification is based upon national and international standards and regulation and execution by certification labs such as DNV GL, Bureau Veritas, Lloyds Register, ABS, TÜV
Regulatory authority	Regulation is defined on national level
Certification schemes/frameworks	• ISO 27001/27002/27005 • DNVGL-RP-0496 • IEC 62351

7.1.3 Passenger servicing and management systems

Description	Information systems used for property management, boarding and access control. This system could hold valuable passenger related information. Critical system that makes sure authorized people can only access the ship.
Products	• Reservation and booking system
Documents	• ISO 27001/27002/27005 • IEC 62443 • IEC 62351 • BIMCO Guidelines • BSI-Standards
Certification authority	Certification is based upon national and international standards and regulation and execution by certification labs such as DNV GL, Bureau Veritas, Lloyds Register, ABS, TÜV
Regulatory authority	Regulation is defined on national level
Certification schemes/frameworks	• ISO 27001/27002/27005 • DNVGL-RP-0496 • IEC 62351

7.1.4 Propulsion and machinery management

Description	This operational system is used to monitor and control on board machinery, propulsion and steering. It is responsible for the motion of the vessel and gives the captain the possibility to fern the ship.
Products	• RTU • PLC • Front-end servers • SCADA
Documents	• ISO 27001/27002/27005 • ISO 13613:2011 • ISO 14885:2014 • IEC 62443 • IEC 62351 • BIMCO Guidelines • BSI-Standards

Certification authority	Certification is based upon national and international standards and regulation and execution by certification labs such as DNV GL, Bureau Veritas, Lloyds Register, ABS, TÜV
Regulatory authority	Regulation is defined on national level
Certification schemes/frameworks	• ISO 27001/27002/27005 • DNVGL-RP-0496 • IEC 62351

7.2 Findings

Within the broad area of transportation, several sub areas like land and rail traffic, maritime and aviation can be identified where ICT plays important and major roles.

The maritime is well regulated internationally and uses international established standards and guidelines on operational, design and safety topics. Logistics and planning systems play an important role within the maritime sub areas and here different ICT systems depend on always-on and real-time information delivery from connected components and other systems. Furthermore, the consistency and reliability of the information is of great importance.

During the recent years, an increase of cyber-attacks has been observed within the Maritime transportation industry. Although there has not been a catastrophic event to this date, stakeholders have taken on the task to assess this emerging threat.

As mentioned in the 2011 ENISA study (ENISA, 2012) a **holistic risk-based approach** is recommended, which would require the assessment of existing cyber risks associated with the current ICT systems implementations relevant to the European maritime sector as well as the identification of all critical assets within this sector. For maritime economic operators and stakeholders, it is important to proactively apply sound cyber and information security risk management principles within their organizations and environments.

7.2.1 Integrated Bridge Systems

7.2.1.1 Certification drivers

- System criticality: is **high** because this system provides the navigational functionality of the ship
- Number of devices: one per vessel (is an aggregate of several other navigational systems)
- Security issues: expected to be **high** because it is a networked navigation system with interfaces to shore side interfaces for updates which make this system vulnerable for cyber attacks
- Access vector: expected to be **high** because all navigation systems within the same network are potentially accessible by external actors either for maintenance of the software or simply has open ports.
- Intersystem dependencies: are **high** because all associated systems for navigation will be affected like ECDIS, GNSS, AIS, VDR and Radar/ARPA

7.2.1.2 Findings

An integrated bridge system (IBS) is a combination of interconnected systems to allow centralized access to sensor information or monitoring/control from workstations. The aim is to increasing the safety and efficiency of the ship's management. The details for each system boil down to integrated entities such as ECDIS, GNSS, AIS, VDR and Radar/ARPA ECDIS, GNSS, AIS, VDR and Radar/ARPA.

7.2.1.3 Recommendations

As several navigational systems are integrated in this one integrated bridge concept, it is recommended to perform security testing before delivery of the vessel or during operations if this step has not been performed. Software

components necessary for the operation of the integrated bridge system should be managed under configuration in a manner to keep track of software updated and any changes to the security configuration.

7.2.2 Cargo management system

7.2.2.1 Certification drivers

- System criticality: is **high** because it performs the management and control of the cargo including hazardous cargo
- Number of devices: one system per vessel
- Security issues: are of **high** importance because unauthorized persons could add see which (container) cargo was loaded and subject to targeted high jacking. Other types of cargo such as LNG would pose other hazardous threats when these dedicated types of cargo management systems would be tampered with.
- Access vector: is **high** because the cargo system could be connected to shore-side cargo. However, the access vector for onboard cargo management systems for bulk type cargo is limited as it is not normally connected to the onshore systems.
- Intersystem dependencies: are **low** because only the cargo management of the vessel will be affected. However, information exchange with onshore system will exist.

7.2.2.2 Findings

In this section we opted to flag a publicly known incident known as the "Roman Holiday" (Szymanski, 2016): involved an undisclosed global shipping conglomerate contacted the Verizon RISK Team after they became alarmed at a series of attacks where the pirates were armed with very specific information in terms of the cargo onboard the vessel. Attackers initially had uploaded a malicious Web shell to the shipping company's Content Management System (CMS) server, which manages shipping inventory and bills of lading for its ships. "The threat actors used an insecure upload script to upload the web shell and then directly call it as this directory was web accessible and had executed permissions set on it". This incident highlights the cargo/content management system to be important for the safe and reliable transport operations.

7.2.2.3 Recommendations

Onshore Content Management systems should be in the scope of certified IT security management system, to be audited and security tested.

7.2.3 Passenger servicing and management systems

7.2.3.1 Certification drivers

- System criticality: is **high** because it provides boarding and access control holding passenger related information, as well as property management
- Number of devices: one on a vessel
- Security issues: are of **high** severity because compromising this system could lead to unauthorized access and boarding
- Access vector: is **high** because several systems are needed to fulfill the functionality and it could be that it interfaces with the internet so passenger are able to check in at home for example
- Intersystem dependencies: **low**

7.2.3.2 Findings

IMO mandatory requirements for the electronic exchange of information on cargo, crew and passengers have been adopted by the International Maritime Organization (IMO) on 11/04/2016. These include standardized forms for the maximum information required for the general declaration, cargo declaration, crew list and passenger list; and agreed essential minimum information requirements for the ship's stores declaration and crew's effects declaration. Although standards and recommended practices relating to stowaways are updated to include

references to relevant sections of the International Ship and Port Facilities' Security (ISPS) Code, the ISPS audits do not currently address the cyber security aspect of the electronic passenger lists.

7.2.3.3 Recommendations

Passenger management systems should be in the scope of IT security management policies to be audited and security tested against cyber security standards and IMO/ISPS code.

7.2.3.4 Propulsion and machinery management

7.2.3.5 Certification drivers

- System criticality: is **high** because it initiates the movement of the ship as commanded by captain
- Number of devices: one on each vessel
- Security issues: are of **high** importance because an attacker could control a ship when the system is compromised
- Access vector: is **low** because this system is normally not connected to systems outside the vessel
- Intersystem dependencies: are **high** because this system is interconnected to bridge monitoring systems

7.2.3.6 Findings

Currently there are various research projects aiming to connect the ship's machinery to sensors in order to improve maintenance using Condition Based Maintenance Systems. This may lead to new types of shore based connections which would need to be further evaluated in the future in order to consider the need for cyber security related certifications. Nevertheless, currently machinery and propulsion systems are subject to software upgrades and software obsolescence. Furthermore, there are projects working on autonomous and even unmanned ships that increase the information exchange with onshore system.

7.2.3.7 Recommendations

As software destined for propulsion systems can become obsolete and thus not upgraded to address newly found vulnerabilities, it should be designed following a defined obsolescence management policy. Network storming tests could be a means to check for robustness and segregation practices should be used in order to isolate machinery and propulsion networks from other non-operational networks. If vendor support remote maintenance must be used, then strong security policies should be applied to remote maintenance operations.

8. Conclusions

The main research aim of this study was to provide the decision makers with a thorough description of the cyber security certification status concerning the most impactful equipment in different critical sectors, and to pave the way towards a more harmonized approach to cyber security certification in EU based on the results of this study. This has been performed by undertaking desk research and interviews with experts to answer the several research questions. Based on the results, findings and recommendations have been presented for each sector.

Here we conclude by presenting common findings which apply to multiple or even all sectors, and are related to using public or private infrastructures and testing of complete systems versus component testing. For each common finding a recommendation is provided. Next, key recommendations are described. Finally, a table is presented providing a clear overview of candidates for certification that should contribute to the agenda to work towards a more harmonized approach to cyber security certification in EU.

8.1 Common Findings

The table below provides the common findings and recommendations:

COMMON FINDING	RECOMMENDATION
In each sector the use of **privately owned infrastructures** for data communication between components or complete systems is considered more secure, however public infrastructures are widely used. The use of these public infrastructures introduces additional challenges to a system.	**Asset owners should take mitigating measures** such as the use of separated APNs when using public cellular networks, VPNs when non-dedicated links are used and additional encryption and authentication.
Furthermore, it was identified that although on component level **standalone certified devices** are considered trustworthy, this **might** not be the case after their integration in a real computing environment, causing proper planning and execution of system tests to be critical. Device certification will **help** to get a generic base line of device quality in terms of cyber security requirements. However, it should be noted that 100% guarantee does not exist when it comes to cyber security of complex computing systems.	Certificate issuing bodies should issue certificates which state that the component is certified as having certain security capabilities built-in the given device, but **cannot be used** as a guarantee that this device is used (configured) correctly.
When it comes to building cyber security resilience in the selected sectors, it is observed that a small part of the security will be supported by the components or devices that compose the systems while the larger part of the security will depend on the processes and procedures that are in place.	Organisations should consider the **security certification of the process** as the **highest** priority in the whole business chain (Dyryavyy, Y., 2015b).
Another important observation is the **increased outsourcing** of specific cyber security relevant tasks or functions, which will also increase the risk of being vulnerable to cyber-attacks.	Customers should verify that external (third parties) service providers, have all the **required knowledge level** in the own organization before entering any contractual agreement with them. This way they will make sure that the specific domain (for example substation

	automation) is known and understood by those delivering the essential cyber security services.
This study focuses only on critical components that are good candidates for cyber security certification. An **overall concern** is the use of devices like laptops, tablets and phones as entry points for potential attacks or malware. This is a cross-section threat where components connected to complex and critical systems are mostly unmonitored and can cause serious danger to the overall stability of such complex system. It should be stated that cyber security certification is as important for design, implantation, configuration, operational and business processes.	Owners of critical infrastructures should take a **holistic approach** that provides a certain level of security assurance at every level of the business value chain instead of merely focusing on the component level.

8.2 Overview findings of the given devices per sector

The table below presents a clear overview of candidates for certification that should contribute to the agenda to work towards a more harmonized approach to cyber security certification in EU.

Overview findings of the given devices

Legend	Certification drivers	Actual market situation	Recommended for certification
⊕⊕	Strong drivers	Mostly certified	Strongly
⊕	Positive drivers	Partly certified	Positively
-	Neutral	No certification	Neutral
⊖	Negative drivers	Limited demand	Not recommended
⊖⊖	Strong negative drivers	No demand	Strongly not recommended

COMPONENT	CERTIFICATION DRIVERS	MARKET SITUATION	RECOMMENDED FOR CERTIFICATION	RECOMMENDATIONS
Routers & Switches	⊕⊕	⊖	⊕⊕	Incorporation security standards in product certification and type-testing is essential.
Firewalls	⊕	⊖	⊕⊕	Same as routers and switches. Use of different firewall brands and role-based access.
Hardware security modules	⊕⊕	-	⊕	Required to be deployed in a separate environment.
Unidirectional Network System	⊕	⊕	⊕	Ensure meeting core requirements requires well design and proven secure engineering method.
Next generation firewalls	⊕	⊕	⊕	Use NGF besides existing firewalls to detect unknown traffic and usage patterns.
Smart meters	⊕⊕	⊕	⊕⊕	Usage of the DLMS in combination with TLS and IEC 62351 to secure the communication.
Intelligent Electronic Devices	⊕⊕	⊖⊖	⊕⊕	Best practice is to equip every substation with IDS to monitor unexpected activity and protocols.
Remote Terminal Unit (RTU)	⊕⊕	⊖	⊕⊕	Detailed network design crucial for cyber security of entire substation.
Advanced meter infrastructure (AMI)	⊕⊕	⊖	⊕	Extend existing certification schemes with test cases for data concentrators and head-end systems.
Virtual power plants (VPP)	⊕⊕	⊖⊖	⊕⊕	Develop certification scheme based on existing smart-meter and substation automation schemes.
Integrated Bridge Systems (IBS)	⊕	-	⊕	Apply configuration and software change management/tracking on software components

Cargo management systems	⊕⊕	-	⊕	Apply network segregation and audit onshore tracking systems against strict security policies
Passenger servicing systems	⊕⊕	-	⊕⊕	Should be security tested to ensure remote tampering possibility is reduced to a minimum.
Propulsion and machinery system	⊕⊕	-	⊕⊕	Apply network segregation and firewall hardening. Software should be managed for obsolescence.
Sector: Transport - Railway				
Automatic train protection (ATP)	⊕⊕	⊖	⊕	Recommended to ensure to follow rules of the standards.
Computer based interlocking (CBI)	⊕⊕	⊖⊖	⊕⊕	Using conformance and penetration testing of devices against applicable standards.
Communication equipment GSM-R	⊕⊕	⊖	⊕⊕	Important to evaluate railway system security as a whole and harden the equipment.
Sector: Health care				
Clinical information systems	⊕⊕	⊕	⊕⊕	Definition of common data-model and profiles for authentication and protection of data.
Implantable medical devices	⊕⊕	⊖	⊕⊕	Focus on security and development standards like Secure Development Life Cycle (SSDLC).

8.3 Key Recommendations

The following general key recommendations are determined for the manufacturers and the users of the certificates:

- Organisations should strive for certifying their management system because it is a powerful tool that helps companies to achieve their business goals. **Process certification and compliance is vital** to support product quality, and it is often a ticket to the market. For markets large enough, product manufacturers can test and certify their products only once as they can have them accepted in many other markets or countries thereafter.
- Both vendors and asset owners should take a holistic view when it comes to security certification and not merely focus on the functional element of the devices they use. Only after **verification** of a system in its entirety, including procedures for operation and maintenance, it can be considered **cyber secure**.
- Organisations should invest more on improving the cyber security education of their engineers. This is because they usually do not have cyber security culture as they are often confronted with new technologies, or other domains unknown to them, until it is too late to adopt mitigation measures. Therefore, they need to be educated, to become aware of cyber risks and to realize that the system is as strong as each individual component, and that actions and decisions taken for a sub-part of the system can have a major impact on the overall performance of the system itself.
- Cyber security service providers are recommended to implement an IT service management framework in their organizations as a proof that their services meet customers' needs.
- Whenever this is financially justified, customers should look for the use of security service providers who provide a **follow-the-sun support** team in order to ensure maximum availability of their services.

Furthermore, they should seek for security service providers with an IT service management system which is based on international and widely known standards e.g. ITIL, ISO/IEC 20000 etc.

9. List of abbreviations

AIS	Automatic Identification System
AMI	Advances Meter Infrastructure
ARPA	Automatic Radar Plotting Aid
ATP	Automatic Train Protection
CA	Certification Authority
CBI	Computer Based Interlocking
CC	Common Criteria
CCT	Conformance Test Tool
CDMA	Code Division Multiple Access
CIP	Critical Infrastructure Protection
CMDCAS	Canadian Medical Devices Conformity Assessment System
CRM	Customer Relation Management
DDOS	Distributed Denial Of Service
DLMS	Device Language Message Specification
DMS	Distribution Management System
DMZ	Demilitarized Zone
DPI	Deep Packet Inspection
DOS	Denial Of Service
DSO	Distribution System Operator
ECDIS	Electronic Chart display and Information System
EMS	Energy Management System
EU	European Union
GIS	Geographic Information System
GMS	Generation Management System
GNSS	Global Navigation Satellite
GPRS	General Packet Radio Service

GSM	Global System for Mobile
HE	Head End
HSM	Hardware Security Modules
IBS	Integrated Bridge Systems
ICCP	Inter-control Center Communication Protocol
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IDS	Intrusion Detection System
IMO	International Maritime Organization
IPS	Intrusion Prevention System
IPSEC	Internet Protocol security
ISPS	International Ship and Port Security
ISO	International Organization for Standardization
IT	Information Technology
LTE	Long Term Evolution
MDD	Medical Device Directive
MDM	Meter Management System
MDSAP	Medical Device Single Audit Program
NERC	North American Electric Reliability Corporation
NGF	Next Generation Firewall
NIS	Network and Information Systems
OT	Operational Technology
PC	Personal Computer
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
RFC	Request for Comments
RTU	Remote Terminal Unit

SCADA	Supervisory Control And Data Acquisition
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SSDLC	Secure Software Development Life Cycle
SSI	Solid State Interlocking
SSL	Secure Socket Layer
TASE.2	Telecontrol Application Service Element 2
TLS	Transport Layer Security
TSO	Transmission System Operator
UPS	Uninterruptible Power Supply
VDR	Voyage Data Recorder
VHP	Virtual Heat & Power
VPP	Virtual Power Plant

10. Bibliography/References

2016/1148/EU, "Directive concerning the measures for a high common level of security of network and information systems across the Union," July 2016, European Parliament and the Council of the European Union, Official Journal of the European Union L 194/1, 19 7 2016, available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. [Accessed 14 10 2016].

Bimco, "The guidelines on Cyber Security Onboard Ships," BIMCO, February 2016, available: https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf. [Accessed 14 12 2016].

COM(2006)786 final, "Communication on a European Programme for Critical Infrastructure Protection," December 2006, Commission of the European Communities, Communication from the Commission, Brussels, 2006, available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF. [Accessed 14 11 2016].

Davis, N., “Secure Software Development Life Cycle Processes: A Technology Scouting Report”, Software Engineering Institute, December 2015.

DNV-GL, "Recommended Practice Cyber Security Resilience for ships and mobile offshore units in operation," DNV GL Maritime, Septemebr 2016, available: https://www.dnvgl.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585. [Accessed 14 10 2016].

Dyryavyy, Y., (a) "Research Insights - Sector Focus: Maritime Industry", NCC Group, 2015, available: https://www.nccgroup.trust/uk/our-research/research-insights-volume-4-sector-focus-maritime-sector/ . [Accessed 14 10 2016].

Dyryavyy, Y., (b) "Cyber Security for the Modern Day Marine Sector," NCC Group, 2015, available: https://www.nccgroup.trust/uk/our-solutions/your-sectors/maritime/ . [Accessed 14 10 2016].

JOIN(2013) 1 final, "Communication on cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace," February 2013, European Commission and the European Union for Foreign Affairs and Security Policy, Brussels, 2013, available: https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace. [Accessed 16 10 2016].

ENISA, "Analysis of cyber security aspects in the maritime sector," European Network and Information Security Agency (ENISA), 2012, Heraklion, Greece, 2011.

ENISA, "Methodologies for the identification of Critical Information Infrastructure assets and services," ENISA, 2015, available: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis. [Accessed 14 11 2016].

Paganini, P., "GPS Spoofing, old threat and new problems," Security Affairs, 2012, available: http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html. [Accessed 14 10 2016].

Pasta, A., "A Security Evaluation of AIS," Trend Micro, 2014, available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf. [Accessed 14 10 2016].

Roberts, F.S., "Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs," Rutgers University, 2015, available: http://www.dimacs.rutgers.edu/People/Staff/froberts/CyberPhysicalSystemsFootballOilRigs1-3-15.pptx.pdf. [Accessed 14 10 2016].

Rossi, B., “Next gen security”, Computer News Middle East, 2012, available http://www.cnmeonline.com/features/next-gen-security/

Szymanski, K., “Top Ten Maritime News Stories”, InterManager, 2016, available, http://www.intermanager.org/2016/07/top-ten-maritime-news-stories-08072016/

Timorin, A., "The great train cyber robbery," SCADA StrangeLove, 2015, available: http://www.slideshare.net/AlexanderTimorin/the-great-train-cyber-robbery-scadastrangelove. [Accessed 14 10 2016].

Trend Micro, "Threats at Sea: A Security Evaluation of AIS," Trend Micro, 2014, available: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais . [Accessed 14 10 2016].

Vattenfall, Europe Wärme AG, "Technical Requirements Specification VHPready 3.0," Industrial Alliance VHP Ready, 2014, available: https://www.vhpready.com/download/vhpready-specification-version-3-0/. [Accessed 14 10 2016].

Wallischeck, E. Y., "ICS Security in Maritime Transportation," U.S. Department of Transportation, 2013, available: http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf. [Accessed 14 10 2016].

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-06-16-286-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-183-0
DOI: 10.2824/42310