Maritime cybersecurity

C A A Verkoelen* BSc Cybersecurity

* *Cybersecurity architect - RH Marine, NLD*
* Corresponding Author. Email: cor.verkoelen@rhmarine.com

Synopsis

In the past several decades cybersecurity gets increasingly more attention and impacts not only the end-users but also system administrators, system owners, and governments as well. Additionally, the frequency in which a cybersecurity incidents and/or newly discovered vulnerabilities reaches international media also increases. One could state that the area of cybersecurity has become a matured area in which not only a market exists for the protection of IT/OT systems, but in which there is also a highly skilled and developed market for the development of the next malware to infect and disturb systems. Recently, the Log4J vulnerability kept the cybersecurity community in its grip. Despite available Cybersecurity approaches to identify and evaluate risks, select security measures, and governance structures to keep in control (e.g. ISO-2700x), high impact incidents still occur. The majority of these cybersecurity frameworks are aimed at an (traditional) Information Technology (IT) environment, like typical business IT infrastructures and business users. Recent years the Operational Technology is catching up and awareness is raising to implement an adequate level of protection.

Keywords: Cybersecurity; Architecture; Integration; Marine systems

1. Introduction: Traditional approach maritime cybersecurity

Looking at the cybersecurity information reaching the media, most is regarding cybersecurity which is typically classified for Information Technology (IT) Systems. New vulnerabilities found within the latest office automation systems, new cybersecurity products launched to better protect the office IT-infrastructure. However, looking at the technology used within a maritime/naval infrastructure, there are significant differences which have resulted in a different approach and current status of protection measures that are considered as a commonality within the maritime domain.

There are two characteristics which are commonly referred to, and which are used as arguments why security measures applied within an IT-environment are not usable within maritime infrastructures. The first argument is with respect to the (inter)connectivity of the systems. The system is considered as a stand-alone system with no interconnections with external systems. The components part of the infrastructure are configured and considered as part of an overall ships infrastructure for which there is no external threat. Moreover, assumptions are made like all systems part of the infrastructure and all users which have access are considered as trusted. So the question raises, why add security functionality to a system for which there is no security threat? The second argument is the difference between IT-environments, in which most systems are not safety-critical, and maritime infrastructures on board of a ship for which safety will prevail over security. Security measures which may have an impact in the assurance of safety of the system are considered unacceptable.

This resulted in maritime architectures which focus on safety. Not implying that this approach does not contribute to the security aspect at all. A well-known model for OT-environments is the *Purdue model* in which a layered infrastructure is made, see Figure 1. This contributes to the protection profile of the system. However, actual cybersecurity measures deployed within OT-systems is traditionally circumvented.

Author's Biography

Cor Verkoelen is an experienced Cyber Security Architect. Started at the Netherlands Organization for Applied Scientific Research (TNO). Cor actively contributed to developments of new NATO security concepts, e.g. Protected Core Networking. For more than 10 years Cor is involved in defining and implementing of Cyber Security for maritime/naval platforms.

 https://doi.org/10.24868/10734

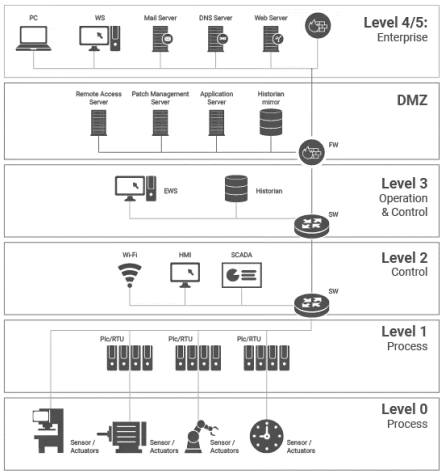

Figure 1: Overview of Purdue model for ICS systems

2. Changes in maritime cybersecurity perception

Despite of traditional perceptions of cybersecurity being an IT-environment challenge, recent security incidents influencing the (business) operations of industries which are considered an OT-based industry changed this perception. As it will be difficult to pinpoint cybersecurity as the root cause of incidents. However incident occurred at Maersk, in which an incident led to the disruption of container handling; the well-known Stuxnet in which SCADA systems where influenced; or news articles regarding maritime vessels collided due to incorrect navigational data, all are examples off possible cybersecurity incidents in OT-environments.

One could wonder why security incidents within the maritime environment are becoming more common. The earlier mentioned Purdue model of OT-infrastructures is still applicable and mostly implemented. Within the environment in which Stuxnet was deployed this model was most certainly followed, and still it was possible to hinder this nuclear program. It became obvious that there were highly skilled and motivated actors behind this cyberattack. One could state that this must be considered as exceptional. However, many governments also have acknowledged cyber as an additional (fifth) domain in modern warfare. Even if we forget this state-actor, the developments along cyber-actors become more mature and professionalised. Figure 2 is an overview of commonly acknowledged cyber-actors. All with their own intention, and potentially targeting the maritime community as their objectives may be reached by influencing/disrupting this sector or individual ships owners. Ranging from extortion, making statements, up to hindering reaching the objectives of the ship's owner.

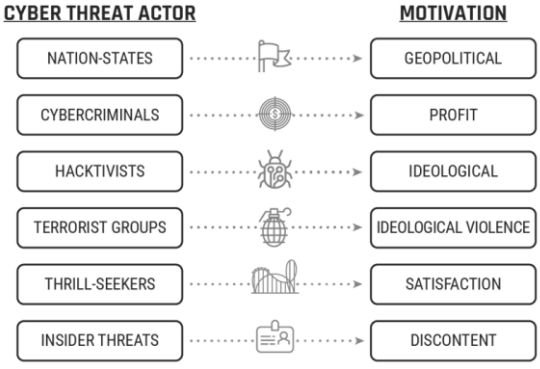

Figure 2: Overview of cyber actors|

Another change which influences the susceptibility of the maritime community to cybersecurity incidents is the application of common IT-technology as part of the infrastructure and the (internal/external) interconnectivity of the (sub)systems. As infrastructures on board are increasingly using the benefits of automation, it also builds this automation on common (IT) technology. Further automation requires even more subsystems to be able to

 https://doi.org/10.24868/10734

create situational awareness. Whereas traditionally infrastructure consists out numerous analogue signals captured by remote input/output devices and processed in (simple) Programmable Logic Controllers (PLC), currently (e.g. motor) breakers are available with own (RJ-45) network interface. Supporting the ability to be connected to IP-based infrastructures, disclosing its information and even be able to operate the breaker remotely by using commonly used IT-based protocols. These new type of devices should be protected to prevent the unauthorized operation.

Based on earlier mentioned assumption that infrastructures consists only out of well-behaving and trusted (sub)components, and lack of interconnectivity with external components, one could still downplay the relevance of cybersecurity. However, this assumption of trusted components, and no external connectivity is not valid anymore. Components integrated are considered very complex, consisting out even more components for which it is impossible to guarantee it will not malfunction or even does not contains malware. Additionally, the need for remote connection is also increasing as the added value of e.g. remote maintenance and/or remote monitoring is recognized. This combination of increasingly complex infrastructure, consisting out of a plethora of subcomponents, and the increase of interconnectivity (internal and external) leads to the renewed perception of the application of cybersecurity within the maritime community.

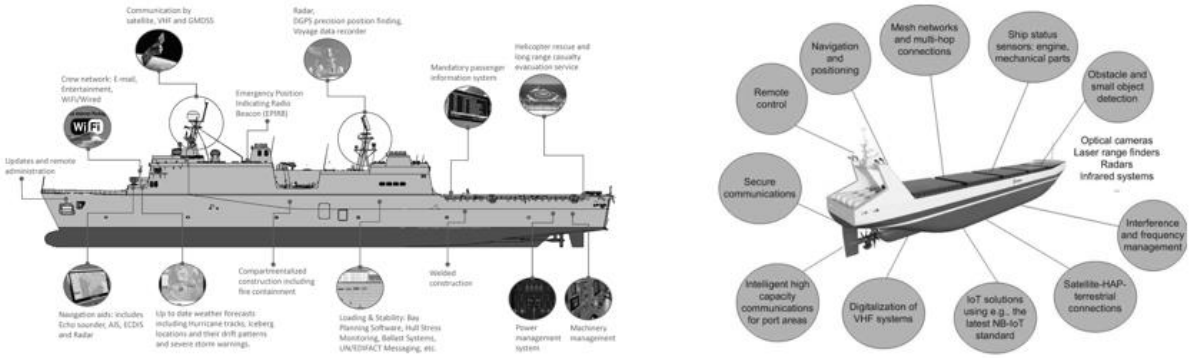

Figure 3: Typical automation and interconnections

At this point where the maritime community is aware of the potential impact and applicability of cybersecurity within a maritime platform, the question raises on how to approach this topic to have an adequate and effective protection.

3. Overview of standardization and regulations

As the awareness raises, there is also an increase in adopting this subject within different rules, regulations and standardizations. Without the intention to provide a complete overview of all rules, regulations and standardization in which cybersecurity is mentioned, the following should be considered as a subset of rules and regulations to indicate the raised awareness.

One organizations addressing cybersecurity as a topic that should be addressed is the International Maritime Organization (IMO). The IMO states "*Cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. The overall goal is to support safe and secure shipping, which is operationally resilient to cyber risks."* As the first part of this quote is generically applicable for all communities for which cybersecurity applies, therefore for IT and OT-based industries, the second part may be perceived as specifically OT-related. It addresses "*safe and secure shipping*". It introduces the needed balance between safe and secure.

 https://doi.org/10.24868/10734

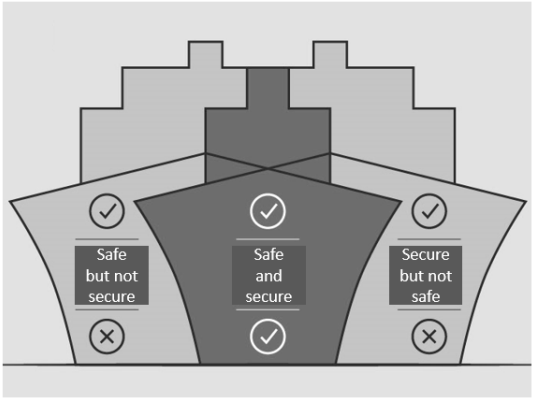

Figure 4: Balanced safety and security

For encouraging the implementation of cybersecurity within the maritime community, IMO has issued guidelines and resolutions such as the MSC-FAL.1/Circ.3 – *Guidelines on maritime cyber risk management* and the Resolution MSC.428(98) – *Maritime Cyber Risk Management in Safety Management Systems*. It started as guidelines and recommendations, the non-committal nature of these initial guidelines will change to standardization which should be complied to in the near future.

Supplemental to the IMO, classification bodies are embracing the need for better cybersecurity and have released their additional notations. As for IMO, these class notation may be seen as optional, we also see an increase in prescribing these cyber-notations in new projects and classification requests. Initial notations are developed and are still evolving and reaching a mature and stable stage at this moment. Some of the classification entities addressing cybersecurity as an emerging topic to be addresses, and their subsequent notations/guidelines, are: Det Norske Veritas (DNV) which has released *Rules for Classification – Ships – Part 6 Additional Class Notation – Chapter 5 Equipment and design features*. Within this rules for classification there is Section 21 dedicated to address cybersecurity. Its objective is set as "*to introduce measures aimed at setting up barriers to prevent, mitigate and respond to cyber security threats.*" It contains an enumeration of technical measures as well as the governance structure for all stakeholders involved. The initial notation is released in July 2019 but is further developed ever since. Other classification entities addressing cybersecurity are for example Lloyd's Register and Bureau Veritas. Both releasing Rule notes and guidance notes. Lloyd's register releasing the guidance note – *Cyber-enabled ships – Deploying information and communication technology in shipping – Lloyd's Register's approach to assurance* and Bureau Veritas releasing rules notes NR 659 DT R01 – *Rules on Cyber Security for the Classification of Marine Units* and rule note NR 642 DT R00 E – *Cybersecurity Requirements for Products to be Installed On-Board Naval ships*.

The topic of cybersecurity is also becoming increasingly common in Program-of-Requirements (PoR) which applies for suppliers and system-integrators. Initial PoR addressing self-defined cybersecurity measures are currently converging towards the aforementioned class notations which enables suppliers and system-integrators to implement and govern cybersecurity in a customer overarching approach.

One major driving force behind the enablement of establishing a customer overarching approach is the International Electrotechnical Commission (IEC) which created the International standard – *Industrial communication networks – Networks and system security*, consisting out of different parts addressing *General, Policies & procedures, System,* and *Component* topics. This standards has formed the basis and is referred to in most of the rules, regulations and standardizations created within the maritime community.

4. RH Marine cybersecurity approach

As cybersecurity within the maritime domain is gaining the attention of cyber threat actors, ships owners, classification bodies, combined with RH Marine strategic objective to be seen as a supplier of cybersecure systems, resulted in the establishment of the cybersecurity architecture. This architecture facilitates to implement cybersecurity measures which can adopt to specifics of the maritime platform. The cybersecurity architecture and the subsequent security measures are risk-based and may between different deployments of the system on various ships.

 https://doi.org/10.24868/10734

To reach this objective, RH Marine has gathered all the different aforementioned cybersecurity standards, supplemented with PoR of previous/ongoing projects in which cybersecurity is mentioned. Based on these notations, and especially taking the IEC-62443(-3-3) into account, security measures are enumerated and structured to identify different cybersecurity functionalities. These form the basis of the architecture, and should be considered as the Architectural Building Blocks (ABB) which are further specified in Top Level Designs (TLD). These TLDs are technology agnostic, as technology will (rapidly) evolve but the security function/objective itself will remain the same.

4.1. Architectural building blocks

The architectural building blocks identified for which the (technical) requirements are also allocated, is a set of fifteen ABBs. RHMNL identifies the following fifteen (interrelated) security functions:

- Communication matrix;
- Configuration Management Database;
- Logging;
- Segmentation;
- Boundary protection;
- Identity & Access Management;
- Network Access Control;
- Integrity protection;
- Hardening;
- Malware protection;
- Confidentiality protection;
- Crypto key management;
- Backup & restore;
- Vulnerability management;
- Monitoring & response.

4.1.1. Communication matrix

The objective of the communication matrix is to provide an overview of all the information flows between (sub)components of the system which are necessary for the correct operation of the system. The communication matrix provides a situational awareness regarding the behaviour of the system on the network. This situational awareness contributes to e.g. optimizing the communication profiles of (sub)components and configuration of other security functions like Monitoring & response. This overview is also used by Boundary protection functionality (Firewalling). Information flows included in the overview will be permitted by the firewall to enter/leave the sub-component. Hence, a complete overview of information flows is crucial to prevent the incorrect operation of the system due to unintentionally blocking information flows by firewalls.

4.1.2. Configuration Management Database (CMDB)

A CMDB creates an insight/overview regarding the software/configuration setup of the system. A CMDB provides an overview of all components (hardware and software) with their current configuration. A CMDB is used to store information about hardware and software assets, commonly referred to as Configuration Items (CI) of a system. The objective of establishing a Configuration Management Database is to enable processes like vulnerability management, detection of software/configuration changes, etc. The CMDB helps to understand the relationship between the components of a system and to track their configurations and deployments. The maintenance of this information allows for certain actions, such as integrity validation, incident, problem and change management of current configurations and/or the execution of the vulnerability management process. The CMDB represents the authorized configuration of the components of the system and where they are deployed.

4.1.3. Logging

The objective of the security function Logging is to provide sufficient (accounting) information which enables (security) analysis. This analysis may be triggered by e.g. the Monitoring & Response security functionality. On the other hand, the information generated for the purpose of Logging may be valuable information for the Monitoring & Response security function. Logging should enable to (based on analysis) provide the evidence which actions are carried out, and which process and/or whom is responsible for carrying out these actions. This support trouble shooting, security analysis, and possibly forensic analysis.

 https://doi.org/10.24868/10734

4.1.4. Segmentation

Applying segmentation and grouping systems into zones will have multiple benefits. This includes the reduction (of propagation) of the effects of failures; reduction of potential network congestion across the whole network; support of the need-to-know principle by limiting access to the different zones; and finally reducing the exposed attack surface by the incorporation of boundary protection at the conduits. Segmentation is augmented with Boundary controls (refer to Boundary protection).

4.1.5. Boundary protection

Boundary protection is part of the Defence-in-Depth principle and the objective of this security functionality is to provide a(n) (extra) layer of defence against malicious intrusions in the system(components) and potential (malicious) exfiltration of (sensitive) information. Additionally, the boundary protection adds a layer of prevention against unwanted usage of assets and contributes to ensuring system performance by controlling which users/information is allowed to access the system(component). Thereby contributing to preservation of the resources/capacity and latency of the protected system(component).

4.1.6. Identity and Access Management

An aspect within Cybersecurity is ensuring that only authorized entities are able to access the (components of the) system and its resources. This means that when access is requested to these resources, several actions should be taken. First of all the entity that is requesting access needs to be identified, which means information should be provided regarding who wants access. Thereafter, a second step is required which is called 'authentication'. During this second step information needs to be provided which proves the identity provided during the first step. In case the identity of the entity is verified during the authentication, the last step is determining the authorizations of the entity. Based on the authorizations the entity requesting access will be granted access, or the access request will be denied.

Controlling/regulating this access to the system is a fundamental because it will prevent unauthorized entities to access the system and cause harm to the system, such as installation of malware and/or changing configuration parameters which will disrupt the normal operation of a system. To realize this controlled access the identities and access privileges needs to be controlled/managed. This controlling/managing of identities and access is precisely the objective of the security function Identity and Access Management (IAM). Where IAM is a commonly and broadly applied technique within the traditional IT, applying this technique within environments where safety is a major concern needs special attention during specification/design and implementation.

4.1.7. Network Access Control

The objective of Network Access Control (NAC) is to deny rogue and unauthorized access to the network. To realize this, NAC as a security function realizes/uses authentication, authorization and possibly accounting of network connections. Implementing NAC should be considered as one of the Defence-in-Depth layers to prevent cyber-attacks and contributes to the overall Cyber Security of the system. NAC represents a category of security products/technologies for which the definition of NAC is both evolving and controversial.

The overarching generic objectives to which the concept of NAC contributes can be distilled as:

- Mitigation of zero-day attacks;
- Authentication, Authorization, and Accounting of network connections;
- Encryption of traffic to the wireless and wired network;
- Role-based controls of user, device, application or security posture post authentication;
- Automation of network role based on other information such as known vulnerabilities, jailbreak status

4.1.8. Integrity Protection

Integrity is the property of assuring the accuracy and completeness of information and/or functionality during their (entire) lifetime. Hence, the objective of integrity protection is the prevention of unauthorized changes, and/or the ability to adequately detect, unauthorized changes to information and/or functionality of the cyber physical system. Often a distinction is made between:

- Integrity protection *of the information* that is generated by; stored on; and/or transferred;
- Integrity protection *of the functionality* that is provided by the cyber physical system.

 https://doi.org/10.24868/10734

Both categories are included in one security function. The reasons behind this grouping are their relation/similarities and the prevention of unnecessary confusion that may be introduced in case a forced split-up if these categories is pursued.

4.1.9. Hardening

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The objective of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within the IT ecosystem.

4.1.10. Malware protection

Malware is any kind of software that is developed with the intention to cause damage to a (component of a) IT/OT system. This (component of the) system can be any kind of device and/or network peripheral including workstations, client, PLCs, routers, switches, et cetera. Malware is not limited to main stream software like Microsoft Windows® computers. There is malware for almost any type of hardware and software. Some malware targets PLCs (e.g. Stuxnet), other targets routers and modems (e.g. the Mirai botnet), and another targets IoT devices. It can also specifically target security devices like firewalls. Because of the intention to harm these systems, malware differs from bugs. Bugs may also cause harm to the (components of the) system, however a bug is not intentionally developed/integrated. A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware.

Because of the hostile intent of malware and the frequent usage of malware by all kind of threat actors, malware should be considered a real threat against the systems delivered by RH Marine. Therefore, the objective of the security function Malware protection is to prevent the infection of (components of the) system with malware. This may be combined with security functions like Boundary protection (e.g. firewalling which may prevent the entrance of malicious traffic and/or traffic from malicious sources) and Monitoring and Response in case systems are despite of malware protection infected, a fast and adequate detection will be realized.

4.1.11. Confidentiality protection

The information that is generated/processed within (components of) the system may have sensitive characteristics. Examples of information with sensitive characteristics are information regarding the capabilities of the ship, and information which may provide an insight with respect to the employability of the ship. The level of sensitivity of the information can be expressed using different classification schemes. Information may be classified using schemes such as commercial confidential or personnel confidential. The objective of the confidentiality security function is to protect the information consistent with the level of classification. This protection applies to the information that is exchanged between (components of the) system, and between (components of the) system and external components. This is known as confidentiality protection of the data in transit. Additionally, the information needs to be protected in case the information is stored on (components of) the system. This is known as confidentiality protection of data at rest.

4.1.12. Crypto key management

As multiple/more security measures rely on a cryptographic operation, the cryptographic keys used by these operations should be managed to be able to e.g. decrypt encrypted information. Where traditionally keys may be registered manually and documented in an offline (e.g. notebook) system, current system requires a key management system which is interconnected to generate, revoke, renew cryptographic keys.

4.1.13. Backup and Restore

Within cyber security different categories of security measures may be identified. Most commonly known are the security measures that are aimed at the prevention of an incident to occur. However, it is not realistic to assume no incident will ever occur. Therefore, security measures with the objective to detect and limit the consequences of an incident are required. The security function of Backup & restore aims to limit the consequences of a security incident (or system disruption) by providing the ability to restore the system (to a state before the incident occurs, or even before the infection of the system occurs). This means that the objective of the Backup & restore is to

 https://doi.org/10.24868/10734

enable to create a backup of the information (or system as a whole), securely store this backup, and the ability to restore a previously made (and stored) backup of the information (or the system as a whole).

4.1.14. Vulnerability management

The objective of vulnerability management is to create an overview/inventory of (all) potential weaknesses that may be present within (components of) the system, and support the informed decision making process (risk management) that is aimed at reducing the ultimate attack surface of the (components of the) system by providing guidance, support, and implementation of appropriate security measures. It is important to realize that vulnerability management is not a one-time activity, but should be considered throughout the entire system life cycle, and should be re-evaluated periodically.

Currently unknown/undetected vulnerabilities will be discovered over time and new vulnerabilities are made public. This enables potential attackers to abuse the newly discovered weaknesses, but it will also enable system suppliers and system users to evaluate the impact of newly identified weaknesses/vulnerabilities and take appropriate security measures to provide sufficient protection.

4.1.15. Monitoring and Response

The purpose of the monitoring and response is to systematically observe services and service components, and record and report selected changes of state identified as events. This practice identifies and prioritizes infrastructure, services, business processes, and information security events, and establishes the appropriate response to those events, including responding to conditions that could lead to potential faults or incidents.

4.2. Architectural building blocks and relations

Figure 5 shows the interrelations between the different Architectural Building Blocks.

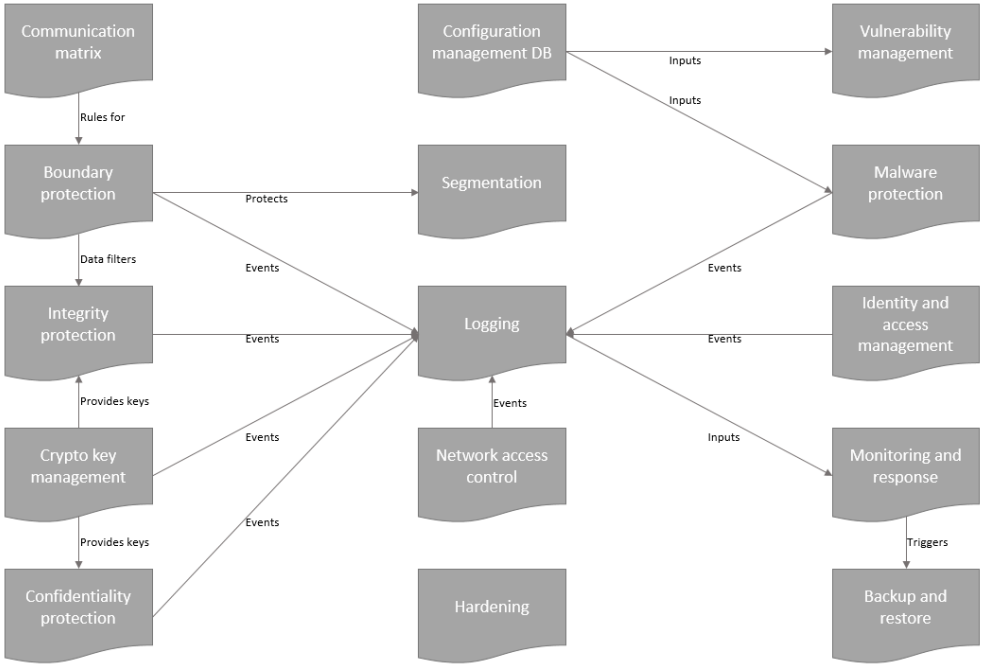

Figure 5: Interrelations

 https://doi.org/10.24868/10734

5. Conclusions

As first implementations of the cybersecurity architecture are ongoing and reaching completion. Some first observations can be made. The first observation is that during the translation of the ABB into the solution building blocks, there are a lot of security measures which may fulfil the requirements within an IT-environment. As expected the applicability of these solutions within an OT environment is in some cases limited. An example of this limited applicability is the Identity and Access Management, where this is within an IT environment a common measure (logon to a system); within OT this is not always accepted. Within RH Marine we had to tailor-made the solution to be accepted within an OT-environment. However, some security measures may benefit from the well-established knowledge available within IT-environments. An example is Logging, where this is broadly available within an IT-environment, the collection and analysis of these loggings may be based on available (unstructured) datastores and big-data analysis concepts.

A second observation is the awareness of the blurring of the boundaries between IT and OT, without falling in the pitfall where IT measures are blindly applied within OT. Where IT security products have tried to gain the position where their products can be used, new security products and vendors have risen which are specifically tailored to OT, where knowledge and experience finds is base the OT environment background.

Finally, a governance structure which becomes clearer in which e.g. classification bodies embrace cybersecurity and (re)use commonly cybersecurity governance/management standards. As cybersecurity will not disappear and is here to stay, structuring a well-defined and future proof cybersecurity architecture has become a license to operate within all environments.

Acknowledgements

The author would like to thank RH Marine to create the opportunity to establish this well-defined cybersecurity architecture. The freedom in defining this architecture, the support of all team members within RH Marine, and especially within the department of Cyber Systems significantly contributed to have a good and trusted outlook to the future.